INTRODUCTION

Marie-José DURAND-RICHARD[1] et Philippe GUILLOT[2]

La cryptologie envahit de plus en plus notre quotidien sans que nous en soyons pleinement conscients. De nombreux usages nouveaux en attestent : carte bancaire, carte vitale, TV à péage, protection des transactions sur Internet, passeport et carte d'identité biométriques, titres de transport électroniques, *etc*. Invisible, non dite et donc essentiellement impensée, cette pratique implicite du secret ne risque-t-elle pas de s'insinuer dans les rapports sociaux au point d'en modifier sensiblement la teneur ? La question mérite d'être posée. Cette banalisation du secret des échanges semble en effet contraire à l'idée d'une libre circulation de l'information, pourtant affirmée comme constitutive de la démocratie. Elle suppose et installe une séparation de fait entre ceux qui échangent à l'intérieur des réseaux ainsi mis en place et ceux qui en sont exclus, au point qu'il est permis de se demander ce qu'il s'agit de protéger exactement : l'autonomie des individus ou la puissance des systèmes organisateurs de ce type d'échanges ? Les nouveaux enjeux de la cryptologie se nouent dans cette opposition entre secret et transparence, entre protection et diffusion des informations et des connaissances. Ils interrogent la signification de ces nouveaux modes d'échange.

Aussi moderne qu'elle puisse apparaître, la cryptologie n'est cependant pas réductible aux supports technologiques – essentiellement informatiques – qui en assurent aujourd'hui le fonctionnement, et grâce auxquels elle se diffuse à grande échelle. Les questions que soulève sa propagation interrogent autant l'évolution de son contenu scientifique et technique que l'évolution de son statut comme discipline et comme phénomène de société. Avec ses deux composantes : la cryptographie ou chiffre de défense, et la cryptanalyse ou chiffre d'attaque, elle n'est devenue

[1] mjdurand.richard@gmail.com. Chercheuse associée, Université Paris Diderot, Sorbonne Paris Cité, SPHERE, UMR 7219, CNRS, F-75205 Paris, France.
[2] philippe.guillot@univ-paris8.fr. Maître de conférences, LAGA, UMR7539, CNRS-Université Paris 8 Vincennes Saint-Denis.

une discipline académique que récemment, installée au cœur des mathématiques, au carrefour entre science, industrie et société. Mais en tant qu'art du secret, la cryptologie a existé bien avant de devenir cette discipline aujourd'hui mathématisée et enseignée dans les universités. Elle était alors pratiquée et transmise dans les mileux diplomatiques et militaires, voire commerciaux, là où le secret de certaines informations revétait une importance stratégique. Elle reposait sur la transmission d'un savoir-faire confidentiel, et a bénéficié plus récemment de formations spécifiques à accès réservé. Pratiquée à l'écart des lieux ouverts de production du savoir, la cryptologie s'est longtemps développée par à-coups, ballottée, oscillant, hésitant entre situations de blocage et réinventions successives, du fait même de sa diffusion limitée. C'est l'ensemble de ces transformations, c'est-à-dire l'analyse des différents « régimes de production, de régulation et d'appropriation » de ce savoir – selon l'expression de Dominique Pestre[3] – qu'il s'agit ici d'analyser pour mieux appréhender la mutation des enjeux que connaît la cryptologie depuis ces dernières décennies.

Cet ouvrage rassemble les éléments d'analyse issus d'un dialogue engagé entre historiens, mathématiciens et cryptologues professionnels, lors des journées d'études organisées au département de mathématiques et d'histoire des sciences de l'université Paris 8, et soutenu par le laboratoire SPHERE d'histoire et de philosophie des Sciences (CNRS-Université Paris-Diderot). Restituer une histoire de la cryptologie en tant que phénomène à la fois scientifique et social suppose en effet un double travail d'analyse. Il s'agit d'une part, d'éclairer directement de l'intérieur les rationalités mises en œuvre pour répondre aux nécessités du secret, et d'autre part, d'observer de l'extérieur l'ensemble des facteurs qui interviennent sur leur développement. Les interrogations issues de ces regards croisés introduisent un recul qui permet d'élaborer un récit historique mis à distance de ses acteurs directs, qu'il s'agisse des chiffreurs du passé ou des mathématiciens d'aujourd'hui. Sont ainsi présentés dans cet ouvrage trois types de textes :

– des témoignages de chercheurs ou de spécialistes des services du chiffre, qui restituent à la fois leur travail au quotidien et l'inertie institutionnelle que doit affronter toute initiative en ce domaine, qu'elle soit de nature conceptuelle ou organisationnelle,

– des traductions de textes fondamentaux, qui concernent trois moments innovants jugés cruciaux pour la cryptologie : l'émergence de la cryptanalyse dans le monde arabe au neuvième siècle, celle de la cryptologie à clé publique dans les années 1970 aux Etats-Unis, et une analyse des relations turbulentes entre mathématiques et cryptologie aujourd'hui,

[3] Pestre, *Introduction aux 'Sciences Studies'*.

– des analyses historiennes tendant à se démarquer des entreprises hagiographiques et à inscrire les activités cryptologiques dans des perspectives contextuelles à plus long terme.

Avant que la cryptologie ne soit investie par les mathématiciens et qu'elle ne prenne une place essentielle au sein des mathématiques appliquées, elle a longtemps été pratiquée comme manipulation du langage écrit, s'appuyant sur des procédés manuels et un état d'esprit bricoleur, enracinée dans des pratiques artisanales, dont elle a conservé le caractère inventif. Dès le départ, il s'agissait pour le cryptographe de trouver des moyens pour dissimuler le sens d'un message, et pour le cryptanalyste, de retrouver le sens caché d'une succession erratique de lettres, en repérant, sous ce désordre construit, des régularités déjà éprouvées dans l'analyse des mots du langage lui-même. Cette pratique s'auréolait volontiers d'une certaine mystique du langage, propre à la recherche de ce sens caché. Nous retracerons dans le premier chapitre l'ancrage de la cryptologie dans ces jeux d'écriture, telle qu'elle a si longtemps été pratiquée avant qu'elle ne s'instrumentalise sous la forme d'un calcul.

Si ces pratiques peuvent être lues aujourd'hui en termes mathématiques, les retranscrire en ces termes pour en faire l'histoire constituerait un anachronisme. C'est bien dans un cadre strictement linguistique qu'elles se sont mises en place. Lorsque la cryptanalyse prend naissance dans le contexte de la civilisation arabo-musulmane, elle émerge dans le même mouvement d'analyse de la structure des langues que celui qui accompagne la naissance de l'algèbre[4]. Étymologiquement d'ailleurs, la référence au « chiffre », traduction du mot anglais *cipher*, provient du mot arabe *sifr* qui désigne le zéro, symbole qui marque une absence dans la numération de position avant de devenir beaucoup plus tard un nombre à part entière. Le plus ancien traité de cryptanalyse qui nous soit parvenu est celui du philosophe al-Kindi (801-873). Son traité est le fruit d'un travail systématique d'analyse et de classification des méthodes, mis en place à la « Maison de la sagesse » (*Bayt al Hikma*) de Bagdad, et qui se prolongera jusqu'au 14e siècle. Al-Kindi établit une technique de comptage des lettres susceptible d'être lue aujourd'hui en termes statistiques d'analyse des fréquences. Mais il s'attache avant tout, à partir d'un travail sur la langue arabe, à classifier les procédés d'« obscurcissement » des textes et à organiser des méthodes pour « extraire l'obscur », comme le montre ce traité traduit par Abderrahman Daif et Kaltoum Tantatoui au chapitre « Sur l'extraction de l'obscur »[5].

À la Renaissance, avec la constitution des « cabinets noirs » dans les principales cours européennes, l'activité de chiffrement et de décryptement

[4] Rashed, *Al-Khwarizmi, le commencement de l'algèbre,* pp. 11-30.
[5] Voir p. 63.

se répand dans les cercles de pouvoir, couplée avec l'espionnage des dépêches diplomatiques au moment même où les humanistes s'interrogent sur les moyens de pénétrer les secrets de la nature[6]. Le diplomate Blaise de Vigenère (1523-96) est l'un d'eux, qui synthétise un mode de chiffrement plus élaboré, le chiffrement polyalphabétique, réputé pendant très longtemps indéchiffrable. Certains mathématiciens sont impliqués dans ces cabinets noirs, comme François Viète (1540-1603) en France ou John Wallis (1616-1703) en Angleterre. Ils appliquent systématiquement leurs méthodes mathématiques à la cryptanalyse, avec parfois des effets en retour sur l'algèbre. Mais l'analyse des caractéristiques du langage, la recherche des mots probables[7], les intuitions sur le sens des messages, restent des outils déterminants pour parvenir à retrouver les messages en clair.

Au cours de la Première Guerre Mondiale, les méthodes de décryptement, toujours attachées pour une bonne part à l'intuition et à la connaissance de la langue, ont connu des succès remarquables. Sophie de Lastour retrace, au chapitre « Les travaux de la Section du Chiffre pendant la Première Guerre Mondiale »[8], les conditions dans lesquelles ont été décryptés le télégramme de Zimmerman en 1917 par les cryptanalystes britanniques, et le fameux radiogramme de la victoire en juin 1918 par le polytechnicien français Georges-Jean Painvin (1886-1980).

Cette pratique du secret n'est pas restreinte à l'activité des cercles diplomatiques et militaires. Elle concerne plus largement des groupes sociaux bien constitués, mais qui tiennent à ce que leurs communications restent confidentielles. Les classes cultivées se passionnent pour les jeux de langage ; les codes secrets font partie de leur culture, même si les méthodes qu'ils utilisent restent souvent très rudimentaires. Avec le développement de la presse, des messages chiffrés sont publiés dans les journaux, comme les *Agony Columns* du *Times*, ces nombreux échanges discrets de l'aristocratie anglaise, dont Charles Babbage (1791-1871) répertorie les techniques dans son riche manuscrit non publié « Philosophy of Deciphering », au moment où il décrypte le chiffre de Vigenère. L'officier prussien Friedrich W. Kasiski (1805-81), qui le décrypte lui aussi quelque temps plus tard, s'est initié à la cryptographie dans les journaux. Celle-ci reçoit même une certaine diffusion, comme dans les écrits d'Edgar A. Poe (1809-49), l'un des premiers maîtres du suspense au 19e siècle. Cette diffusion va également s'étendre aux milieux commerciaux avec le développement du télégraphe, où le chiffrement intervient pour protéger le contenu des échanges, tant du regard des employés du télégraphe que de celui des concurrents.

---

[6] Coumet, « Cryptographie et numération ».

[7] La technique du *mot probable* est un procédé de décryptement qui repose sur l'hypothèse qu'un certain mot figure probablement dans le message en clair, par exemple *Sire*, ou *Mon Général*.

[8] Voir p. 87.

Quoi qu'il en soit, avec l'industrialisation des pays occidentaux, ce sont d'abord les États qui, pour des raisons économiques et militaires, vont s'assurer la maîtrise de ces nouveaux systèmes de communication, surtout avec l'installation des réseaux transatlantiques. Dès lors que les messages chiffrés sont susceptibles de circuler entre de nombreuses mains, le secret doit changer de nature, et s'attacher davantage au système d'échanges qu'au message chiffré proprement dit. Le principe énoncé par Auguste Kerckhoffs (1835-1901) en 1883, affirmant que le procédé de chiffrement doit pouvoir sans dommage tomber entre les mains de l'ennemi, et que le secret ne doit résider que dans une clé, relève d'un remarquable effort d'adaptation des moyens de la cryptographie aux échanges télégraphiques nationaux et internationaux. Cette mutation des enjeux de la cryptographie, qui passe ainsi de l'analyse du message chiffré à celle du système cryptographique, est analysée par Marie-José Durand-Richard dans le chapitre « Du message chiffré au système cryptographique »[9], mettant en lumière certains travaux fondateurs de la cryptologie moderne, comme ceux de Gilbert Vernam (1890-1960), Claude E. Shannon (1916-2001) et Horst Feistel (1915-90).

Cependant, au début du 20e siècle, la cryptologie reste toujours principalement une activité manuelle, marquée par l'ingéniosité d'acteurs talentueux dotés de compétences tant mathématiques que linguistiques. La multiplication des échanges télégraphiques et téléphoniques, ainsi que la mécanisation matérielle du calcul, vont jouer un rôle crucial dans un développement devenu plus collectif des activités cryptologiques. Des mathématiciens professionnels sont progressivement intégrés dans les équipes travaillant dans ce secteur d'activité. La mécanisation des calculs suppose une adaptation des méthodes aux machines, et donc une explicitation des différentes étapes du calcul, qui débouche sur la réalisation d'opérations de plus en plus complexes. Cette évolution met au premier plan les procédures de calcul initialement réalisées dans des dispositifs spécifiques, spécialement conçus et fabriqués pour effectuer les opérations requises. Se dégage ainsi la notion d'algorithme, qui va marquer l'abandon progressif de la référence au sens antérieurement à l'œuvre lors du recours aux mots probables dans les décryptements. Les échanges entre théorisation mathématique et techniques cryptographiques deviennent alors systématiques. Ce type d'évolution s'observe notamment dans le recours à l'algèbre. Le chiffre élaboré par Lester S. Hill (1890-1961) en 1929 et 1930, qui utilise des matrices modulo 26 – la taille de l'alphabet latin – semble être le premier système à se référer explicitement aux structures algébriques. L'entre-deux-guerres a vu la construction des premières machines mécaniques, puis électromécaniques, opérant explicitement sur un alphabet représenté par des entiers modulo 26, comme les machines C35 et C36,

[9] Voir p. 107.

commandées par l'armée française à l'industriel suédois Boris Hagelin (1892-1983). La Seconde Guerre Mondiale va encore amplifier la concentration des moyens de recherche autour de la question des communications et du calcul. Cette période voit se renforcer les relations entre recherches théoriques et développements technologiques. À la fin des années 1940, Claude E. Shannon, à la fois ingénieur et mathématicien, sera à son tour au cœur d'un basculement entre l'usage des statistiques propre à l'analyse des fréquences, et celui des probabilités, exprimant le message comme un choix dans un ensemble de possibles. L'évolution de la cryptologie comme discipline mathématique a marqué un changement dans les relations entre les domaines diplomatiques, militaires et civils. André Cattieuw retrace cette évolution pour la France au 20e siècle au chapitre « La cryptologie gouvernementale française »[10].

À l'origine, le secret résidait principalement dans le procédé lui-même, qui suffisait à en faire un savoir-faire protégé. Cette contrainte s'est avérée contre-productive avec la mise en place du réseau télégraphique. Il est devenu nécessaire de mettre en avant la clé comme élément central du secret. Avec la mathématisation des procédés cryptographiques, la clé elle-même, en devenant une suite de symboles aléatoires, peut être traitée comme un objet mathématique. La connaissance publique du procédé de chiffrement devient un argument de sécurité en ce sens qu'une communauté de cryptologues, devenue internationale, va pouvoir l'étudier, le décrypter, l'améliorer, pour finalement avérer sa résistance. Avec le renforcement de la sécurité des procédés de chiffrement, la confidentialité des messages anciens devient vaine. La sphère du secret se déplace et se réduit en même temps que sa qualité se renforce. Ce mouvement de réduction de la part secrète dans un mécanisme cryptographique a abouti à ce qui s'est appelé la « révolution des clés publiques ». Avec celle-ci, le système cryptographique s'appuie sur deux clés : la clé de chiffrement, mise à la disposition de tous dans un annuaire, et la clé de déchiffrement, différente de la précédente, seule à devoir rester secrète. Les promoteurs de cette nouvelle cryptographie ont ainsi résolu le problème crucial du transport des clés sur un réseau de plus en plus ouvert et où les protagonistes ne font qu'échanger des informations sans jamais se rencontrer physiquement. De ce fait, elle est largement déployée dans tous les dispositifs qui nous sont familiers : carte bancaire, paiement sécurisé en ligne, *etc*. Cette « cryptologie paradoxale », comme la nomme Jacques Stern[11], a été motivée par la nécessité de protéger les communications entre ordinateurs, et de garantir les nouveaux échanges commerciaux qu'ils permettent de réaliser. Elle mobilise des mathématiques de plus en plus élaborées. Par leur article fondateur de 1976, Whitfield

[10] Voir p. 153.
[11] Stern, *La science du secret*.

Diffie (né en 1944) et Martin Hellman (né en 1945) ont jeté les bases de la cryptologie à clé publique. Une traduction de cet article figure au chapitre « Les nouvelles orientations de la cryptographie »[12].

Il a néanmoins fallu deux années de nouvelles recherches pour aboutir à un système cryptographique effectif qui réalise les ambitions de Diffie et Hellman. Le RSA, du nom de ses auteurs Ronald Rivest (né en 1947), Adi Shamir (né en 1952) et Leonard Adleman (né en 1945), s'appuie sur la difficulté de factoriser les grands entiers. La cryptologie voit alors s'opérer une mutation en investissant des problèmes mathématiques connus pour être difficiles à résoudre, relevant de l'algèbre et de la théorie des nombres. La rencontre de la cryptologie et de l'algèbre est manifeste dans les premiers systèmes à clé publique Diffie-Hellman et RSA. Elle l'est plus encore aujourd'hui, où la géométrie algébrique constitue un élément important de la recherche cryptographique contemporaine avec l'utilisation des courbes elliptiques et des accouplements de points, lesquels permettent la réalisation de nouvelles fonctions cryptographiques comme la cryptographie à clé publique choisie, ou l'identité du destinataire peut être utilisée comme clé de chiffrement.

Face à ces nouveaux procédés cryptographiques réputés mathématiquement inviolables, l'ingéniosité des attaquants se tourne désormais vers les dispositifs mettant en œuvre les calculs, par l'exploitation de la fuite des secrets par des canaux inattendus, comme le bruit des téléscripteurs, la consommation électrique des processeurs électroniques, leur rayonnement électromagnétique, le temps de calcul ou encore l'injection intentionnelle de fautes dans leur fonctionnement. Ce sont ces techniques, relevant de la physique, qui ont rendu inopérants certains mécanismes de protection mis en œuvre par exemple dans la TV à péage dans les années 2000. La mise en évidence de ces failles et les corrections apportées résultent d'une coopération de plus en plus étroite entre mathématiciens et ingénieurs électroniciens. Dans son chapitre sur le rôle de la carte à puce en cryptologie[13], Louis Guillou montre comment cet objet aujourd'hui familier, archétype de tels dispositifs, a évolué dans ce contexte en France, parallèlement à la cryptologie.

Au chapitre « Crypotographie et théorie des nombres »[14], Catherine Goldstein réinterroge les dynamiques à l'œuvre dans la constitution de la cryptologie comme discipline académique, et souligne les multiples façons de la concevoir selon les critères retenus pour la définir comme telle. Reprenant la double temporalité de son histoire, entre la longue durée de l'art du secret et la courte existence de la cryptographie contemporaine, elle

[12] Voir p. 173.
[13] Voir p. 203.
[14] Voir p. 245.

examine les proximités antérieures, entre cryptographie et théorie des nombres au 17e siècle, entre théorie des nombres et industrie aux 19e et 20e siècles. Cette analyse montre l'importance des contextes dans le processus d'émergence d'un nouveau champ de savoir, bien au-delà d'un simple processus de transfert ou d'appropriation de connaissances.

Dans le contexte actuel, si la cryptologie contemporaine emprunte beaucoup aux mathématiques, elle leur offre aussi de nouveaux débouchés, et tend à fonctionner en retour comme forme de légitimité de l'activité mathématique elle-même. Les premières conférences publiques et formations en cryptologie datent des années 1980. Elles marquent le début de la reconnaissance de la cryptologie comme une discipline académique à part entière, multipliant les échanges entre techniques cryptographiques et théorisation mathématique. Jean-Louis Nicolas, au chapitre « L'influence de la cryptologie moderne sur les mathématiques et l'université »[15], témoigne de ce moment où des formations de haut niveau en cryptographie ont été établies en France à partir d'initiatives relativement individuelles, le premier congrès *Eurocrypt* de 1984 à la Sorbonne inspirant la constitution du premier DEA (Diplôme d'Études Approfondies) de Cryptographie et Optimisation à l'université de Limoges en 1985.

Désormais au cœur des mathématiques appliquées, la cryptologie devient elle-même une discipline scientifique à part entière, voire une branche des mathématiques théoriques. Ainsi, la fin du 20e siècle a vu naitre la théorie cryptographique, en réponse au problème posé par la découverte de failles dans des procédés pourtant érigés comme normes. Il devient crucial, pour la protection de systèmes de communication déployés au niveau mondial, d'accompagner tout procédé cryptographique d'arguments attestant la qualité de la sécurité qu'il est censé garantir. Cette branche de la cryptologie contemporaine énonce des théorèmes prouvant la sécurité des procédés cryptographiques, en s'appuyant sur une modélisation formelle de l'adversaire et sur l'hypothèse que le problème mathématique sous-jacent est aujourd'hui insoluble en pratique.

Du fait de cette intrication renforcée avec les mathématiques, certains acteurs de cette théorie cryptologique, comme Jonathan Katz et Yehuda Lindell[16], affirment avec force la mutation de la cryptologie d'art en science, contrastant avec l'ingéniosité intuitive déployée par les premiers artisans du chiffre. Cette revendication de scientificité suscite cependant des questions dans la mesure où les implications socio-politiques de cette discipline placent la question de la sécurité bien au-delà de la seule démonstration d'un théorème. La référence nouvelle à la notion de « sécurité prouvée » induit l'idée que la sécurité est aujourd'hui affaire de théorie mathématique. Le

[15] Voir p. 267.
[16] Katz et Lindell, *Introduction to Modern Cryptography*.

calcul ne peut pourtant être complètement dissocié du dispositif qui l'effectue ni du système qu'il est supposé protéger. Il se trouve fortement soumis aux progrès considérables de la puissance de calcul observés depuis plusieurs décennies en informatique. Cette tension entre effort de théorisation et dépendance technique se traduit par des relations tumultueuses entre mathématiques et cryptologie, que le mathématicien Neal Koblitz met en évidence dans un article dont nous présentons la traduction au chapitre « La relation agitée entre mathématiques et cryptographie »[17].

Ce débat est fondamental, dans la mesure où il réintroduit la question du sens à la fois en cryptologie et en mathématiques, une question trop souvent passée sous silence du fait de la nature même de ces deux disciplines. La cryptographie vise à dissimuler le sens d'un message, et la cryptanalyse a longtemps porté sur des procédés d'analyse liés à la structure de la langue, même si elle devait aussi avoir recours à la recherche de mots probables. L'abandon de toute référence au sens dans les pratiques cryptologiques s'est progressivement installé avec leur mécanisation et leur structuration par les mathématiques. La cryptologie traitant de messages chiffrés par des méthodes mathématiques, le problème de la signification n'y est plus abordé. Qui plus est, il est classique d'affirmer que les mathématiques ne signifient que pour elles-mêmes, qu'elles trouvent leur raison d'être du seul fait de l'agencement interne de leur édifice théorique. De fait, cette idée d'un abandon du sens en mathématiques s'appuie sur un mode de théorisation du langage qui ne prend en compte que ses dimensions syntaxiques et sémantiques et qui les envisage séparément. Chez les mathématiciens, la pensée de Descartes n'est jamais loin, lui qui voyait la syntaxe comme grammaire du langage, et affirmait qu'un dictionnaire à entrée unique permettrait de définir une langue parfaite. Or, parmi les théories du langage développées au 20e siècle, la pragmatique revendique la polysémie du langage comme une richesse. Et les significations sont en général multiples, même en mathématiques, dès lors que se trouve restituée la pluralité contextuelle de ses interventions[18]. En ce qui concerne la cryptologie en tant que discipline mathématisée, sa présence dans de nombreux domaines de la vie publique rend donc d'autant plus légitime de poser la question de ses implications signifiantes pour les sujets qui la pratiquent : non pas pour le sujet ou l'humain en général, mais pour ses différents acteurs selon la place qu'ils occupent dans la société, et plus spécifiquement dans les réseaux de

[17] Voir p. 285.

[18] À titre d'exemples significatifs de ces théories du langage développées surtout au 20e siècle, et qui mobilisent les contextes de l'énonciation, on peut se référer à : Austin, *Quand dire, c'est faire* ; Ricœur, *La métaphore vive* ; Victorri et Fuchs, *La polysémie, construction dynamique du sens.*

communication dont la cryptologie permet de garantir une partie de la gestion.

L'art du secret a longtemps été associé aux classes dirigeantes et à la stratégie militaire. Aujourd'hui, avec le développement des ordinateurs et la prégnance de la notion d'information, la cryptologie contribue à la gestion de très nombreux secteurs de la vie civile comme en témoignent par exemple la carte à puce et le téléphone mobile. Un tel basculement de son champ d'activité introduit des questions nouvelles quant aux modes de pouvoir et de contre-pouvoir dont disposent les acteurs d'une société qui se veut gouvernée par des principes démocratiques, où la circulation de l'information et la liberté de connaître sont des valeurs fondamentales. L'expression de Francis Bacon (1561-1626), « savoir c'est pouvoir »[19], peut se conjuguer aujourd'hui en termes d'information. Et les débats portent précisément sur l'étendue du pouvoir que peut conférer toute innovation du côté des organisateurs de réseaux, et toute initiative du côté de leurs utilisateurs, de telle sorte que soient préservés les équilibres indispensables au fonctionnement démocratique d'une société. Les termes du débat peuvent d'ailleurs se trouver faussés si les différents acteurs n'ont pas la même audience pour s'exprimer, et lorsque les véritables enjeux économiques sont passés sous silence. C'est ainsi que le chiffrement des contenus multimédia, sous couvert de défense du droit d'auteur, protège essentiellement le modèle économique des sociétés de production audiovisuelle. Et les véhicules automobiles sont aujourd'hui dotés de moyens cryptologiques d'anti-démarrage pour limiter les coûts associés au traitement des vols, à la demande des compagnies d'assurance. La cryptologie est devenue une technologie nécessaire pour mettre en confiance les acteurs du commerce électronique et permettre son développement.

Plus fondamentalement encore, celui qui détient une information détient un pouvoir lié à la connaissance de cette information, et celui qui maîtrise les conditions d'échange de cette information jouit d'un pouvoir bien plus considérable encore. L'ampleur du développement du programme d'interception ECHELON[20] témoigne de l'importance accordée par les autorités des États-Unis à cette dimension. C'est dire que, s'il existe un discours sur la science qui l'associe à l'ambition de rendre le monde transparent à la connaissance, cette même science reste traversée par des enjeux économiques qui l'installent dans le non-dit et le secret. Les marqueurs RFID (*Radio Frequency IDentification*), par leur capacité à lire des informations à distance, sont présentés comme une contribution à l'accroissement de la productivité, mais ils sont également considérés

[19] Bacon, « *Nam et ipsa scientia potestas est* », in Bouillet, *Œuvres philosophiques de Bacon*, tome 3, p. 474.
[20] Voir note 87 p. 143.

comme une menace sur l'identité numérique de chacun. Cette tension entre liberté individuelle et contrôle social se joue autour du problème de la confidentialité des échanges. Elle n'a sans doute rien de nouveau dans son principe, mais devient une question cruciale du fait de son importance stratégique, et du fait qu'elle participe massivement à l'organisation des échanges sociaux. Un conflit entre les tenants du maintien d'une cryptologie contrôlée par les états, et les partisans de sa libéralisation induite par le développement du commerce électronique, s'est manifesté très explicitement dans les années 1990. Une telle tension se manifeste encore aujourd'hui sous couvert de lutte antiterroriste, où des états peuvent adopter des mesures de protection qui ne sont pas sans risque sur leur organisation démocratique propre. Les documents publiés en juillet 2013 par Edward Snowden, ancien consultant privé auprès de l'agence de sécurité états-unienne NSA (*National Security Agency*) ont révélé au grand public l'existence d'un programme « PRISM » (*Planning tool for Resource Integration Synchronization and Management*) permettant aux autorités états-uniennes d'accéder aux données personnelles de tous les utilisateurs de leurs plus grands fournisseurs d'accès à l'Internet, en totale contradiction avec le droit à une correspondance privée inscrit dans la loi de la plupart des pays[21].

C'est cependant au sein même de cette cryptologie, utilisée comme instrument institutionnalisé au service du pouvoir économique, que s'est développé le mouvement d'inspiration libertaire *Cypher Punk*, pour qui la cryptologie est un moyen qui permet à l'individu de protéger ses droits et sa vie privée contre le contrôle étatique et policier. Et c'est dans la mouvance d'un tel mouvement que Philip Zimmermann a élaboré en 1991 le logiciel PGP (*Pretty Good Privacy*) pour la protection du courrier électronique et qu'il présente comme un outil au service des droits humains (*Human Rights Tool*). Reste à apprécier l'importance respective de ces nouveaux pouvoirs et contre-pouvoirs, ce qui sort des limites de notre propos.

Cet ouvrage tente de fournir les éléments qui permettent d'examiner plus avant le soupçon qu'une telle tension fait peser sur le mythe d'une science égalitaire et universelle. Si cette universalité appartient sans nul doute au registre des possibles, sa mise en œuvre effective dépend des conditions d'échange et de développement des pratiques scientifiques, qui relèvent elles-mêmes de pratiques sociales en partie contrôlées par les institutions. C'est sans doute à trop oublier cette dimension sociale que le Siècle des

[21] Le lecteur trouvera dans cet ouvrage de très nombreuses références à l'activité de la NSA depuis sa création en 1952. Voir les chapitres « Du message chiffré au système cryptographique » p. 143 et 146 ; « La cryptographie gouvernementale française » p. 163 ; « Pourquoi et comment la cryptologie a envahi le domaine public » p. 209, 214, 217 et 238 ; « Cryptographie et théorie des nombres » p. 277 ; et « La relation agitée entre mathématiques et cryptologie » p. 289, 293, 294, 298 et 302.

Lumières a misé sur la seule rationalité pour faire de tout humain un citoyen libre et autonome. Nous voudrions précisément contribuer à expliciter les conditions d'exercice de la science, à élaborer des outils d'analyse qui permettent aux acteurs sociaux de se pourvoir des moyens de s'approprier les enjeux de la connaissance scientifique, et acquérir ainsi le pouvoir de penser le réel autant que le possible.

BIBLIOGRAPHIE

Austin, J. L., *Quand dire, c'est faire,* Paris, Seuil, 1970.

Bacon, F., *Meditiationes sacrae* (1597), texte original latin, *in* (ed.) M.N. Bouillet, *Œuvres philosophiques de Bacon, avec notice, sommaires et éclaircissemens*, Paris, Hachette, 1834, tome 3.

Coumet E., « Cryptographie et numération », *Annales, Économies, Sociétés, Civisisations,* 1975, 30e année, n° 5, pp. 1007-1027.

Diffie, W. et Hellman M., « New Directions in Cryptology », *IEEE Transactions on Information Theory*, 1976, vol. 22, n° 6, pp. 644-654.

Katz, K. et Lindell, J., *Introduction to Modern Cryptography*, Boca Raton, Chapman et Hall / CRC Press, 2007.

Pestre, D., *Introduction aux 'Science Studies',* Paris, La Découverte, 2006.

Rashed, R., *Al-Khwārizmī, le commencement de l'algèbre,* Paris, Blanchard, 2007.

Ricœur, P., *La métaphore vive.* Paris, Seuil, 1985.

Stern, J., *La science du secret*, Paris, Odile Jacob, 1998.

Victorri, B., et Fuchs, C., *La polysémie, construction dynamique du sens*, Paris, Hermès, 1996.

L'ANCRAGE DE LA CRYPTOLOGIE DANS LES JEUX D'ECRITURE

Marie-José DURAND-RICHARD[1], Philippe GUILLOT[2]

L'histoire des deux versants de la cryptologie – la cryptographie et la cryptanalyse – est d'un abord d'autant plus délicat à étudier qu'elle concerne des pratiques longtemps tenues secrètes. Avant que la mécanisation du calcul et les théories mathématiques ne s'y investissent, les publications ont donc été rares, mal connues, et leur accès reste difficile. Qui plus est, comme pour toute discipline récente, les premiers auteurs à s'intéresser à son histoire en ont d'abord été les acteurs, observant la cryptologie de l'intérieur. Il leur est alors difficile d'embrasser l'ensemble des enjeux auxquels elle s'est trouvée historiquement confrontée. L'approche qui tend à analyser le passé en y recherchant les traces du présent, conduit à négliger bon nombre de facteurs contextuels qui ont accompagné les pratiques cryptologiques au cours de leur lent développement. Elle fait alors apparaître une histoire linéaire qui gomme les méandres de l'action et de la pensée.

Cette difficulté est particulièrement sensible pour ce qui est de la structuration de la cryptologie autour des mathématiques. Si cette discipline, aujourd'hui enseignée à l'université, fait désormais un vaste usage des structures algébriques et de la théorie des nombres, il est essentiel d'avoir conscience du fait que son contenu mathématique est récent. L'introduction des mathématiques en cryptologie a convergé avec le processus de mécanisation dès le début du 20^{e} siècle.

De fait, la raison majeure pour laquelle la cryptologie n'a pas investi plus tôt les mathématiques dépasse de très loin cette simple question de périodisation. Elle tient également au fait que la cryptologie s'est développée pendant de nombreux siècles dans un contexte bien différent. Avant de dégager les procédures qui aujourd'hui s'expriment mathématiquement, la

[1] mjdurand.richard@gmail.com. Chercheuse associée, Université Paris Diderot, Sorbonne Paris Cité, SPHERE, UMR 7219, CNRS, F-75205 Paris, France.
[2] philippe.guillot@univ-paris8.fr. Maître de conférences, LAGA, UMR7539, CNRS-Université Paris 8 Vincennes Saint-Denis.

cryptologie a d'abord mis en œuvre des pratiques instrumentales. Les moyens de dissimuler le sens d'un message sont initialement attachés à la matérialité des supports utilisés. Elle a rencontré à plusieurs reprises d'autres activités d'ordre linguistique comme la littérature ou la philologie. La théorisation de ces procédures est issue d'une lente convergence de plusieurs facteurs : la circulation et l'appropriation de ces moyens techniques, parallèles au développement des mathématiques elles-mêmes, et la rencontre entre cryptologues et mathématiciens.

L'objet de ce chapitre est précisément d'inscrire la cryptologie dans la pratique de ses acteurs, afin de mieux ressaisir l'ampleur et les implications de la mutation fondamentale qu'elle a connue en basculant progressivement du champ de l'analyse du langage à celui des mathématiques. Marqués du sceau du secret, pratiqués dans des milieux différents, procédés matériels et efforts de théorisation se développent souvent séparément sans forcément se transmettre ni se rejoindre, donnant lieu parfois à des réinventions. Après les premières dissimulations de messages dont témoignent les textes anciens, la cryptanalyse naît véritablement de l'étude des langues par les érudits arabes lors de leur travail d'assimilation des savoirs antérieurs, tant grecs que latins. Mais les traces manquent d'un héritage effectif de leurs procédés d'« extraction de l'obscur » vers l'Europe de la Renaissance. Il est clair cependant que les humanistes auront à cœur de rassembler à leur tour l'ensemble des procédés connus, au moment où les cours royales établiront les « cabinets noirs », officines spécialisées chargées d'intercepter les correspondances chiffrées et d'en tenter le décryptement. Un écart demeure cependant entre les pratiques de chiffrement dans les cercles proches du pouvoir, et les efforts de généralisation d'humanistes tels qu'Alberti, Trithème ou Vigenère. Si le chiffrement polyalphabétique de ce dernier marque l'aboutissement d'un certain nombre des pratiques matérielles que ces humanistes élaborent, il ne sera pas pour autant adopté par les praticiens du chiffrement, qui préféreront des procédés plus rudimentaires et plus automatiques. Certes, des mathématiciens commencent à intervenir dans ces cabinets noirs, mais ils restent le plus souvent isolés et sans héritage. C'est la mécanisation des procédés de chiffrement qui permettra d'explorer les potentialités du chiffrement polyalphabétique, et qui débouchera sur la mathématisation des méthodes qu'elle aura contribué à expliciter.

PREMIERES TRACES DE DISSIMULATION DU SENS DES MESSAGES

Des traces d'un changement volontaire de marques et de symboles écrits sont attestées dès la naissance de l'écriture. Elles apparaissent comme des variations sur le langage écrit, qui sera longtemps réservé à un groupe social restreint, et souvent empreint de certaines formes de sacralité associées au

savoir. L'écriture constitue donc d'elle-même un moyen de limiter la circulation des informations entre ceux qui la pratiquent. Il n'est donc pas certain que les premières transformations intentionnelles de l'écriture aient eu lieu à des fins supplémentaires de confidentialité. D'autres motivations symboliques peuvent s'y manifester.

Des hiéroglyphes inscrits sur la pierre tombale du nomarque Khnoumhotep II (XII[e] dynastie, vers 1900 avant notre ère) ont ainsi été volontairement transformés[3]. Il ne s'agissait vraisemblablement pas de la volonté de rendre inintelligible la description de sa vie, mais plutôt d'une variation sur l'écriture, dont la forme était alors loin d'être fixée. Par ce biais, le roi semble vouloir imposer ses règles jusqu'au-delà de la mort.

Quoi qu'il en soit, les écritures secrètes resteront longtemps une constante de la culture et de l'éducation des classes aisées, et ce dans des aires culturelles bien différentes[4]. Ainsi, le Kama-Sutra, recueil indien attribué à Vatsyana, écrit entre le 4[e] et le 7[e] siècle, est destiné à la bonne éducation des hommes et des courtisanes. Il est surtout connu pour ses descriptions des différentes façons d'honorer les relations charnelles, mais il énumère également les soixante-quatre arts que doivent connaître les personnes cultivées. Le quarante-cinquième est consacré aux puzzles de langage et à l'écriture secrète[5]. Dans un tout autre contexte, et à une toute autre époque, Charles Sorel (vers 1602-1674), romancier et érudit français, auteur de plusieurs romans et écrits sur la poésie, l'histoire et le droit, est en particulier l'auteur d'un ouvrage, *La Science Universelle*, écrit de 1644 à 1647, qu'il considérait comme un cours complet d'éducation. Le chapitre 7 du livre 4, « De l'écriture, de l'orthographe et des chiffres secrets », comprend une dizaine de pages consacrées aux manières secrètes d'écrire. L'auteur considère comme acquis que l'homme instruit doit être familier avec cet exercice.

La scytale lacédémonienne

La première trace d'un procédé de dissimulation intentionnelle du sens d'un message écrit afin de le rendre inintelligible lors d'une éventuelle interception est la scytale de Sparte. Le terme « scytale » désigne l'instrument lui-même : initialement, il s'agit du bâton que se transmettent

---

[3] Kahn, *The Code-breakers*, p. 72.

[4] De nombreux exemples en feront foi dans la suite de ce texte et de l'ouvrage.

[5] Kahn, *The Codebreakers*, p. 74 ; Vatsyayana, *Kamasutra*, London, Cosmopoli, 1883, p. 25 : « *The art of speaking by changing the forms of words. It is of various kinds. Some speak by changing the beginning and end of words, others by adding unnecessary letters between every syllable of a word, and so* ».

les coureurs lors d'une course de relais aux Jeux Olympiques, et dans ce cas précis, du bâton qui sert à brouiller l'écriture du message.

La référence à la scytale est présente dans des textes très anciens : Archiloque (7e siècle avant notre ère), Pindare (~518-~466), Aristophane (~455-~385), Thucydide (~460-~399)[6].

Elle y est toujours présentée comme un support de message écrit. Thucydide écrit ainsi : « On crut alors ne devoir plus dissimuler : les éphores[7] lui envoyèrent un héraut avec une scytale, s'il ne voulait pas que Sparte lui déclarât la guerre »[8]. Son utilisation explicite comme moyen de chiffrement est rapportée par les historiens antiques Plutarque (40-120), et Aulu Gelle (vers 120-180). Plutarque explique en détail son utilisation :

> « Quand un général part pour une expédition à terre ou en mer, les éphores prennent deux bâtons ronds, d'une longueur et d'une grandeur si parfaitement égales, qu'ils s'appliquent l'un à l'autre sans laisser entre eux le moindre vide. Ils gardent l'un de ces bâtons, et donnent l'autre au général ; ils appellent ces bâtons des scytales. Lorsqu'ils ont quelque secret important à faire passer au général, ils prennent une bande de parchemin, longue et étroite comme une courroie, la roulent autour de la scytale qu'ils ont gardée, sans y laisser le moindre intervalle, en sorte que la surface du bâton est entièrement couverte. Ils écrivent ce qu'ils veulent sur cette bande ainsi roulée, après quoi ils la déroulent, et l'envoient au général sans le bâton. Quand celui-ci la reçoit, il ne peut rien lire, parce que les mots, tous séparés et épars, ne forment aucune suite. Il prend donc la scytale qu'il a emportée, et roule autour la bande de parchemin, dont les différents tours, se trouvant alors réunis, remettent les mots dans l'ordre où ils ont été écrits, et présentent toute la suite de la lettre. On appelle cette lettre scytale, du nom même du bâton, comme ce qui est mesuré prend le nom de ce qui lui sert de mesure »[9].

Le grammairien romain Aulu Gelle (Aulus Gellus) précise le contexte d'utilisation de la scytale et donne une manière d'écrire le message qui conduit à casser le graphisme plutôt qu'à changer l'ordre des mots et des lettres :

> « Quand on avait à écrire au général quelque chose de secret, on roulait sur ce cylindre une bande de médiocre largeur et de longueur suffisante, en manière de spirale ; les anneaux de la bande, ainsi roulés, devaient être exactement appliqués et unis l'un à l'autre. Puis on traçait les caractères transversalement,

---

[6] Collard, *Les langages secrets dans l'antiquité gréco-romaine.*

[7] Les éphores sont des magistrats lacédémoniens, au nombre de cinq, établis pour contrebalancer l'autorité des rois et du sénat. Ils étaient élus par le peuple et renouvelés tous les ans.

[8] Thucydide, *Histoire grecque*, livre I, ch. 131.

[9] Plutarque, *Vie de Lysandre*, ch. XXIV.

> les lignes allant de haut en bas. La bande, ainsi chargée d'écriture, était enlevée du cylindre et envoyée au général au fait du stratagème ; après la séparation, elle n'offrait plus que des lettres tronquées et mutilées, des corps et des têtes de lettres, divisés et épars : aussi la dépêche pouvait tomber au pouvoir de l'ennemi sans qu'il lui fût possible d'en deviner le contenu »[10].

Ces deux témoignages décrivent l'utilisation de la scytale à des fins militaires et pour assurer la confidentialité de messages sensibles. Mais la nature du procédé employé diffère. Dans le texte de Plutarque, la scytale opère une transposition – c'est-à-dire un changement d'ordre – des lettres, alors que dans celui d'Aulu Gelle, le graphisme des lettres est lui-même rompu, celles-ci pouvant être inscrites sur des portions différentes de la lanière enroulée.

La première publication connue d'une cryptanalyse de la scytale est récente, et témoigne de la rareté des informations sur le sujet. La cryptologie fait l'objet d'un vif intérêt dans les journaux, qui se développe dans la première moitié du 19e siècle. L'écrivain américain Edgar A. Poe (1809-1849) en nourrit ses histoires à suspense. Il explique la cryptanalyse de la scytale dans l'une d'elles. L'objet et le titre de ce conte sont précisément la cryptographie :

> « Dans aucun des traités de Cryptographie venus à notre connaissance, nous n'avons rencontré, au sujet du chiffre de la scytale, aucune autre méthode de solution que celles qui peuvent également s'appliquer à tous les chiffres en général. On nous parle, il est vrai, de cas où les parchemins interceptés ont été réellement déchiffrés ; mais on a soin de nous dire que ce fut toujours accidentellement. Voici cependant une solution d'une certitude absolue. Une fois en possession de la bande de parchemin, on n'a qu'à faire faire un cône relativement d'une grande longueur – soit de six pieds de long – et dont la circonférence à la base soit au moins égale à la longueur de la bande. On enroulera ensuite cette bande sur le cône près de la base, bord contre bord, comme nous l'avons décrit plus haut ; puis, en ayant soin de maintenir toujours les bords contre les bords, et le parchemin bien serré sur le cône, on le laissera glisser vers le sommet. Il est impossible, qu'en suivant ce procédé, quelques-uns des mots, ou quelques-unes des syllabes et des lettres, qui doivent se rejoindre, ne se rencontrent pas au point du cône où son diamètre égale celui de la scytale sur laquelle le chiffre a été écrit. Et comme, en faisant parcourir à la bande toute la longueur du cône, on traverse tous les diamètres possibles, on ne peut manquer de réussir. Une fois que par ce

[10] Aulu Gelle, *Nuits attiques*, livre XVII, ch. 9.

> moyen on a établi d'une façon certaine la circonférence de la scytale, on en fait faire une sur cette mesure, et l'on y applique le parchemin »[11].

Mais la rareté des informations au sujet de la scytale induit souvent le doute et les débats. Il a été récemment mis en cause comme procédé de chiffrement par plusieurs historiens des langues anciennes ou de la cryptologie[12], arguant à ce sujet de ce qu'il est convenu d'appeler le « mythe de la scytale ». Thomas Kelly se fonde notamment sur la faiblesse du procédé en matière de camouflage pour considérer que la scytale n'était qu'un procédé pour le transport des messages. Mais Brigitte Collard, dans une étude historique de ces langages secrets de l'Antiquité, s'appuie sur les écrits de dix-huit auteurs de cette période pour conclure au contraire : « Nous sommes convaincue que la scytale a été utilisée de façon cryptographique par les Spartiates, mais nous pensons que cet emploi s'est doublé d'autres usages qui ont pu endormir les esprits »[13].

Le chiffre de César

Le chiffre de César est l'exemple type d'un mode de chiffrement souvent présenté aujourd'hui sous forme mathématique, en se référant à un langage des permutations qui n'a pourtant commencé à se constituer en Europe qu'au 17e siècle[14]. À l'époque de César, il s'agit plus modestement d'un exemple de remplacement d'une lettre par une autre, par décalage de l'alphabet, ce qui sera qualifié plus tard de « chiffrement par substitution ». Il est mentionné par les historiens Suétone[15] et Aulu Gelle. Suetone écrit :

> « On possède enfin de César des lettres à Cicéron, et sa correspondance avec ses amis sur ses affaires domestiques. Il écrivait, pour les choses tout à fait secrètes, à travers des marques[16], c'est-à-dire un ordre arrangé de lettres de

---

[11] Poe, « La cryptographie », pp. 270-271.
[12] Jeffery, *The Local Scripts of Archaic Greece*, et Kelly, *The Myth of the Scytale*.
[13] Collard, *Les langages secrets dans l'antiquité gréco-romaine*, ch. I, § B-II 3.
[14] Ce langage des permutations fait notamment l'objet des travaux du père Marin Mersenne (1588-1648), la « boîte aux lettres de l'Europe savante », explorant les multiples potentialités de l'écriture humaine, à la recherche de toutes les façons possibles de combiner des mots ou des notes de musique. Cette exploration, alors dépourvue de toute notation spécifique, nourrira l'élaboration du calcul des probabilités à la fin du 17e siècle. Mersenne, *Harmonie universelle.*
[15] Suetone (Caius Suetonius Tranquillus, vers 70-vers 140) est un érudit romain qui vécut sous le règne de l'empereur Hadrien dont il fut le secrétaire. À cette époque où l'histoire est essentiellement hagiographique, il est connu pour avoir écrit les biographies des empereurs (*La vie des douze Césars*) et des écrivains (*Des hommes illustres*).
[16] Dans la plupart des traductions, le mot « nota » est traduit par « chiffre », et non par « marque », ce qui est un bel exemple d'anachronisme, et d'approche rétro-historique de la

> sorte qu'aucun mot ne pût être reconnu. Si on veut chercher et s'acharner jusqu'au bout, on change la quatrième lettre, c'est-à-dire un *D* à la place d'un *A* et pareillement pour toutes les autres »[17].

Ce procédé concerne à l'évidence des correspondances privées, traitant d'« affaires » particulières, alors que les textes décrivant la scytale placent clairement les messages échangés dans le contexte de campagnes militaires. De fait, César, lors d'une campagne militaire au cours du siège par les Nerviens – peuple de la Gaule belgique – du quartier d'hiver de Quintus Cicéron – frère cadet de l'orateur connu et légat de César –, utilise une autre technique qu'il décrit lui-même dans la guerre des Gaules. Parlant de lui à la troisième personne, il écrit **:** « Il décide alors un cavalier gaulois, en lui promettant de grandes récompenses, à porter une lettre à Cicéron. Il l'écrit en grec pour que, si elle est interceptée, l'ennemi ne connaisse pas nos plans »[18].

Ce procédé de César a eu une très longue postérité. Il deviendra le principe de base du chiffrement par simple substitution. Il aurait encore été utilisé[19] pendant la guerre de Sécession par des officiers sudistes, ainsi que par l'armée russe en 1915, avec un décalage différent. Un chiffrement de ce type subsiste encore aujourd'hui sous le nom de ROT13, un décalage de 13 positions dans l'alphabet, qui réalise un codage involutif[20]. Il sert à brouiller le texte dans le réseau Usenet (*netnews*), encore utilisé pour l'échange d'articles au sein d'une communauté. Il n'y a là aucun secret dans ce brouillage, qui ressemble plutôt à un argot d'Internet. Mais contrairement à la présentation qu'en font de nombreuses histoires de la cryptologie, au temps de César, ce procédé était bien loin d'être perçu comme une « transformation bijective modulo 26 »[21]. Il correspondait alors strictement à une simple manipulation de l'alphabet !

---

part des traducteurs. Le mot « chiffre » est d'origine arabe, et n'est apparu dans le langage qu'à partir du 8e siècle, et dans le langage de la cryptologie qu'à partir du 15e siècle.

[17] Suétone, *De vita duodecim Caesarum libri,* livre I, ch. LVI, § 8. Traduction Suzanne Fleixas.

[18] César, *Gaules,* V, XLVIII, 3-4, édition folio classique Gallimard, 1981, p 209. Le texte original précise « *graecis litteris* » laissant penser que le message est écrit, non pas en grec, mais en utilisant l'alphabet grec. Mais les Gaulois se servaient davantage de l'alphabet grec que de l'alphabet latin. La traduction de *Biblioteca Classica Selecta* disponible sur http://bcs.fltr.ucl.ac.be/caes/bgv.html est : « Alors il décide, à force de récompenses, un cavalier gaulois à lui porter une lettre : elle était écrite en caractères grecs, afin que les ennemis, s'ils l'interceptaient, ne puissent connaître nos projets ».

[19] Kahn, *The Codebreakers,* p. 216.

[20] Tel que le chiffrement soit identique au déchiffrement.

[21] À l'image de la page fr.wikipedia.org/wiki/Chiffrement_par_décalage.

LA CRYPTANALYSE ARABE

Selon Aulu Gelle, la première trace connue d'une cryptanalyse du chiffre de César provient du grammairien Valerius Probus de Berytus[22] (1er siècle de notre ère). Aulu Gelle écrit : « Il existe un mémoire assez curieux du grammairien Probus sur la signification des lettres cachées dans l'écriture de la correspondance de Caius César ». Ce texte ne nous est pas parvenu[23].

Mais la cryptanalyse en tant qu'activité organisée est véritablement née de la science arabe à partir des 8e et 9e siècles, dans un contexte où l'analyse des langues fait intégralement partie de l'activité des lettrés. Dès la phase de structuration de la civilisation arabo-musulmane, son rayonnement économique et culturel s'étend rapidement, de l'Espagne à l'ouest jusqu'à l'Afghanistan à l'est, et la langue arabe est un puissant vecteur d'échange et d'unification. La transcription écrite orthodoxe des différentes récitations dialectales du Coran, rapidement exigée par le calife Uthman vers 650, induit déjà un travail d'analyse et de codification de cette langue, qui marque le passage d'une transmission orale à une transmission écrite de la culture[24]. Au moment où l'organisation socio-politique se structure autour de ce nouveau monothéisme, la diffusion du Coran et des Hadith induit celle de la lecture et de l'écriture, soutenue par le développement de la fabrication du papier[25]. Mais cette diffusion de la langue va se trouver essentiellement portée par les besoins d'administration et de gestion de ce si vaste territoire. Dans les différentes régions administrées – « diwans » –, les « kuttab »[26] sont des lettrés, à la fois fonctionnaires, gestionnaires et écrivains publics qui maîtrisent aussi bien les questions de langue et d'écriture que de mathématiques.

De plus, la volonté d'assimilation des connaissances antérieures, soutenue par les fondements mêmes de la nouvelle religion[27], engage un énorme travail de traduction – essentiellement du grec, du syriaque, du persan et du sanskrit – et débouche sur l'écriture de nombreux traités

---

[22] L'actuelle ville de Beyrouth.

[23] Aulu Gelle, *Nuits attiques*, livre XVII, IX, ch. 9.

[24] Djebbar, *Une histoire de la science arabe*, pp. 21-66.

[25] La technologie du papier fut introduite dans le monde arabe à la suite de la bataille de Talas (Kirghizstan) en 751, qui marque à la fois la limite orientale de l'expansion arabe et la limite occidentale de l'expansion chinoise. Cette date coïncide avec l'avènement du règne des Abbassides. Au cours de cette bataille, des artisans papetiers chinois furent capturés, et la ville de Samarcande devint alors le premier centre de production de papier du monde musulman.

[26] Outre des qualités morales et sociales, le « kuttab » doit maîtriser l'arabe, l'histoire, l'arithmétique, et les sciences religieuses, selon les besoins de son travail. Rashed, *Entre arithmétique et algèbre*, pp. 1-29. Rashed, « Algèbre et linguistique ».

[27] Selon ces principes, la connaissance est un trésor de l'humanité toute entière et doit être recueillie et acceptée d'où qu'elle vienne.

d'analyse des langues : phonétique, morphologie, syntaxe, sémantique, lexicographie, grammaire, prosodie. L'arabe devient ainsi langue savante, assimilant d'anciens vocabulaires avant de produire de nouveaux termes. L'algèbre arabe est également née dans ce contexte d'études combinatoires, sous forme strictement littérale, avant d'être symbolisée dans l'Europe marchande des 16e et 17e siècles. On qualifie aujourd'hui de « science arabe » l'ensemble des textes de nature scientifique écrits dans cette langue, quelle que soit l'origine des lettrés qui les ont composés – chrétiens, juifs, païens, perses ou arabes.

Les éléments de base de la cryptanalyse arabe

Ces travaux d'ordre linguistique sur l'analyse des textes dessinent en quelque sorte les conditions de production de la cryptanalyse, lui fournissant des données, des règles et une méthodologie scientifique éprouvée. Les lettrés arabes assurent une vaste correspondance et se doivent de protéger celle qui concerne les affaires d'Etat. Ils effectuent très tôt des études phonétiques sur les consonnes et les voyelles, étudient la fréquence des lettres dans les textes, leurs combinaisons possibles et impossibles, procèdent à des études de syntaxe et de grammaire. Ils ont été parmi les premiers à produire des dictionnaires. C'est sur ces bases qu'ils inaugurent la cryptanalyse en élaborant pour la première fois une méthode systématique de comptage des lettres, qui correspond à ce qu'on appelle aujourd'hui « l'analyse des fréquences »[28]. L'utilisation de ce terme doit cependant rester prudente, dans la mesure où le mot « fréquence » doit être pris plutôt ici dans son sens courant, contraire de « rareté », sans renvoyer pour autant au vocabulaire des statistiques, qui ne se constitueront comme discipline que beaucoup plus tardivement, au 18e siècle, également dans un contexte étatique[29]. Cette méthode consiste à compter l'occurrence des lettres dans un texte de référence assez long écrit dans la langue, à lui comparer l'occurrence des lettres dans le texte chiffré analysé, et à identifier les lettres de même fréquence pour retrouver le message initial.

Le premier cryptologue arabe connu est le grammairien al-Khalil (vers 718-vers 791), auteur d'un ouvrage aujourd'hui perdu, *Le livre du langage secret* (*Kitab al mu'amma*). Dès cette époque, le monde arabe semble avoir utilisé des méthodes de chiffrement pour sa politique et son administration.

[28] Voir le chapitre « Sur l'extraction de l'obscur » p. 75.
[29] Brian, *La mesure de l'Etat.*

Le premier traité de la cryptologie arabe qui nous soit parvenu[30] est un ouvrage écrit par al-Kindi (801-873), philosophe, mathématicien et astronome auquel le calife al-Mamun confie la « Maison de la Sagesse » (*Bayt al Hikma*) à Bagdad, une sorte d'académie des sciences, avec bibliothèque et centre de recherche. Al-Kindi ne l'a écrit qu'à contrecœur, à la demande explicite d'Abu al-Abbas ar-Rasid, l'un des califes abbassides :

> « Cela n'était pas mon souhait et mon sens du devoir de t'aider à atteindre tout ce que tu exiges avec moins d'efforts – que Dieu facilite tes actions et t'accorde toujours l'éloquence ! J'aurais préféré suivre la voie des savants qui m'ont précédé et qui pensaient à obscurcir les trésors de la signification plutôt que de les afficher et de les révéler »[31].

Il donne d'abord les bases de ce qui doit être maîtrisé pour aborder la cryptanalyse, et définit les termes et notions qui seront au cœur de ses développements ultérieurs :
– obscurcissement (*at-ta'miya*) : ce terme désigne la conversion d'un message pour le rendre incompréhensible à ceux qui ne sont pas dans le secret de la méthode, et accessible à ceux qui le sont. L'arabe moderne utilise plutôt le mot *at'tashfir* pour désigner le chiffrement, terme dérivé de l'anglais *cipher* qui a donné « chiffre », et provenant lui-même de l'arabe *sifr* qui signifie « zéro »,
– traduction (*at-targjma*) : ce mot d'origine perse désigne la cryptographie et ses méthodes, mais il est parfois utilisé dans le sens de cryptanalyse,
– science pour extraire l'obscurité – aujourd'hui la cryptanalyse (*'ilmu istikhraj al-mu'mma*) : cette expression désigne le procédé par lequel un cryptogramme est converti en message clair par une personne qui est ignorante du procédé, ou de la clé utilisée pour le chiffrement.

Les auteurs arabes ont très tôt établi la notion de clé (*al-miftah*) qui est un ensemble de lettres, de nombres, ou même de versets poétiques, convenu entre les correspondants, et qui permet au destinataire de retrouver sans difficulté le message clair à partir du cryptogramme.

Le chapitre spécifique sur la cryptanalyse (*subul assinbati al mu'mma*, méthodes pour extraire l'obscurité), décrit les principes qui seront mis en œuvre pendant toute la période traditionnelle de la cryptologie. Al-Kindi distingue :
– les méthodes quantitatives (*al kamiya*) qui consistent à compter les occurrences des lettres dans le texte, mais également des digrammes

---

[30] Mrayati et *al., Al-Kindi's Treatise on Cryptanalysis,* p. 12. Les traductions en français des citations de cet ouvrage bilingue arabe-anglais ont été assurées par Abderrahman Daif et Kaltoum Tantaoui à partir du texte arabe. Voir le chapitre « Sur l'extraction de l'obscur » p. 63.
[31] Al-Kindi, chapitre « Sur l'extraction de l'obscur » p. 64.

(groupements de deux lettres) ou des trigrammes (groupements de trois lettres),
– et les méthodes qualitatives (*al kaïfiya*), qui travaillent sur la langue du texte. Elles s'appuient sur la connaissance des lettres qui s'associent et qui ne s'associent pas, des combinaisons possibles et impossibles de lettres, des idiomes de la langue. Les mots probables, les formules convenues, les titres, permettent de deviner le sujet du texte. Cette analyse s'appuie sur une intuition informée par l'expérience, le bagage linguistique, et une étude minutieuse. Elle commence par la recherche des mots courts.

L'analyse des fréquences est très clairement décrite dans le traité d'al-Kindi, qui contient en particulier la première table de fréquences connue pour une langue à alphabet[32]. Cette table porte à l'évidence sur le comptage des lettres et ne se réfère à aucun autre outil mathématique plus élaboré. Elle est établie à partir d'un texte dont al-Kindi prescrit qu'il doit être suffisamment long pour que ce comptage ait un sens, et ne peut être utilisée que pour décrypter un texte lui-même suffisamment long. Les analyses d'al-Kindi restent cependant très attachées à la pratique de l'écriture de la langue arabe. L'assimilation de ses résultats par les cryptologues européens ultérieurs passera par un long travail de transposition aux autres modes d'écriture.

Ces études sur la cryptanalyse ont été poursuivies par une succession d'auteurs :
– le poète du Caire ibn Adlan (1187-1268), auteur d'un manuel de cryptanalyse rédigé à la demande du roi de Damas, al-'Asraf[33],
– ibn Dunaynir (1187-1229), qui inaugure une méthode de chiffrement numérique[34],
– ibn ad-Durayhim (1312-1361), émissaire du sultan en Egypte, puis en Abyssinie, dont le *Trésor pour clarifier les chiffres* (*Miftah al-Kunuz fi Idah al-Marmuz*), récemment redécouvert et publié, est l'ouvrage le plus complet qui nous soit parvenu sur le sujet[35],
– et al Qalqashandi, le plus connu, dont l'encyclopédie de 1412, en 14 volumes, *Subh al-A'sha*, comporte une section sur la cryptologie[36], directement inspirée d'al-Durayhim.

Mais ces travaux, protégés par le secret, sont restés sous forme de manuscrits et ont été négligés par l'histoire. Les plus anciens n'ont été redécouverts que très récemment, et publiés en édition bilingue arabe-anglais.

---

[32] Mrayati et *al.*, *Al-Kindi's Treatise.,* p. 169 et chapitre « Sur l'extraction de l'obscur » p. 76.
[33] Mrayati et *al.*, *Ibn 'Adlan's Treatise al-mu'allaf lil-malik al-« Asraf.*
[34] Mrayati et *al.*, *Ibn Dunaynir's Book : Expositive Chapters on Cryptanalysis.*
[35] Mrayati et *al.*, *Ibn ad-Durayhim's Treatise on Cryptanalysis.*
[36] Al-Kahi, « Origins of Cryptology : the Arab Contributions ».

Ibn Dunaynir : إبن الدنينير

الفصل 26

أما الترجمة بقصد تعميتها بقسم من أقسام المركب، وهو أن تعمد إلى العدد الموضوع بإزاء حرفٍ من الحروف فتضاعفه مرة أو مرتين أو أكثر من ذلك، فإن ذلك يخفي عمن يقصده .مثال ذلك إذا أردت أن تكتب "الله ولي التوفيق":

ب س س ي يب س ك ب س ض يب قس ك ر

فوضعنا "ب" وهي اثنان في حساب الجُمّل وهي ضعف الألف، والسين ستين في حساب الجُمّل وهي ضعف اللام، وكذلك الباقي وغيره من التضاعيف، فانظر ما أحسن هذه اللطيفة.

Chapitre 26 :

Pour la transcription, dans le but d'obscurcir [le texte] à partir d'une des méthodes composées, avoir recours au nombre correspondant à la lettre et le doubler une fois ou deux ou plusieurs fois, ce qui dissimulera le sens à la personne qui le lit. En voici un exemple : « الله ولي التوفيق » (Dieu qui accorde le succès) :

ب س س ي يب س ك ب س ض يب قس ك ر

On a mis « ب », dont la valeur numérale est « deux », et qui est le double de la valeur numérale de « ا », et « س » dont la valeur numérale est soixante et qui est le double de la valeur numérale de « ل ». De même pour le reste. Alors admire cette jolie méthode[37].

Note : En arabe, la « valeur numérale » d'une lettre est un nombre qui lui est attribué selon un codage préétabli et reconnu de tous.
Voici l'explication de cet exemple :

lettre	ق	ي	ف	و	ت	ل	ا	ي	ل	و	ه	ل	ل	ا
valeur numérale	100	10	80	6	400	30	1	10	30	6	5	30	30	1
double	200	20	160	12	800	60	2	20	60	12	10	60	60	2
transcription	ر	ك	قس	يب	ض	س	ب	ك	س	يب	ي	س	س	ب

Fig. 1. Ibn Dunaynir, *Trésor pour clarifier les chiffres,* p. 127.

Il est néanmoins vraisemblable que, comme les travaux d'algèbre, ils aient pu être transmis en Europe au moment de la Renaissance. Un livre arabe sur les alphabets a notamment été publié en anglais par l'orientaliste John von Hammer en 1806, et étudié par le spécialiste de la langue arabe Sylvestre de Sacy en 1810, avant d'inspirer Champollion pour déchiffrer les

[37] Traduit par Abderrahman Daif, étudiant en master de cryptologie à l'Université Paris8-Vincennes-Saint-Denis, département de Mathématiques et d'Histoire des Sciences.

hiéroglyphes[38]. L'avancée des méthodes de ces auteurs arabes en cryptologie est indéniable, et leur caractère systématique leur confère une méthodologie tout à fait remarquable. Tout comme la naissance de l'algèbre arabe elle-même est fortement marquée par le contexte des études combinatoires, la cryptanalyse arabe naît et se structure dans le contexte des études sur l'analyse des structures langagières.

Un exemple littéraire de cryptanalyse chez Edgar Poe

L'analyse de la scytale lacédémonienne n'est pas la seule incursion d'Edgar Poe du côté de la cryptologie. Il y fait de nombreuses références, et s'en nourrit pour attirer le public cultivé vers la littérature[39]. En 1843, il publie une nouvelle dans le *Philadelphia Dollar's Newspaper*, « The Golden Bug » (« Le scarabée d'or »), qu'il structure autour de la cryptanalyse[40], afin que les conditions rocambolesques de l'intrigue se résolvent rationnellement. L'intérêt ici du « Scarabée d'or » est que Poe y décrit très clairement les étapes du décryptement du chiffrement monoalphabétique[41], qui sont les mêmes que celles présentées par al-Kindi : le comptage des fréquences et l'analyse des combinaisons de lettres dans la langue du texte en clair. En fait, le décryptement de l'énigme suit presque mot pour mot un article de David A. Conradus, « Cryptographia Denudata », paru en 1842 dans le *Gentleman's Magazine*.

Une chasse au trésor repose sur un message secret :

```
53‡‡†305))6*;4826)4.)4‡);806*;48†8¶60))85;1‡(;:‡
*8†83(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:*‡(;4956*2(5*
4)8¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡1;48†85;4)485†
528806*81(‡9;48;(88;4(‡?34;48)4‡161;:188:‡?;
```

[38] Mrayati et *al.*, *Al-Kindi's Treatise on Cryptanalysis.*

[39] Voir note 11 p. 24. Edgar A. Poe a pu être initié à la cryptographie au cours de sa carrière militaire (1827-31), notamment lors de son séjour à l'académie militaire de West Point. Il s'est ensuite passionné par ce sujet qui conjugue, comme ses *Histoires extraordinaires*, mystère et rationalité.

[40] Il a déjà écrit sur le sujet dans le *Alexander's Weekly Express Messenger* dès 1839, où il invitait les lecteurs à lui envoyer des messages chiffrés en se proposant de les décrypter, ce qu'il a effectivement fait. Il y a notamment publié « A Few Words on Secret Writing ».

[41] En cette première moitié du 19e siècle, d'autres modes de chiffrement ont cependant déjà été produits, comme on le verra dans la suite de ce chapitre.

La première étape du décryptement est l'analyse des fréquences[42] :

Le caractère	8	se trouve	33	fois
"	;	"	26	"
"	4	"	19	"
"	‡ et)	"	16	"
"	*	"	13	"
"	5	"	12	"
"	6	"	11	"
"	† et 1	"	8	"
"	0	"	6	"
"	9 et 2	"	5	"
"	: et 3	"	4	"
"	?	"	3	"
"	¶	"	2	"
"	- et .	"	1	"

L'étude des mots probables, des combinaisons possibles et impossibles, est l'objet d'un long développement, illustré par le début du décryptement :

> « Donc 8 représentera *e*. Maintenant, de tous les mots de la langue, '*the*' est le plus utilisé ; conséquemment, il nous faut voir si nous ne trouverons pas répétée plusieurs fois la même combinaison de trois caractères, ce 8 étant le dernier des trois. Si nous trouvons des répétitions de ce genre, elles représenteront très probablement le mot '*the*' »[43].

La suite de la nouvelle poursuit la description détaillée du décryptement par l'analyse des mots et des combinaisons les plus probables, en utilisant les particularités de la langue anglaise. Le message clair, qui révèle l'emplacement d'un trésor, est finalement :

> « *A good glass in the bishop's hotel in the devil's seat forty-one degrees and thirteen minutes north-east side shoot from the left eye of the death's-head a bee-line from the tree through the shot fifty feet out* »[44].

[42] Poe, « Le Scarabée d'or », p. 157.
[43] *ibid.*, p. 158.
[44] « Un bon verre dans l'hôtel de l'évêque dans la chaise du diable quarante et un degrés et treize minutes nord-est quart de nord principale tige septième branche côté est lâchez de l'œil gauche de la tête de mort une ligne d'abeille de l'arbre à travers la balle cinquante pieds au large » *ibid.*, p. 162.

Edgar Poe conclut cet exercice en affirmant que ces substitutions simples sont faciles à décrypter : « Je vous en ai dit assez pour vous convaincre que des chiffres de cette nature sont faciles à résoudre »[45]. C'est sans doute la raison pour laquelle, après avoir lancé plusieurs défis de décrypter tous les messages chiffrés qu'on lui enverrait, il publie un essai dans le *Graham Magazine* en 1841, où il affirme :

> « Peu de personnes peuvent être amenées à croire que ce n'est pas chose tout à fait aisée d'inventer une méthode d'écriture secrète qui puisse déjouer toute recherche. On peut cependant affirmer rondement que l'intelligence humaine ne peut concocter un chiffrement que l'intelligence humaine ne puisse résoudre »[46].

Humour, dispersion ou échec : Edgar Poe publiera cependant deux nouveaux cryptogrammes relevant cette fois d'un chiffrement polyalphabétique, envoyés par un hypothétique Mr Tyler, et qu'il ne décryptera pas[47].

Le chiffre monoalphabétique comme celui de César est donc une méthode fragile. Mais cette incursion du côté de la littérature nous entraîne vers une analyse des méthodes qui ne correspond pas à la chronologie. De César à la Renaissance, et en dépit des avancées de la cryptologie chez les lettrés arabes, les praticiens du chiffre ne sont généralement pas des lettrés. Dans ces conditions, les méthodes employées doivent être élémentaires et faciles à mettre en œuvre sans se tromper. C'est la raison pour laquelle il ne s'agira pas immédiatement pour les cryptographes de produire des méthodes théoriquement plus solides, mais de développer une technicité qui permette d'inscrire la méthode dans le geste, et ainsi de la mémoriser plus facilement.

PERCEE DE LA CRYPTOLOGIE OCCIDENTALE A LA RENAISSANCE

Au cours du Moyen-Âge, l'Europe est dans un état de développement économique et culturel moins avancé que la civilisation arabo-musulmane. Les guerres qui s'y déroulent, en particulier les Croisades, ne manquent cependant pas de mobiliser le recours aux échanges secrets. Mais les transformations d'écriture utilisées alors ne concernent pas toujours

---

[45] *ibid.*, p. 161-162.

[46] Poe, « A Few Words on Cryptography » : *« Few persons can be made to believe that it is not quite an easy thing to invent a method of secret writing which shall baffle investigation. Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve* ».

[47] Les récentes études sur le sujet ont conduit à penser qu'Edgar Poe et Mr Tyler ne font qu'un. Rosemheim, *The Cryptographic Imagination.*

strictement le remplacement d'une lettre par une autre. Elles peuvent faire intervenir d'autres systèmes de signes, dont la dimension symbolique n'est pas exclue. L' « alphabet des Templiers » en est un exemple notable. L'ordre du Temple est cet ordre religieux et militaire issu de la chevalerie chrétienne au Moyen-Âge, créé en 1129 à partir d'une milice, les *Pauvres Chevaliers du Christ et du Temple de Salomé*, qui a œuvré pendant les 12e et 13e siècles à la protection des pèlerins qui se rendaient à Jérusalem. Il a constitué dans toute l'Europe un réseau de « commanderies », à la fois monastères et places fortes, drainant une immense fortune issue de leur production agricole et du dépôt des pèlerins[48].

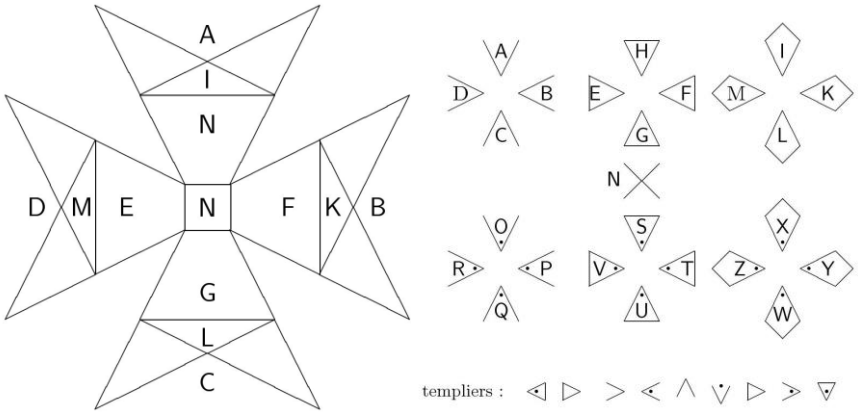


Fig. 2. Le code des Templiers (13e siècle). Illustration P. Guillot.

Les Templiers utilisaient un code pour protéger les lettres de crédit qui circulaient entre leurs neuf mille commanderies. Le codage de l'alphabet reposait sur la croix des huit béatitudes, qui était l'emblème de l'ordre. À chaque lettre est substitué le graphisme de sa position dans la croix. L'utilisation de ce code, avec sa référence à cet emblème, suffisait, semble-t-il, à assurer la confiance sur l'origine des missives[49].

Vers une cryptologie d'Etat : les cabinets noirs

Dès la fin du Moyen-Âge et le Quattrocento italien, le dynamisme européen se manifeste autour des nouveaux centres de pouvoir que sont d'abord les grandes cités italiennes – Florence, Milan, Venise, la Curie

[48] L'ordre a été dissout par le pape Clément V le 13 mars 1312 après l'arrestation de tous ses membres par Philippe le Bel et un procès en hérésie.
[49] Hébrard, *La cryptanalyse dans l'histoire,* p. 41.

romaine – et les cours royales ou princières. Dans le climat instable de cette période, marquée par la naissance de nouveaux pouvoirs, la protection des correspondances acquiert une importance capitale. Les échanges diplomatiques sont officialisés par la création d'ambassadeurs permanents. En 1495, les Sforza, ducs de Milan, disposaient déjà d'un service du chiffre bien développé, et Louis XII s'en est vraisemblablement inspiré, lors de son expédition en Italie, pour introduire l'usage du chiffre à la cour de France. François 1er (1494-1547) crée la fonction officielle de secrétaire-chiffreur en 1546, chargé de protéger et d'espionner les correspondances. Il en confie la charge à Philibert Babou (vers 1484-1557), sieur du château de la Bourdaisière près de Tours. Dans chaque centre de pouvoir s'organise ainsi, autour de cette nouvelle fonction, un service professionnel du chiffre souvent qualifié de « cabinet noir », et qui peut mobiliser un personnel assez important d'exécutants peu instruits. On peut citer par exemple le service du chiffre créé par Francis Walsingham (vers 1532-90), premier ministre de la reine Elizabeth I (1533-1603) : c'est grâce à son cryptanalyste polyglotte Thomas Phelippes (1556-1625), « maître en analyse des fréquences », que la trahison de Marie Stuart (1542-87) put être établie[50], et celle-ci condamnée à mort le 15 octobre 1586. Ces services sont parfois dirigés par des mathématiciens reconnus : François Viète (1540-1603) au service de Henri IV (1553-1610) depuis les guerres de religion, John Wallis (1616-1703) responsable du service du chiffrement du Parlement et de la Cour Royale anglaise. Leur savoir mathématique est avant tout investi en cryptanalyse.

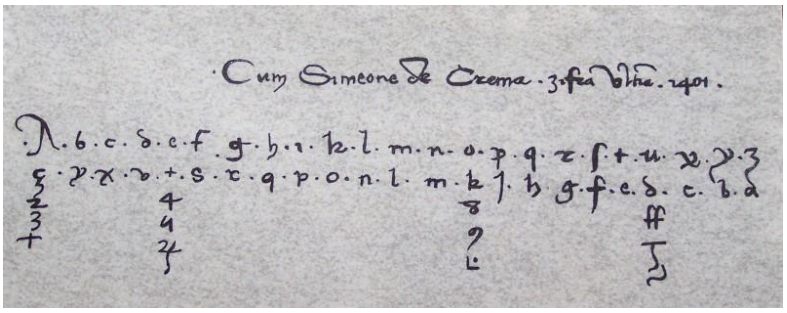


Fig. 3. Chiffrement homophone de Simeone de Crema. Kahn, p. 107.

Pour ce qui est de la cryptographie, le souci est alors de chiffrer le plus rapidement possible une correspondance très abondante qui circule à travers toute l'Europe, et de résister à une possible analyse des fréquences. Pour ce

[50] Singh, *Histoire des codes secrets*, ch. 1.

faire, un système de substitution à représentation multiple a d'abord été élaboré : le chiffrement homophonique. Il consiste à coder les lettres les plus fréquentes comme le *e* ou le *a*, de plusieurs façons différentes, en alternant au hasard le choix du codage. En contrepartie, les lettres qui peuvent, sans inconvénient pour la compréhension, être remplacées par une autre, comme le *j* par un *i* ou le *v* par un *u*, sont supprimées. Le premier alphabet homophone occidental connu date de 1401. Il fut utilisé dans le duché italien de Mantoue pour correspondre avec Simeone de Crema[51].

Face à la double préoccupation de chiffrer rapidement et de résister aux attaques, le chiffrement homophonique est complété par des langages conventionnels, rassemblés dans des « nomenclateurs », où un répertoire de mots courants est associé à des substitutions de lettres[52]. Le premier rôle du secrétaire-chiffreur est de réaliser de tels nomenclateurs, qui resteront l'outil majeur de la cryptographie jusqu'au milieu du 18e siècle.

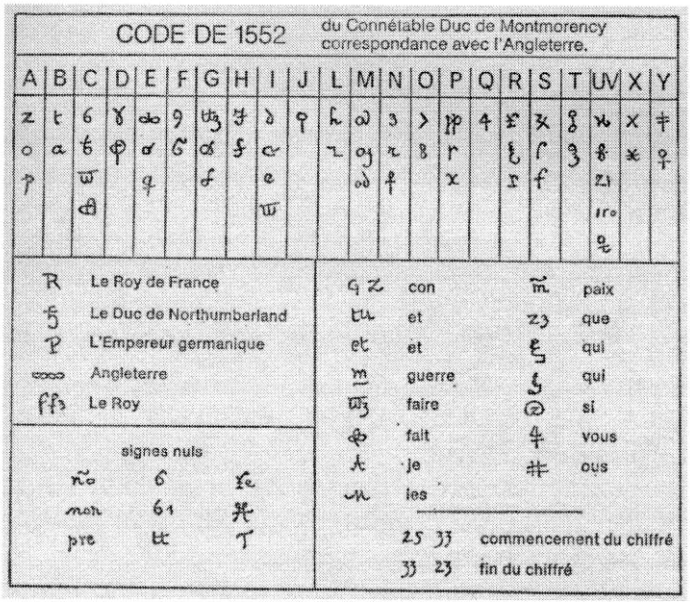


Fig. 4. Code du duc de Montmorency de 1552, Lerville, *in* Hébrard p. 61.

Le code de 1552, utilisé par le connétable duc de Montmorency, comportait ainsi quatre alphabets – chaque lettre pouvant être indifféremment codée de quatre façons différentes – et des symboles nuls

[51] Kahn, *The Codebreakers*, p. 107.
[52] C'est pourquoi ils sont également qualifiés de « systèmes à répertoires ».

qui ne désignaient rien, auxquels s'ajoutait la représentation par un signe de noms particuliers[53]. Le plus connu est le « Grand Chiffre du Roi » Louis XIV (1638-1715), établi par Antoine Rossignol (1600-1682), qui comportait un répertoire de 587 entrées, dont beaucoup représentaient des syllabes[54]. Il existait aussi un « Petit Chiffre du Roi » de 265 entrées pour les échelons subalternes. Le dernier nomenclateur établi en France l'a été dans les années 1970 par André Cattieuw, alors responsable des services centraux du chiffre[55]. Il comportait plus de cinquante mille entrées. La mécanisation du chiffrement a définitivement rendus obsolètes ces nomenclateurs.

Pendant cette même période, parallèlement à cet usage professionnel, des traités de cryptologie sont publiés par des humanistes de la Renaissance soucieux de rassembler les connaissances dans tous les domaines. Ces publications apportent des innovations successives qui vont conduire à l'élaboration d'un chiffrement polyalphabétique beaucoup plus sûr. Son usage tardera néanmoins à s'imposer du fait d'une mise en œuvre assez délicate.

L'élaboration du chiffrement polyalphabétique

Comme son nom l'indique, le chiffre polyalphabétique mobilise plusieurs substitutions alphabétiques. Un même symbole du message clair peut être représenté différemment dans le cryptogramme. Le travail du cryptanalyse se trouve donc ainsi compliqué, puisque le choix de l'alphabet de substitution varie au cours du message, ce qui casse la fréquence des lettres dans le cryptogramme.

Ce chiffrement est d'une solidité considérable. Longtemps considéré comme indécryptable, il ne sera résolu qu'au 19e siècle et inspirera les procédés modernes. Il faudra cependant attendre près de 400 ans, et la mécanisation du chiffrement, pour que son utilisation se généralise. Dans la pratique, sa mise en œuvre par des opérateurs humains se heurte en effet à des difficultés rédhibitoires : sensibilité aux erreurs de chiffrement et lenteur du travail. En 1716, l'ancien ambassadeur de Louis XIV François de Callières (1645-1717), dans un manuel devenu classique chez les

---

[53] Un procédé similaire a encore été utilisé par l'armée mexicaine jusqu'à la Première Guerre Mondiale, faisant intervenir cette fois un chiffrement numérique. Chacune des 25 lettres les plus courantes pouvait être codée de quatre façons possibles en un nombre entre 0 et 99. Kahn, *The Codebreakers*, p. 322.

[54] Il est tombé en désuétude après la mort du petit-fils d'Antoine, les Rossignol n'ayant laissé aucune trace de son fonctionnement. Il sera décrypté en 1893 par Etienne Bazeries (1846-1931), sollicité par un historien, après trois années de travail.

[55] Voir le chapitre « La cryptologie gouvernementale française » pp. 156 et 164.

diplomates, *De la manière de négocier avec les Souverains*, en soulignait ainsi les défauts, opposant théoriciens et praticiens du chiffrement :

> « On ne parle point de certains chiffres inventés par des régents de collège et faits sur des règles d'algèbre ou d'arithmétique, qui sont impraticables à cause de leur trop grande longueur et de leurs difficultés dans l'exécution, mais des chiffres communs dont se servent tous les négociateurs et dont on peut écrire une dépêche presque aussi vite qu'avec des lettres ordinaires »[56].

La mise au point du chiffrement polyalphabétique résulte pourtant d'une pratique instrumentale qui va se trouver progressivement améliorée et théorisée, avant qu'une synthèse n'en soit établie par le diplomate Blaise de Vigenère (1523-1596), qui lui a laissé son nom.

Le cadran d'Alberti et l'invention du polyalphabétisme

Tout comme Léonard de Vinci (1452-1519), l'architecte florentin Leon Battista Alberti (1404-72) est une des grandes figures humanistes de la Renaissance italienne. Organiste, poète, philosophe et compositeur, il est l'auteur de nombreux traités, dont le plus important marque la naissance du traitement géométrique de la perspective[57].

Il est initié aux problèmes cryptologiques par le secrétaire pontifical Leonardo Dato, qui compare le décryptement des lettres interceptées par les espions du Pape à celui des secrets de la nature. Son traité *De Componendis Cyphris* (1466) est le premier essai de cryptanalyse connu en Europe. Alberti y expose une méthode de décryptement de textes en langue latine, reposant sur l'analyse des fréquences, et en particulier sur la recherche des voyelles et des consonnes, puisque : « sans voyelle, il n'y a pas de syllabe ». Il utilise également les propriétés du latin, comme par exemple : « lorsqu'une consonne suit une voyelle à la fin d'un mot, celle-ci ne peut être qu'un *t*, un *s*, un *x* ou encore un *c* ».

Mais surtout, après avoir expliqué comment ces chiffrements peuvent être résolus, il propose une solution pour s'en prémunir, qu'il qualifie d'incassable : son cadran chiffrant. Son utilisation complexifie le décalage de César, qui peut ainsi changer à la guise du chiffreur.

> « Je découpe deux disques dans une plaque en cuivre. L'un, plus grand sera fixe, et l'autre plus petit, mobile. Le diamètre du disque fixe est supérieur d'un

[56] De Callières, *De la manière de négocier avec les Souverains*, pp. 320-326.

[57] Son traité de perspective est inséré dans le livre I – entièrement présenté de manière mathématique – de son traité de peinture, *De Pictura*, rédigé en 1435, et publié à Bâle en 1540. Golsenne et Prévost, *Leon Battista Alberti. La Peinture.*

neuvième à celui du disque mobile. Je divise la circonférence de chacun d'eux en 24 parties égales appelées secteurs. Dans chaque secteur, du grand disque, j'inscris en suivant l'ordre alphabétique normal une lettre majuscule rouge : d'abord *A*, ensuite *B*, puis *C*, *etc*. omettant *H*, *K* (et *Y*) qui ne sont pas indispensables »[58].

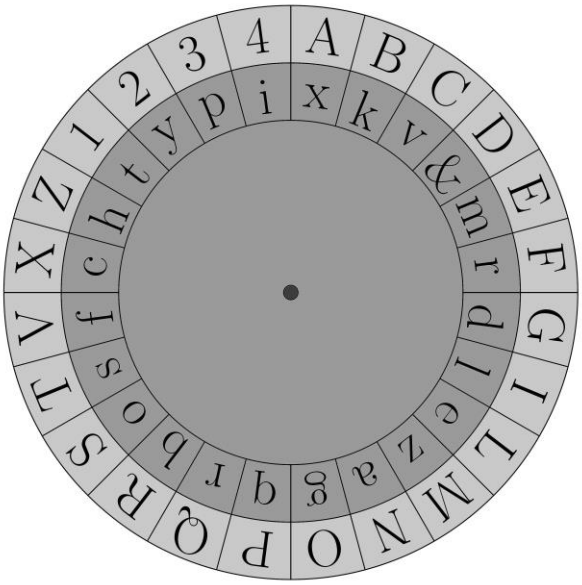


Fig. 5. Le disque d'Alberti. Illustration P. Guillot.
Exemple de cryptogramme : BqxboGqvgiMteRkomcoyvXilya

Le disque extérieur comporte donc 20 lettres, car *J*, *U* et *W* ne figurent pas dans cet alphabet. Et dans les quatre secteurs restants, Alberti inscrit les chiffres 1, 2, 3 et 4. Dans chacun des 24 secteurs du disque mobile, il place :

> « une lettre minuscule en noir, non pas dans un ordre normal comme pour le disque fixe, mais dans un ordre incohérent. […] Je place le petit disque sur le grand de façon qu'une aiguille passée dans les deux centres serve d'axe commun autour duquel tournera le disque mobile »[59].

Les lettres du disque fixe sont écrites en majuscules et représentent les lettres du message clair. Les lettres du disque mobile sont écrites en minuscules et représentent les lettres du cryptogramme.

[58] *ibid.*, pp. 705-725.
[59] *ibid.*, pp. 705-725.

L'expéditeur et le destinataire du message possèdent chacun un cadran identique. Ils conviennent d'un index repéré par une lettre sur le disque mobile, par exemple la lettre *k*. Dans le cryptogramme, la première des lettres écrites en majuscules, par exemple *B*, indiquera qu'il faut placer le *k* en face de cette lettre.

> « À partir de ce point de départ, chaque lettre du cryptogramme représentera la lettre fixée au-dessus d'elle. Après avoir écrit trois ou quatre lettres, je peux changer la position de l'indice de façon à ce que *k* soit par exemple sous le *D*. Donc dans mon message, j'écrirai un *D* majuscule, et à partir de ce point, *k* ne signifiera plus *B*, mais *D* et toutes les lettres du disque fixe auront de nouveaux équivalents »[60].

Les chiffres 1, 2, 3, 4 du disque fixe sont utilisés comme entrées dans un répertoire pour signifier des mots courants, comme dans un nomenclateur. Ainsi, la suite 341 peut signifier « Pape ».

Toute nouvelle position du disque conduit à un nouvel alphabet chiffrant, dans lequel le rapport entre les lettres du clair et les lettres du cryptogramme a changé. Il y a autant d'alphabets que de positions possibles du disque. Un même mot pourra donc être chiffré d'une certaine manière à un endroit du cryptogramme, et d'une autre manière un peu plus loin.

Le premier chiffre polyalphabétique était inventé. Toutefois, l'analyse des fréquences pouvait encore fonctionner sur certaines portions du chiffré, puisque le chiffre d'Alberti reste localement monoalphabétique. Le cryptanalyste pouvait ainsi exploiter les lettres doubles de certains mots, comme *Papa* (Pape), qui seront également des lettres doubles dans les portions du cryptogramme où le cadran n'a pas tourné. Les successeurs d'Alberti vont faire évoluer ce dispositif.

La Tabula Recta *de Jean Trithème (1462-1516)*

La deuxième étape dans le développement du chiffre polyalphabétique vient de l'abbé bénédictin allemand Johannes Heidenbert, né à Trittenheim[61]. Il est l'auteur du premier grand ouvrage de cryptologie connu en Europe *Polygraphiae Libri Sex* (1518), qui fait partie d'une réflexion plus générale sur les écritures littérales et numériques[62].

Le livre 5 contient sa contribution au chiffrement polyalphabétique : il le présente sous la forme systématique d'une table, la *Tabula Recta*. Le mode

---

[60] *ibid.*, pp. 705-725.

[61] Son nom de Jean Trithème vient du surnom *Tritemius* qu'il s'est donné pour se faire connaître lorsqu'il a fondé une société littéraire.

[62] Coumet, « Cryptographie et numération », pp. 1008-1009.

d'emploi que donne Trithème de ce tableau reste cependant élémentaire. Il propose de coder la première lettre du message avec le premier alphabet, la seconde lettre avec le second alphabet, *etc*. Ainsi, le message clair NUNC CAVEO VIRUM sera-t-il codé par HXPF GFBX DSCGW.

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w
b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a
c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b
d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c
e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d
f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e
g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f
h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g
i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h
k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i
l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k
m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l
n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m
o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n
p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o
q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p
r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q
s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r
t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s
u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t
x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u
y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x
z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y
w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z

La supériorité de ce mode de chiffrement sur celui d'Alberti est qu'il change d'alphabet à chaque lettre. De plus, l'ensemble de tous les alphabets possibles est utilisé avant d'être repris, ce qui brouille davantage les fréquences. Par contre, la régularité du procédé le rend extrêmement rigide, et lui fait perdre toute sécurité dès qu'il est connu.

Le recours à une clé de chiffrement.

Giovani Battista Belaso (1505-1553) est un auteur fort peu connu, issu d'une famille noble de Brescia, appartenait à l'entourage du Cardinal de Capri dont il était probablement le chiffreur. Rompant avec la régularité de la méthode de Trithème, il introduit une innovation majeure dans la cryptographie européenne[63] : le recours à une clé de chiffrement. Dans un petit fascicule, *La cifra del sig* (1553), il propose de chiffrer en choisissant

[63] Cette notion avait déjà été produite par les cryptologues arabes. Voir plus haut « La cryptanalyse arabe » dans ce chapitre.

les alphabets selon l'ordre des lettres d'un mot facilement mémorisable et facilement modifiable qu'il nomme le « *contresigne* ».

> « Ce contresigne peut consister en quelques mots d'Italien ou de Latin, ou de n'importe quelle autre langue, et les mots peuvent être en nombre réduit ou important comme on le veut. Ensuite, nous prenons les mots que l'on désire écrire, on les place sur le papier en ne les écrivant pas trop proches les uns des autres. Ensuite, au-dessus de chaque lettre, on place notre contresigne. Supposons par exemple que notre contresigne est le petit verset *virtuti omnia parent*[64]. Supposons également que nous voulions écrire ces mots *Lamarta Turchesca partira a cinque di Luglio*[65]. Nous allons le placer sur le papier ainsi :
>
> virtuti omniapare ntvirtu t iomnia pa rentvi
> lamarta turchesca partira a cinque di luglio »[66].

La lettre de la clé indique l'alphabet choisi pour chiffrer la lettre du clair. Ainsi, avec la *Tabula Recta* de Trithème, la lettre *l* du message de Belaso sera chiffrée avec l'alphabet *v* soit *f*, la lettre *a* sera chiffrée avec l'alphabet *i*, soit *i*, *etc*. D'où le chiffré :

FIDTMNI HGELHTCKA CTMCALU T LYWDDE SI CWTEDY

Grâce à son « contresigne », Belaso introduit dans le choix des alphabets une irrégularité, qui diversifie le procédé de chiffrement. La connaissance du procédé ne permet pas automatiquement le décryptement. Le secret dépend du contresigne.

La synthèse de Giambattista della Porta (1535-1615)

Dans la droite ligne des savants de la Renaissance, ce grand érudit napolitain s'intéresse à tous les aspects de la philosophie naturelle – de l'optique à l'alchimie –, sans négliger les sciences occultes dont il traite dans *Magia Naturalis*. Le soupçonnant de magie, le pape Paul III fit supprimer *l'Accademia secretorum* qu'il venait de créer. Son *De furtivis literarum notis* (1563), qui le fit reconnaître comme cryptologue, offre une synthèse des méthodes traditionnelles et de l'apport de ses prédécesseurs Alberti, Trithème et Belaso. Les lettres-clé – *litterae clavis* – associent des alphabets désordonnés – et non plus simplement décalés comme dans la *Tabula Recta* – pour coder les lettres écrites – *litterae scripti*. Il avance certaines remarques sur les conditions de sécurité données par la clé,

[64] « Tout cède à la vertu ».
[65] « L'armée turque se mettra en marche le cinq juillet ».
[66] Belaso, *La cifra del sig.*

conseillant par exemple d'utiliser des clés longues et de préférence dénuées de sens :

> « L'ordre des lettres (dans le tableau) […] peut être arrangé arbitrairement, à condition qu'aucune lettre ne soit omise […]. Plus elles seront éloignées de la connaissance commune, et plus grande sera la sécurité qu'elles apporteront à l'écriture »[67].

Outre cette synthèse entre l'alphabet désordonné d'Alberti, le système polyalphabétique de Trithème et l'utilisation d'un mot-clé par Belaso, della Porta donne la classification des méthodes de chiffrement toujours en vigueur aujourd'hui, distinguant la « transposition » – mélange des lettres du message clair – et la « substitution » – le remplacement d'une lettre par une autre. Il propose aussi une substitution digrammique, qui travaille cette fois sur des couples de lettres. La sienne utilise un alphabet de 400 symboles pour chiffrer tous les couples possibles des 20 lettres de l'alphabet latin. Della Porta fait également le point sur les méthodes de cryptanalyse, mettant l'accent sur l'étude des caractéristiques linguistiques et sur l'utilisation des mots probables, qui varient selon le type de correspondance à décrypter.

Dans cet ouvrage, della Porta exprime un souci manifeste d'organisation et d'extension des connaissances en cryptologie, qu'on retrouvera dans l'ouvrage plus connu de Blaise de Vigenère en France.

L'autoclave de Girolamo Cardano (1501-76)

Ce grand médecin italien[68] à la vie mouvementée – qui soigna la reine d'Angleterre et le pape Grégoire XIII – est davantage connu pour ses avancées dans le domaine des probabilités et pour sa contribution à l'introduction en algèbre des « quantités impossibles » – qui deviendront les « nombres complexes » trois siècles plus tard – que pour sa contribution à la cryptologie.

Dans ce domaine, il a inventé le mécanisme autoclave, ou auto-clé, qui utilise le message clair lui-même comme clé de chiffrement. La clé commence par répéter le premier mot du message clair. Le chiffrement du message *sic ergo elementis* s'effectue à partir de la disposition suivante, en utilisant la *Tabula Recta* de Trithème :

---

[67] Porta, *De furtivis literarum notis.*

[68] G. Cardano est l'auteur de la première autobiographie, composée en 1575-76, et publiée en 1646. Cardan, *Ma vie, autobiographie.*

Clé	s i c	s i c e	r g o e l e m e n
Clair	s i c	e r g o	e l e m e n t i s
Cryptogramme	l r e	y a i s	x r s q p r f n f

Mais la méthode de Cardan présente une ambiguïté : elle ne permet pas un déchiffrement unique, puisque le déchiffreur doit deviner le premier mot du message clair. La lettre *n* du cryptogramme peut être aussi bien un *s* chiffré avec la lettre *s* qu'un *f* chiffré avec la lettre *f*. Le déchiffreur se trouve donc exactement dans la même position que le cryptanalyste. C'est finalement Vigenère qui corrigera la formulation de Cardan pour conduire à un procédé d'une très grande sécurité.

Le chiffre indécryptable de Vigenère (1523-96)

C'est surtout grâce au *Traicté des chiffres, ou secrètes manières d'escrire* (1586), écrit en français[69], que sont connus les travaux de ses prédécesseurs. Diplomate érudit, Vigenère en synthétise les différentes avancées en une vaste fresque sur l'histoire des langages et de leurs secrets, dont la cryptologie n'est qu'un aspect. Fidèle serviteur de la maison de Nevers (1547-62), il est entré dans le secret des chiffreurs italiens au cours d'une mission diplomatique auprès de la Curie romaine (1549-51), et surtout, en tant que secrétaire d'ambassade à Rome (1566-70) au service de Charles IX (1550-1574). Il y rencontre notamment Belaso, tout en effectuant son « voyage d'Italie » – Florence, Venise, Turin –, alors classique dans la formation des hommes de lettres du 16e siècle[70].

Le *Traicté des chiffres* est tout à fait révélateur des questions qui préoccupent la Renaissance concernant le langage et les modes d'écriture[71]. Guerres de religion et grandes découvertes bousculent les représentations traditionnelles du monde tout autant que les avancées techniques – imprimerie, gouvernail d'étambot, boussole – avec l'intense brassage social et intellectuel qui accompagne ces bouleversements[72]. Si la culture reste réservée à une élite, elle fait l'objet de vastes remises en cause. La synthèse scolastique se trouve confrontée à un intérêt renouvelé pour d'autres

[69] C'est l'époque où les langues vernaculaires commencent à se substituer au latin pour l'écriture des ouvrages savants : Galilée écrit en italien et Descartes en français.
[70] À son retour d'Italie, alors que la France est secouée par les guerres de religion, Vigenère se retire de la vie publique pour se consacrer à l'étude et à l'écriture en tant qu'auteur d'ouvrages historiques, alchimiques ou philologiques, traducteur d'ouvrages antiques ou modernes, et théoricien des arts. Crescenzo, *Peintures d'instruction,* pp. 80-104.
[71] Coumet, « Cryptographie et numération », pp. 1010-1011.
[72] Morazé, *La science et les facteurs de l'inégalité,* pp. 81-94.

systèmes de pensée qui vont du platonisme à la Kabbale, en passant par l'alchimie et la magie[73]. Tous sont alors mobilisés pour déchiffrer les secrets de la nature. Le langage n'échappe pas à ce vaste questionnement sur la relation entre le signe et le sens, dont surgira de fait la rationalité scientifique propre au 17e siècle. Galilée en est un remarquable exemple lorsqu'il écrit que « *la Nature est écrite en langage mathématique* »[74].

Dans ce contexte, ce féru d'occultisme qu'est Vigenère est à la recherche du sens profond caché au profane. Il est convaincu que « toutes les choses de ce monde ne sont qu'un vray chiffre », et que toute écriture est porteuse d'un sens, aussi caché soit-il : « sous le chiffre est caché la vraye escriture et le sens qui nous représente la connaissance de la chose que nous voulons exprimer »[75]. La Kabbale le fascine tout autant que les mythes, dont il recherche une interprétation symbolique.

La synthèse que présente Vigenère dans ce traité est donc intégrée dans une réflexion générale sur les secrets de la nature. L'histoire des procédés de chiffrement relève des moyens qu'ont élaborés les érudits dans l'histoire pour les décrypter. À l'évidence, la pratique des écritures secrètes dépasse le seul cadre des activités militaires et diplomatiques de cette époque. Vigenère se livre à un travail de sécularisation de cette forme de savoir, tout en persistant à la réserver à la sagesse d'une élite :

> « L'escriture au surplus est double : la commune dont on use ordinairement ; et l'occulte secrète, qu'on desguise d'infinies sortes, chacun selon sa fantaisie, pour ne la rendre intelligible qu'entre soy et ses consçachans. Ce sont les chiffres, comme on les appelle d'un mot corrompu, aujourd'huy non appropriez à autres effects que pour les affaires du monde, et les negociations et practiques, aussi bien des particuliers que des Princes ; là où anciennement les Hébreux, Chaldéens, Egyptiens, Ethiopiens, Indiens, ne s'en servaient que pour voiler les sacrés secrets de leur Théologie, et Philosophie; […] Afin de les garantir et substraire du prophanement de la multitude, et en laisser la cognoissance aux gens dignes, […] pour autant qu'ainsi que parle le Philosophe Melisse […] '*Les yeux de l'âme du commun peuple, ne sauraient bonnement supporter les lumineux estincellemens de la divinité',* Ce traicté donques sera de semblables usages de chiffres, diversifiez en plusieurs manieres; tant pour incidemment parcourir ce qui se presentera à propos de ces beaux et cachez mysteres, adombrez sous l'escorce de l'escriture; que pour à l'imitation de cela en trasser beaucoup de rares, et à peu de gens divulguez artifices ; partie de nous apris et receuz des autres, voyageant ça et là en

[73] Febvre, *Le problème de l'incroyance au XVIe siècle.*
[74] Chauviré, *L'essayeur de Galilée,* p. 141.
[75] Vigenère, *Traicté des chiffres,* p. 53 v et p. 52 v.

divers endroits de l'Europe; et la plus grand'part provenans de nostre forge et méditation »[76].

Vigenère explique en détail la méthode de chiffrement qui utilise le mot-clé de Belaso et la *Tabula Recta* de Trithème. Son apport spécifique réside dans l'amélioration du système autoclave de Cardan par l'utilisation conjointe d'un mot-clé et du message clair pour constituer la clé de chiffrement. Au lieu de répéter le premier mot du clair comme le faisait Cardan, il choisit un contresigne convenu comme début de la clé de chiffrement. Et il envisage deux modes autoclaves : le mode autoclave sur le clair, qui prolonge le contresigne par le message clair, et le mode autoclave sur le cryptogramme, qui utilise comme clé le cryptogramme au fur et à mesure qu'il s'écrit. Par exemple, soit à chiffrer le message « au nom de l'éternel », en utilisant la table de Trithème de la page 41, avec comme contresigne la lettre *d* :

Autoclave sur le clair :

Clé	D	a	u	n	o	m	d	e	l	e	t	e	r	n	e
Clair	A	u	n	o	m	d	e	l	e	t	e	r	n	e	l
Cryptogramme	D	u	h	b	a	p	h	p	p	z	z	x	x	r	p

Autoclave sur le cryptogramme:

Clé	D	d	z	l	w	l	o	s	d	h	b	f	y	k	o
Clair	A	u	n	o	m	d	e	l	e	t	e	r	n	e	l
Cryptogramme	d	z	l	w	l	o	s	d	h	b	f	y	k	o	w

L'autoclave sur le cryptogramme présente l'avantage de fournir une clé incohérente, mais a l'inconvénient rédhibitoire de laisser la clé à la vue du cryptanalyste. Le système autoclave sur le clair est très sûr. Pourtant, il n'a pratiquement jamais été utilisé en raison de la grande complexité du déchiffrement, mais surtout de sa grande sensibilité aux erreurs : si une erreur survient au déchiffrement, tout le reste du message devient incompréhensible.

Le traité de Vigenère présente aussi un intérêt nouveau : il dégage un certain nombre de propriétés théoriques de l'opération de chiffrement, qui relèvent aujourd'hui de la théorie des permutations, même si leur expression reste difficile. Il se moque par exemple de la vanité du surchiffrement, qui consistait à chiffrer deux fois successivement un message, en montrant qu'il équivaut à un chiffrement unique[77] :

[76] *ibid.*, p. 3v.
[77] Autrement dit, la composée de deux permutations est une permutation.

> « Cependant ce n'était autre chose comme n'est aussi l'artifice duquel nous prétendons parler, sinon qu'un même sujet couvert de plusieurs chiffres réitérés les uns sur les autres […]. Mais je dirai bien davantage, car non que de trois enveloppes tant seulement, ainsi de cinquante, voire cent mille, et encore plus jusqu'en infini que cela s'étend, que puissent être réitérés ces surchiffrements, d'alphabet en alphabet les uns sur les autres, il n'importe de rien auquel de tous vous vous preniez pour le déchiffrer, étant en cela tous égaux, autant le dernier comme le premier ou second; parce que la disposition des lettres dont est issu le sens qui en résulte, ores qu'elle s'altère de figure, comme pourrait être un *a* pour un *d*, son ordre primitif ne se pervertit pas pour cela, que s'il y a deux mêmes lettres toutes de suite, vous n'en trouviez deux aussi qui s'entresuivront; si qu'il demeure toujours arrangé selon son premier établissement, et composition, et sa forme particulière renclose tacitement dedans soi, preste à s'en expliquer au dehors, tout ainsi que l'espèce de quelque oiseau dans un œuf; et d'un végétal en ses pépins, noyaux, greffes, ou semence, pour s'éclore, germer et poindre hors de leur puissance endormie, en une réveillée action de leur consemblable »[78].

Son langage laisse apparaître combien il est difficile d'exprimer ces propriétés en l'absence d'un vocabulaire spécifique et d'une description mathématique. D'autres textes de cette époque témoignent de cette même difficulté, par exemple les travaux de Mersenne sur les combinaisons[79], et permettent d'appréhender les différentes étapes du processus d'élaboration du savoir mathématique.

Ce qui est connu aujourd'hui sous le nom de chiffre de Vigenère est donc en fait le chiffre de Belaso avec une clé courte répétée. Ce procédé a résisté près de quatre cents ans à la cryptanalyse. S'il existe des exemples de décryptements réussis, ils s'appuient sur le fait qu'on est parvenu à deviner la clé, et non pas à la découvrir par une analyse du chiffré. Il faudra attendre la fin du 19e siècle pour voir une méthode systématique de décryptement, suite aux travaux de Charles Babbage (1791-1871) et de Friedrich W. Kasiski (1805-81). Pourtant, ce chiffre était toujours présenté comme indécryptable dans la revue *Scientific American*[80] en 1917.

Réinventions du chiffrement de Vigenère

Du fait de la faible diffusion des connaissances cryptographiques, la méthode de chiffrement polyalphabétique a été plusieurs fois réinventée, avec parfois quelques adaptations, y compris après qu'elle ait été résolue.

---

[78] Vigenère, *Traicté des chiffres,* pp. 222v-223r.
[79] Mersenne, *Harmonie universelle.*
[80] Kahn, *The Codebreakers,* p. 148.

Le chiffre de Grondsfeld a ainsi été produit par le comte du même nom, l'homme de guerre et diplomate belge José de Bronkchorst. Vers 1734, il a mis au point son propre système de chiffrement. Celui-ci améliorait le chiffre de César grâce à une clé numérique dont chaque chiffre indiquait le décalage à opérer successivement et cycliquement pour chiffrer le message clair. Ainsi, avec la clé 1734, la première lettre sera décalée d'un rang, la seconde de 7, la troisième de 3 et la quatrième de 4, après quoi le processus est répété. Le chiffre de Grondsfeld figure dans le roman de Jules Verne *La Jangada*[81]. L'auteur y décrit aussi le décryptement à partir d'un mot probable, retrouvant la clé grâce à la signature de l'auteur du cryptogramme.

Deux autres exemples sont contemporains du travail de Babbage. L'amiral anglais Sir Francis Beaufort (1774-1857), connu pour son échelle des vents, est également l'auteur du « chiffre de Beaufort »[82]. Ce chiffre est une variante très proche du chiffre de Vigenère : la méthode de chiffrement échange seulement l'ordre du choix entre la lettre de la clé et celle du chiffré dans la table des alphabets. En fait, et bien que ce chiffrement porte le nom de Beaufort, son origine est assez mystérieuse[83]. Il a seulement fait l'objet d'une publication posthume par son fils, et les manuscrits de Beaufort ne contiennent aucune trace de ce type de recherche. Par contre, Beaufort appartenait à un cercle de gentlemen cultivés qui, autour de Babbage, s'intéressaient de près à ces questions, en particulier au moment de la guerre de Crimée (1853-56). Babbage était alors considéré comme un expert en cryptologie, et en 1854, la *Society of Arts* lui envoya la demande de brevet de John H. B. Thwaites, dentiste à Bristol, convaincu d'avoir inventé une méthode de chiffrement tout à fait exceptionnelle, dont il vantait l'utilité dans les échanges commerciaux au moment de l'invention du télégraphe. En publiant sa méthode de décryptement dans le *Journal for the Society of Arts*, Babbage lui démontra qu'il se trompait[84] et que Thwaites n'avait en fait que réinventé le chiffre polyalphabétique de Vigenère.

Une autre adaptation du chiffre de Vigenère est également connue dans les cercles militaires sous le nom de « variante à l'allemande ». En outre, elle exprime numériquement le chiffre de Vigenère en termes d'un calcul modulaire : les lettres de l'alphabet étant représentées par des nombres de 0 à 25, pour chaque lettre, le nombre du chiffré est alors la différence entre celui du clair et celui de la clé. La procédure de chiffrement est alors identique à la procédure de déchiffrement.

---

[81] Verne, *La Jangada*, p. 25.

[82] Cette même méthode de chiffrement aurait déjà été produite par Jean Sestri vers 1710, voir. http://www.apprendre-en-ligne.net/crypto/vigenere/beaufort.html.

[83] Frankssen, « On the mystery of Admiral Beaufort's cypher ».

[84] Babbage, « Philosophy on Deciphering », folios 133-179. Voir le chapitre « Du message chiffré au système cryptographique » p. 115.

Ces variantes et adaptations du chiffrement de Vigenère, relativement tardives, se multiplient au 19e siècle, au moment où les conditions d'échange des messages se modifient considérablement avec la naissance de télégraphe. Quoi qu'il en soit, les méthodes de chiffrement restent attachées aux modifications des systèmes d'écriture, et s'améliorent relativement peu avant que les attaques cryptographiques ne résolvent le mode de chiffrement polyalphabétique.

L'EMERGENCE D'UNE METHODE ANALYTIQUE EN CRYPTANALYSE

L'évolution des méthodes cryptographiques témoigne des hésitations de leur développement, et surtout des difficultés à en raffiner les pratiques du fait du faible niveau de formation des acteurs. Les nomenclateurs résistent tout autant à la cryptanalyse que le chiffrement polyalphabétique. Et des méthodes de chiffrement ultérieures, utilisant des transpositions plus sophistiquées, se révéleront également très résistantes[85]. Mais le caractère artisanal du travail de chiffrement n'est qu'un des facteurs qui permet de comprendre la lenteur avec laquelle ces procédures ont été théorisées, et traduites mathématiquement. Le facteur principal n'est autre que l'inexistence à cette époque des théories mathématiques correspondantes, qui ne seront véritablement constituées qu'au début du 20e siècle[86].

Paradoxalement, la cryptanalyse a investi les mathématiques beaucoup plus tôt que la cryptographie. Sa naissance au cœur de la science arabe a déjà été signalée. Et au 17e siècle, à la tête des cabinets noirs, les secrétaires-chiffreurs en charge du travail de décryptement sont souvent des mathématiciens[87]. Au moment où s'unifient les ébauches de symbolisation de l'algèbre[88], ils ont plus systématiquement recours à des méthodes analytiques. Ces méthodes mobilisent davantage l'étude de la structure logique du langage que la recherche intuitive des mots probables et de la signification particulière du message dans un contexte donné.

Les difficultés de la cryptanalyse

Les savants du monde arabe, depuis les travaux d'al-Kindi, ont jeté les bases de la cryptanalyse pour ce qui est du chiffrement par substitution

---

[85] Voir le chapitre « Du message chiffré au système cryptographique » p. 109.
[86] Il s'agit essentiellement de la théorie des groupes, et plus généralement de la théorie des structures algébriques, qui réorganise le champ de l'algèbre dans les années 1930.
[87] François Viète (1540-1603) est le secrétaire-chiffreur de Henri IV, John Wallis (1616-1703) celui du Parlement pendant la guerre civile en Grande-Bretagne.
[88] Durand-Richard, « Calcul et signification ».

simple. Ils ont mis en place une méthode systématique reposant sur l'analyse des fréquences, et sur une recherche linguistique des combinaisons possibles et impossibles de lettres. Ces techniques apparaissent en Europe à la Renaissance[89] avec Porta, qui innove à son tour en introduisant la méthode du mot probable.

En dépit de ces méthodes, le décryptement reste un travail difficile et très laborieux, faisant davantage appel à l'habileté du cryptanalyste, à son acharnement, voire à sa chance, qu'à une quelconque méthode déductive. Vigenère, tout en saluant l'apport de Porta, y voit même une tâche inexhaustible et s'interroge sur la vanité de la recherche d'une méthode générale de décryptement :

> « Baptiste Porte Napolitain en un juste volume à part, intitulé *De furtiuis literarum notis*, où toutefois ce à quoi il insiste le plus, est d'enseigner les moyens de déchiffrer sans alphabet, exercice certes d'un inestimable rompement de cerveau, et en fait un travail tout inglorieux, joint qu'avec toutes les règles et maximes qu'on en peut donner, dont il y en a à la vérité qui y apportent beaucoup de lumière, il se trouvera à l'encontre assez de manières de chiffres du tout inexpugnables et invincibles, à qui n'en aura le secret »[90].

L'étude de l'histoire de la cryptanalyse reste délicate en raison de la rareté des documents rédigés ou publiés par les acteurs eux-mêmes. Rendre publique une méthode de cryptanalyse suppose d'annoncer que la méthode de chiffrement de l'adversaire est désormais connue, ce qui conduit à s'affaiblir soi-même, l'adversaire étant alors susceptible de pouvoir alors changer son procédé de chiffrement.

En dépit de ces difficultés et de ces doutes, la recherche de règles de décryptement fait de la cryptanalyse un domaine de recherche où s'investit le raisonnement déductif, et les mathématiciens versés dans la cryptanalyse vont y introduire des méthodes algébriques.

La méthode analytique de François Viète (1540-1603)

S'il est moins connu que René Descartes (1596-1650), Viète est un mathématicien important, le premier auteur en France à publier – mais en latin – une synthèse de la symbolisation de l'algèbre, la « logistique spécieuse », introduisant l'étude des propriétés des équations algébriques, notamment les relations entre leurs racines et leurs coefficients. De

[89] Si les preuves manquent pour affirmer que ces techniques ont été transmises du monde arabe en Europe à la Renaissance, cette transmission est néanmoins tout aussi vraisemblable que celle des méthodes de l'algèbre à cette même époque.
[90] Vigenère, *Traicté des Chiffres*, p. 12r.

formation juridique, il a été l'avocat des grandes familles protestantes, avant de devenir conseiller au Parlement de Rennes sous Charles IX, puis maître des requêtes ordinaires de l'Hôtel du Roi[91] sous Henri III. Il devient membre du Conseil du Roi et cryptanalyste attitré de Henri IV dès que celui-ci devient roi de Navarre en 1589. Il est sans doute l'auteur de nombreux codes utilisés à cette époque (code de Sully de 1599, code de Henri IV de 1604)[92]. Ces codes sont constitués de substitutions homophones, de lettres nulles et d'un répertoire pour coder des mots entiers, des expressions, des noms propres.

Du fait de sa confession protestante, le roi Henri IV luttait contre la Ligue catholique soutenue par le roi d'Espagne Philippe II. Viète réussit à décrypter plusieurs lettres interceptées, écrites par l'officier de la Ligue Juan de Moreo à Philippe II et à son ambassadeur en France. Ces lettres révélaient que le duc Charles de Mayenne guignait le trône de France et projetait de renverser Henri IV. Bien qu'il soit en général plus stratégique de dissimuler ce type de succès – afin de continuer à espionner la correspondance secrète –, Viète publia le contenu de la lettre de Moreno dès 1590, sans doute avec l'assentiment du roi. Celui-ci se dotait ainsi d'un avantage certain sur Philippe II et la Ligue catholique dans ses négociations pour conserver le trône de France, avantage dépassant de très loin l'affaiblissement stratégique induit par la révélation de Viète.

Philippe II fut d'ailleurs à ce point incrédule qu'il déposa une plainte en sorcellerie auprès du pape Clément VIII, accusant Viète d'avoir eu recours la magie. Clément VIII se garda bien de poursuivre, car ses services avaient déjà percé la correspondance du roi d'Espagne. La cryptanalyse était alors davantage un art qu'une science, et les cours d'Europe souvent convaincues de disposer des méthodes de chiffrement les plus sûres. Philippe II l'était à tel point qu'il ne changea pas son code.

Quelques temps avant sa mort en 1603, sans doute soucieux de transmettre ses méthodes[93], Viète laisse à Sully, Premier Ministre de Henri IV, une sorte de testament cryptologique où il donne davantage de détails sur ses méthodes et sur le contenu des messages décryptés qu'échangeaient l'Espagne et l'Italie pendant les guerres de la Ligue[94]. Dans ce mémoire aujourd'hui perdu[95], Viète revient sur sa publication de 1590

[91] Viète est tout à fait contemporain de Vigenère, mais contrairement à ce dernier, il effectue l'ensemble de sa carrière en France.
[92] Bien que Viète soit mort en 1603.
[93] La transmission des méthodes de cryptographie pose de sérieux problèmes pour cette discipline marquée du sceau du secret.
[94] Après ses premiers succès de décryptement, il eût à traiter une quantité de plus en plus importante de messages, jusqu'à plus d'une dizaine de liasses par mois.
[95] Une transcription de ce mémoire, réalisée au 19e siècle par un historien amateur, Frédéric Ritter, a néanmoins été récemment retrouvée à la Bibliothèque de l'Institut de France, et

avant de présenter une nouvelle méthode de cryptanalyse, à la fois analytique et systématique :

> « Je n'ai point caché la voie que j'ai tenue, mais j'en ai toujours ouvert la lumière à ceux qui se sont adressés à moi de la part du Roy. Et si ce service a profité ou non, nul ne le sait mieux que M. de Mayne auquel par le commandement de sa Majesté, plusieurs paquets furent faits voir afin qu'il connût la conspiration que ses partisans mêmes faisaient contre lui »[96].

La nouvelle méthode de Viète, qu'il estime « infaillible », repose sur l'assertion suivante :

REGLE INFAILLIBLE : *Parmi trois lettres consécutives, on trouve toujours une ou plusieurs des cinq voyelles* A, E, I, O *ou* U.

Cette propriété est en effet presque toujours satisfaite en espagnol. Elle l'est moins en français, mais encore suffisamment pour mener à bien un décryptement. Il est d'ailleurs vraisemblable que le choix de Viète en algèbre, de représenter les inconnues par des voyelles, lui ait été dicté par cette règle infaillible en cryptanalyse[97]. Il en explique la mise en œuvre sur un chiffrement monoalphabétique. Le premier travail est donc de rechercher les voyelles. Sur le cryptogramme suivant par exemple[98] :

```
t y e n l p y e n l q w q y f y k l m l q t
y h g m j w n k k y j m f o g g w g x y k y
w j y l k q a f y z j n f w g q k u q y l y
```

on examine les triplets successifs qui n'ont pas de lettre en commun : *tye*, *nlp*, *qwq*, *hgm*. On repère ainsi 11 lettres. Tous les autres triplets contiennent au moins une de ces 11 lettres. On en déduit que les 5 voyelles se trouvent parmi ces 11 lettres.

Le premier triplet qui fait intervenir deux autres lettres que les 11 précédentes est *fyk*. Il contient une voyelle qui n'est donc ni *f*, ni *k* ; ce qui conduit à conclure que *y* représente une voyelle.

Un raisonnement similaire permet d'identifier les 5 voyelles. Dans ce raisonnement, la signification du texte n'a pas été prise en compte. Il s'agit

---

analysée, par l'historien de la cryptologie Peter Pesic. Pesic, « François Viète, father of Modern Cryptanalysis ».

[96] Delahaye, « Viète, inventeur de la cryptanalyse mathématique », p. 91.

[97] Descartes remplacera cette convention par celle qui a été adoptée, de représenter les inconnues par les dernières lettres de l'alphabet : *x*, *y*, et *z*. Pesic, « Secrets, Symbols and Systems », pp. 684-685.

[98] Cet exemple est extrait de l'article de Jean-Paul Delahaye, « Viète, inventeur de la cryptanalyse mathématique ».

d'explorer les relations entre les symboles. Pour cette raison, la méthode de Viète a pu être qualifiée d'algébrique.

Une fois les voyelles déterminées, le bon sens, l'intuition et le « rompement de cerveau » interviennent à nouveau, faisant appel au contexte et au sens du message. À ce stade, Viète ne peut abandonner complètement le recours à la signification. Dans son mémoire de 1603, il utilise le terme « chiffres essentiels » pour désigner les nombres qui, en général, ne sont pas chiffrés dans un message, contrairement aux autres caractères. Ainsi, dans un message militaire, il est vraisemblable que « 4000 » soit suivi par le mot « fantassins », et « 50 » par le mot « cavaliers », alors que dans un message au contenu commercial, « 100 000 » désignera plus vraisemblablement des « ducats » (unité monétaire). Autour d'un nombre proche d'une année, on trouvera probablement le nom d'un mois, *etc*. La présence de ces nombres permet donc de présumer du terme qui suit.

Si méthode algébrique il y a, elle concerne bien plutôt les tentatives de décryptement par une classification systématique des problèmes rencontrés, qu'un quelconque recours à des modes de résolution d'équations, eux-mêmes en cours d'élaboration. Si des mathématiciens – et des algébristes surtout – sont souvent investis dans les cabinets noirs, le secret qui accompagne leur travail en fait une activité isolée et solitaire, difficile à diffuser et à transmettre. L'activité principale, celle du chiffrement, mobilise en plus grand nombre des exécutants auxiliaires peu instruits, employés à exécuter le chiffrement dans les meilleurs délais, et privilégiant de ce fait l'automatisation des procédés plutôt qu'une réflexion sur le chiffre. L'extension des méthodes cryptographiques passera précisément par l'extension de leur mécanisation, dont les mathématiques ne s'empareront qu'ultérieurement.

MECANISATION DES METHODES DE CHIFFREMENT

L'écart entre pratiques cryptographiques et élaboration de méthodes théoriques ou sophistiquées reste important jusqu'au 19e siècle. Il est lié aux difficultés matérielles auxquelles sont confrontés les chiffreurs : l'écriture des messages chiffrés doit être rapide et peu sensible aux erreurs, elle exige une grande concentration de la part de ces exécutants. C'est sans doute la raison majeure pour laquelle, en dépit de l'existence de la cryptographie polyalphabétique, les services de chiffrement vont persister longtemps à utiliser des méthodes plus traditionnelles manipulant des codes[99]. Cet écart

[99] Si le chiffrement polyalphabétique n'a pratiquement pas été utilisé dans les milieux professionnels, il l'a été par des acteurs individuels intéressés par la confidentialité de leurs

s'estompera au 19e siècle du fait des développements techniques issus de la révolution industrielle. La mécanisation des méthodes de chiffrement permettra de surmonter ces difficultés. Au moment où les guerres deviennent mondiales, elles s'appuient sur des moyens techniques plus considérables, qui du même coup décuplent la quantité des échanges secrets. En se complexifiant, cette mécanisation débouchera sur une très vaste diffusion du chiffrement polyalphabétique, qui reste notamment à la base du chiffrement de la machine *Enigma* pendant la Seconde Guerre Mondiale.

La grille de Fleissner

Parallèlement aux méthodes élaborées de chiffrement, des procédés sommaires, et cryptographiquement plus faibles, sont régulièrement utilisés, qui facilitent l'écriture des messages chiffrés. La grille de Cardan, utilisée dans les échanges diplomatiques au 16e et au 17e siècles, est une plaque de carton ou de métal, percée de trous dans lesquels est inscrit le message clair La grille enlevée, le texte est alors complété par des lettres, avec parfois le souci de donner un sens au texte final[100]. Ce procédé relève davantage de la stéganographie que du chiffrement[101].

La grille de Fleissner[102] repose sur le même principe. Elle porte le nom du colonel autrichien Edouard Fleissner von Wostrovitz (1825-88), qui l'a

---

échanges. En témoigne par exemple la correspondance de la reine Marie-Antoinette et d'Axel von Fersen après l'échec de la fuite à Varennes des 20 et 21 juin 1991. Voir Patarin et Nachef, « "I Shall Love You Until Death" ». En témoignent également les jeux cryptographiques entre Charles Babbage et son neveu. Voir chapitre « Du message chiffré au système cryptographique » p. 109.

[100] Ce souci est une constante des échanges chiffrés. L'*Ave Maria* de Trithème donne ainsi une méthode de dissimulation qui consiste à remplacer chaque lettre du message clair par un verset, afin de composer un message qui ait un semblant de sens, évitant ainsi que l'intercepteur potentiel ne s'aperçoive d'emblée du caractère chiffré du message.

[101] La stéganographie est un procédé qui consiste à dissimuler un message plutôt qu'à le modifier. David Kahn cite par exemple ce message, transmis par un espion allemand pendant le premier conflit mondial : « *President's embargo ruling should have immediate notice, grave situation affecting international laws. Statement fore-shadows ruin of many neutral. Yellow journals unifying national excitement immensely* ». Le véritable message transmis est obtenu en sélectionnant la première de chaque mot : « *Pershing sails from NY june I* ». Un second message, confirmant le précédent porte en lui la même information cachée : « *Apparently neutral's protests is thoroughly discounted and ignored. Ismam hard hit. Blockade issues affects pretext for embargo on by-product, ejecting suets and vegetable oils* ». Cette fois, c'est la seconde lettre de chaque mot qu'il faut considérer. Kahn, *The Codebreakers*, p. 521. Contrairement à ce que semble avoir appris notre espion, le général Pershing, commandant le corps expéditionnaire américain en Europe, a en fait quitté New-York le 28 mai 1917 !

[102] Voir le chapitre « Les travaux de la section du chiffre pendant la Première Guerre Mondiale » p. 98.

présentée en 1881 dans son manuel de cryptographie[103]. Elle est également connue grâce à Jules Verne, qui en a décrit le fonctionnement dans *Mathias Sandorf*.

Le cylindre de Jefferson

Thomas Jefferson (1743-1826), troisième président des États-Unis d'Amérique (1801-09), et co-auteur de la Déclaration d'indépendance, fit d'abord une carrière de diplomate et d'homme politique. Alors qu'il était secrétaire d'état de George Washington (1790), il mit au point un dispositif mécanique, le *Wheel Cipher*, un cylindre constitué de 26 disques rotatifs sur la tranche desquels était imprimé un alphabet désordonné[104].

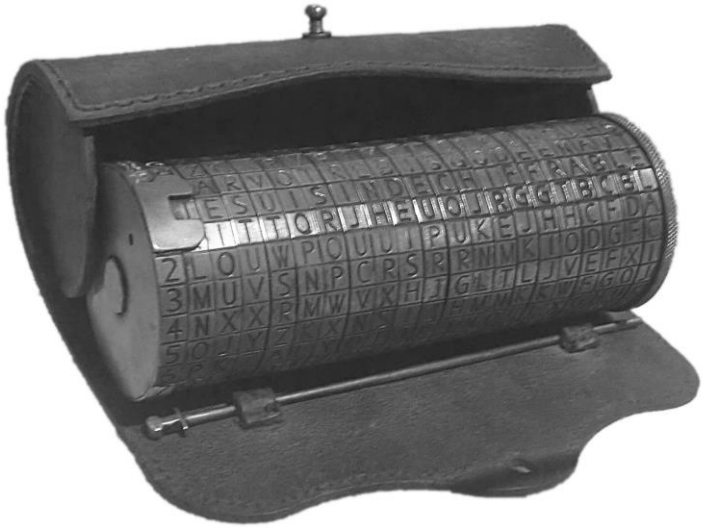


Fig. 6. Le cylindre de Bazeries. Exemplaire exposé au Musée des Télécommunications de Rennes. Photographie P. Guillot

Pour chiffrer un message, il suffit de faire tourner les roues de manière à lire le message sur une certaine ligne. Le cryptogramme transmis n'est autre que l'une quelconque des séquences de lettres lues sur une autre ligne. Pour déchiffrer, le destinataire doit disposer du même cylindre constitué des

[103] von Wostrovitz, *Handbuch der Krytographie.*

[104] La structure circulaire du cylindre de Jefferson améliore un dispositif préalablement inventé par John H. B. Thwaites sous forme de réglettes coulissantes maintenues dans un cadre en carton. Voir plus haut « Réinventions du chiffrement de Vigenère ».

mêmes disques. Il lui suffit alors d'aligner les lettres du cryptogramme et de lire le seul texte qui semble avoir un sens parmi les autres alignements. Changer de clé revient à changer l'ordre des disques.

Une fois de plus, ce dispositif sera réinventé par le cryptanalyste militaire français Étienne Bazeries (1846-1931) en 1891 et par le colonel italien Durcos en 1900. Une variante de ce cylindre, le cylindre M-94, amélioré aux États-Unis par le colonel Joseph O. Mauborgne (1881-1971), a été utilisé par l'armée américaine entre 1922 et 1942.

D'autres exemples de mécanismes élémentaires pourraient être donnés. Le cadran chiffrant de Charles Wheatstone (1802-75)[105], cet acousticien qui fit fonctionner la première liaison télégraphique à fil au nord de Londres en 1836, est une version améliorée du disque d'Alberti, où le disque chiffrant pivote par engrenage devant le cadran fixe. Il suscitera un vif intérêt à l'Exposition Universelle de Paris en 1867. La réglette de Saint-Cyr, en est un autre exemple. Elle sera utilisée à l'Ecole militaire française de même nom de 1880 au début du 20e siècle. En faisant coulisser l'alphabet de chiffrement sous l'alphabet du message clair, elle simplifie également les deux étapes du travail.

Les machines à rotors

De fait, le chiffre polyalphabétique ne verra son utilisation se généraliser qu'avec l'apparition des machines électromécaniques à rotors au début du 20e siècle. Presque simultanément, ces machines ont été proposées par quatre inventeurs de pays différents, sans convaincre immédiatement de leur intérêt.

L'Américain Edward Hugh Hebern (1869-1952) dépose un brevet en 1918 pour proposer sa machine à l'armée américaine qui refuse l'offre pour des raisons de vulnérabilité. Le Hollandais Hugo Alexander Koch (1870-1928) en dépose un autre en 1919. Et l'ingénieur suédois Arvid G. Damm (?-1927) a déposé des brevets qui seront exploités à partir de 1925 par la société *Aktiebolaget Cryptograph*, fondée par l'industriel suédois Boris Hagelin (1892-1983). Cette société deviendra la société suisse *Crypto-AG*, encore en activité aujourd'hui, et équipera de nombreuses armées occidentales, dont l'armée française, en machines mécaniques et électromécaniques.

---

[105] Wheatstone est également l'auteur d'une méthode de chiffrement par transposition, dite « chiffre de Playfair », qui sera encore en usage au-delà de la Première Guerre Mondiale. Voir le chapitre « Du message chiffré au système cryptographique » p. 110.

Fig. 7. Vue ouverte de la machine *Enigma*. Photographie P. Guillot.

La machine de ce type la plus connue est l'*Enigma*, dont l'Allemand Arthur Scherbius (1878-1929) a déposé le brevet en 1918. Pour la commercialiser, il fonde la société *Chiffriermaschinen* en 1923, et propose d'abord sa machine aux milieux bancaires et commerciaux qui ne l'adopteront pas. La force de la machine de Scherbius réside dans la sécurité du chiffrement polyalphabétique et dans sa simplicité d'utilisation : l'opérateur actionne une touche sur le clavier et une lampe s'allume qui donne le caractère chiffré correspondant. C'est l'armée allemande, consciente de la faiblesse du procédé de chiffrement ADFGVX[106], qui verra l'intérêt de cette nouvelle machine : la *Reishmarine* l'adoptera en 1926, la *Reishwehr* en 1928, et enfin la *Luftwaffe* en 1935. Du fait de la *Blitzkrieg*, qui consiste en une attaque rapide et synchronisée des différentes forces armées – infanterie, unités mécanisées et aviation –, le commandement militaire allemand doit se doter d'un vaste système de communications entre chaque unité et le quartier général. La *Blitzkrieg* donne une place très importante aux communications radio, et donc au chiffrement du fait de la dispersion des ondes électromagnétiques qui les rendent par nature sensibles

[106] Voir le chapitre « Les travaux de la section du chiffre pendant la Première Guerre Mondiale » p. 87.

à une interception par ses ennemis. Un chiffrement portable sur le front, mécanique, dispensant l'opérateur d'efforts de chiffrement manuel est un élément stratégique déterminant.

Le principe de ces machines repose sur des cylindres rotatifs, les rotors, qui sont bordés de 26 contacts, représentant chacun une lettre de l'alphabet. Ces rotors sont traversés par des circuits électriques qui réalisent une permutation entre les contacts de chaque bord. Plusieurs rotors sont mis en série pour composer les permutations. La clé est constituée du choix et de la disposition des rotors.

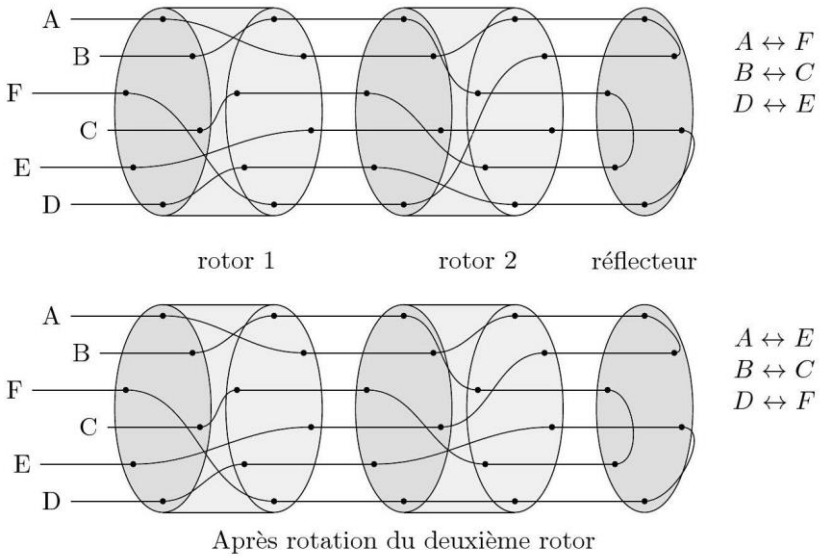


Fig. 8. Mode de fonctionnement d'une machine à 2 rotors. Illustration P. Guillot.

Un réflecteur compose ces substitutions avec leurs substitutions réciproques, rendant l'opération de chiffrement identique à l'opération de déchiffrement, ce qui évite d'avoir à inverser l'ordre des rotors pour déchiffrer. La machine dispose également, à l'avant de l'appareil, d'un tableau de connexions qui modifie la suite des lettres du message en permutant deux à deux certaines d'entre elles Et pour chaque lettre, les rotors tournent à la manière d'un compteur, changeant ainsi la substitution qui s'opère sur l'alphabet.

Le nombre de substitutions est ainsi devenu considérable, atteignant un nombre voisin de 1,5 x 10^{20} pour un tableau de connexions de dix fiches et

trois rotors en ordre quelconque[107]. Il est tel que le chancelier Adolf Hitler (1889-1945) n'a jamais voulu croire à la résolution du chiffre de cette machine. Les machines appelées « Bombes » ont été essentielles à leur décryptement. Elles ont été réalisées à partir des travaux conjugués des cryptanalystes polonais en 1939 et d'Alan M. Turing (1912-54) à Bletchley Park[108] (1939-1943).

CONCLUSION

Les développements de la cryptologie sont ainsi marqués par une longue tradition d'analyse des modes d'écriture, et se trouvent de ce fait profondément attachés à celle du langage. En témoigne d'ailleurs l'intérêt constant des écrivains portés vers les thématiques scientifiques, comme Edgar Poe, Jules Verne, ou Conan Doyle[109] et Maurice Leblanc[110]. Cette relation quasiment intrinsèque entre cryptologie et langage s'inscrit dans la culture de ses meilleurs praticiens, l'éducation des personnes éduquées s'attachant à les initier aussi aux manipulations d'écriture[111]. L'efficacité des procédés d'exécution est longtemps restée plus essentielle que les jeux d'esprit pour assurer la qualité du travail du chiffrement au service des centres de pouvoir. Quantitativement au moins, la recherche de procédés automatiques, voire mécaniques, de chiffrement a été plus essentielle au bon fonctionnement des services du chiffre que l'utilisation de méthodes systématiques ou mathématiques. Les débuts de la mécanisation de ces procédés annoncent la fin de l'ancrage de la cryptologie dans les jeux d'écriture.

C'est pourtant au moment où les formes traditionnelles de la cryptologie entrent en littérature que celle-ci change de nature et d'échelle. Lorsque les écrivains valorisent les astuces personnelles de l'individu cryptanalyste, ils en masquent paradoxalement les plus récentes avancées. Avec les nouveaux moyens de communication de la société industrielle, la cryptologie bascule

---

[107] Ce nombre est exactement $C_{26}^{20} \times \prod_{i=1}^{9} C_{2(10-i)}^{2} \frac{1}{10!} \times 26^3 \times 3!$, puisque 20 lettres sont choisies parmi 26, et que, parmi ces 20 lettres, 2 sont d'abord choisies parmi 20, puis 2 parmi les 18 restantes, *etc*. La division par 10 ! correspond au fait que l'ordre des paires ne compte pas, alors que dans le comptage qui précède, chaque paire a été dénombrée de 10! manières différentes. $26^3 \times 3$! est le nombre de combinaisons offertes par les trois rotors en ordre quelconque.

[108] Voir le chapitre « Pourquoi et comment la cryptologie vient de surgir dans le domaine de la carte à puce ? » note 6, p. 207 et « Cryptographie et théorie des nombres » p. 163.

[109] Doyle, *Sherlock Homes, Les hommes dansants.*

[110] Leblanc, *Arsène Lupin, L'aiguille creuse.*

[111] Sorel, *La science universelle*.

vers la recherche d'une maîtrise globale du secret des échanges organisés en divers réseaux, télégraphiques, téléphoniques, radiophoniques, et informatiques. La notion de système cryptographique, issue de ce processus d'adaptation, apparaît comme le concept majeur de ce basculement, à la fois théorique et sociologique. Il soutiendra l'ouverture de cette activité vers de nouveaux champs de possibles, et la professionnalisation du milieu. Et c'est dans ce milieu en voie de professionnalisation que les mathématiques seront progressivement investies comme outil d'analyse plus systématique.

BIBLIOGRAPHIE

Alberti, L. B., « De cyphris », *Actes du Congrès International de Paris*, tenu en 1995 sous la direction de F. Furlan, P. Laurens, S. Matton, Paris, Vrin, et Turino, Nino Aragno editore, 2000, pp. 705-725, éd. F. Furlan et al.

Aulu Gelle, *Nuits attiques*, *Tome IV*, Les Belles Lettres, 1998.

Babbage, C., « Philosophy on Deciphering », manuscrit, London, British Library, Add. Mss. 37205.

Barbin, E. et Boyé, A. (éds), *François Viète, un mathématicien sous la Renaissance*, Paris, Vuibert, 2005.

Belaso, G. B., *La cifra del sig. Giovan Battista Bellaso, gentil'huomo bresciano, nuovamente da lui medesimo ridotta à grandissima brevità et perfettione*, Venetia, 1553.

Brian, E., *La mesure de l'Etat. Administrateurs et géomètres au XVIII^e siècle*, Paris, Albin Michel, 1994.

de Callières, F., *De la manière de négocier avec les Souverains*, Paris, Michel Brunet éditeur, 1716.

Cardan, J., *Ma vie*, *Autobiographie*, Paris, Belin, 1992.

César, *Gaules*, Paris, Gallimard Folio Classique, 1981.

Chauviré, C., *L'essayeur de Galilée*, Paris, Les Belles Lettres, 1980.

Collard, B., *Les langages secrets dans l'antiquité gréco-romaine*, thèse de l'Université Catholique de Louvain, 2004, bcs.fltr.ucl.ac.be/FE/07/CRYPT/Crypto44-63.html.

Coumet E., « Cryptographie et numération », *Annales, Économies et Société, Civisisations*, 1975, 30^e année, n° 5, pp. 1007-1027.

Crescenzo, R., *Peintures d'instruction, la postérité littéraire des Images de Philostrate en France de Blaise de Vigenère à l'époque classique*, Genève, Droz, 1999.

Delahaye, J.-P., 2003, « Viète, inventeur de la cryptanalyse mathématique », *Pour la Science*, n° 313, novembre 2003, pp. 90-95.

— id., 2005, « Viète et les codes secrets », *in* (éds.) E. Barbin et A. Boyé,

François Viète, un mathématicien sous la Renaissance, Paris, Vuibert, pp. 161-164.

Della Porta, G., *De furtivis litteratum notis*, Naples, 1583.

Djebbar, A., *Une histoire de la science arabe*, Paris, Seuil, 2001.

Doyle, A. C., *Sherlock Holmes, Les hommes dansants,* Paris, Editions Ebooks libres et gratuits, 2013. http://www.diogene.ch/IMG/pdf/conan_doyle_hommes_dansants_im.pdf.

Durand-Richard, M.-J., « Calcul et Signification », *Images des Mathématiques*, CNRS, 2012. http://images.math. cnrs.fr/Calcul-et-Signification.html.

Febvre, L., *Le problème de l'incroyance au XVI^e siècle, La religion de Rabelais,* Paris, Albin Michel, 1947.

Franksen, O. I., 1993, « Babbage and cryptography. Or, the mystery of Admiral Beaufort's cipher », *Mathematics and Computers in Simulation*, n° 35, pp. 327-367.

Golsenne T., Prevost, B., *Leon Battista Alberti. La Peinture,* Paris, 2004, édition, traduction, commentaire, édition revue par Y. Herant.

Hébrard, P., *La cryptologie dans l'histoire*, Paris, ARCSI, édition privée interne, 2001.

Jeffery, L. H., *The Local Scripts of Archaic Greece*, Oxford, Oxford University Press, 1961.

Kahn, D., *The Codebreakers, the Story of Secret Writing,* New York, McMillan Publications, 1996.

(eds.) M. Mrayati, Y. Meer Alam, M.H. al-Tayyan, *Al-Kindi's Treatise on Cryptanalysis*, Riyadh, King Faisal Center for Research and Islamic Studies, 2003.

— *Ibn Adlan's Treatise al-mu'allaf lil-malik al-Asraf*, Riyadh, King Faisal Center for Research and Islamic Studies, 2003.

— *Ibn ad-Durayhim's Treatise on Cryptanalysis*, Riyadh, King Faisal Center for Research and Islamic Studies, 2004.

— *Ibn Dunaynir's Book : Expositive Chapters on Cryptanalysis*, Riyadh, King Faisal Center for Research and Islamic Studies, 2005.

Kelly, Th., « The Myth of the Scytale », *Cryptologia,* vol. 22, n° 3, july 1998, pp. 244-260.

Leblanc, M. *Arsène Lupin, L'aiguille creuse*, Paris, Fleurus Classiques, 2012.

Lerville, E., *Les cahiers secrets de la cryptographie, Le chiffre dans l'histoire des histoires du chiffre*, Paris, Editions du Rocher, 1972.

Mersenne, M., *Harmonie universelle, contenant la théorie et la pratique de la musique*, Paris, Sébastien Cramoisy, 1636-37. Paris, Ed. CNRS, 1960.

Morazé, C., *La science et les facteurs de l'inégalité*, Paris, PUF, 1985.

Patarin, J. et Nachef, V. « "I Shall Love You Until Death" (Marie-Antoinette to Axel von Fersen) », *Cryptologia*, vol. 34, n° 2, 2010, pp. 104-114.

Pesic, P., 1997, « Secrets, Symbols and Systems : Parallels between Cryptanalysis and Algebra, 1580-1700 », *Isis*, vol. 88, n° 4, dec. 1997, pp. 674-692.

— id., 1997, « François Viète, father of Modern Cryptanalysis. The two Manuscripts », *Cryptologia*, vol. 21, n° 1, 1997, pp. 1-29.

Poe, E. A., « A Few Words on Cryptography », *Graham Magazine*, 1841.

— « Le scarabée d'or », *Histoires Extraordinaires*, traduction française de Ch. Baudelaire, Paris, Le livre de poche, 1960.

— « La cryptographie », *Derniers contes*, traduction française de F. Rabbe, Paris, Albert Savine éditeur, 1887, pp. 269-300.

Plutarque, « Vie de Lysandre », *La vie des hommes illustres*, Paris, Firmin Didot, 1883.

Rashed, R., *Entre arithmétique et algèbre : recherche sur l'histoire des mathématiques arabes*, Paris, Les Belles Lettres, 1984.

— « Algèbre et Linguistique : l'analyse combinatoire dans la science arabe », *in* R. Cohen, *Boston Studies in the philosophy of sciences*, Reidel Publ. Company, vol. X, 1973, pp. 383-99.

Rosenheim, S. J., *The Cryptographic Imagination: Secret Writing from Edgar Poe to the Internet*, Johns Hopkins, 1997.

Singh, S., *Histoire des codes secrets*, Paris, J. C. Lattès, 1999.

Sorel, Ch., *La science universelle*, Paris, Toussaint Quinet, 1647.

Suetone, *La vie des douze Césars* http://bcs.fltr.ucl.ac.be/SUET/CAES/texte.html.

Thucydide, *Histoire grecque de Thucydide*, traduction de J.-B. Gail, Paris, Gail neveu, 1807.

Trithème, J., *Polygraphiae libri sex, Ioannis Trithemii abbatis Peapolitani, quondam Spanheimensis, ad Maximilianum Ceasarem*, Oppenheim, J. Haselbergii de Aia, 1518.

Vigenère, B. de, *Traicté des Chiffres, ou secrètes manières d'escrire*, Paris, Abel Langelier, 1596.

von Wostrovitz, E. B., *Handbuch der Kryptrographie, Anleitung zum Chiffriren und Dechiffriren von Geheimschriften*, Wien, Selbsverlage des Verfassers, 1881.

Verne, J., *Mathias Sandorf*, Paris, Pierre-Jules Hetzel, 1885.

— *La Jangada*, Paris, Ed. Motif, 2005.

SUR L'EXTRACTION DE L'OBSCUR

AL-KINDI[1]
Traduction[2] Abderrahman DAIF et Kaltoum TANTAOUI[3]

Au nom de Dieu le tout miséricordieux et le très miséricordieux !
Dieu seul nous suffit.

Epitre d'Abī Yūssef Ya'qūb ibn Isāq al-Kindī sur l'extraction de l'obscur adressée à Abū al-'Abbās

INTRODUCTION[4]

J'ai compris – que Dieu étende ta compréhension et accroisse ton savoir ! – ce que tu as ordonné d'écrire dans ce livre – des ruses[5] sur l'extraction de ce qui est consigné dans les livres obscurcis – afin d'en faire

[1] NdT. : Abī Yūssef Ya'qūb ibn Isāq al-Kindī (801-873) est considéré comme l'un des savants arabes les plus importants. Il a travaillé en philosophie, mathématiques, médecine, musique, philosophie naturelle et astronomie. Sous le califat abbasside d'Al-Mansur, il a dirigé, à la Maison de la Sagesse (*Bayt al Hikma*) de Bagdad, la traduction des manuscrits grecs, en compagnie du mathématicien al-Khwarizmi. Rashed, *Œuvres philosophiques et scientifiques d'al-Kindi.*

Ce traité d'al-Kindi est le premier grand traité de cryptologie arabe qui nous soit parvenu. Il est significatif de l'importance des savants arabes dans la naissance de cette activité. Il porte essentiellement sur une analyse de l'écriture arabe, et s'appuie sur un travail systématique de classification des méthodes, tant de chiffrement que de décryptement. Le travail de classification, caractéristique d'une science selon Aristote, témoigne de l'appropriation de la philosophie aristotélicienne, depuis le recours aux catégories aristotéliciennes du quantitatif et du qualitatif, jusqu'à la référence aux notions de genre et d'espèce. Voir le chapitre « L'ancrage de la cryptologie dans les jeux d'écriture » pp. 26-31.

[2] NdT. : Cette traduction a été réalisée à partir de l'édition bilingue arabe-anglais éditée à Riyad en 2003-2005. Elle a été relue par Philippe Guillot. Les traducteurs se sont attachés à ne pas utiliser les termes apparus ultérieurement comme cryptologie ou cryptanalyse. Ils sont restés au plus près du sens originel des mots afin de ne pas leur conférer une signification qui renverrait à la situation actuelle de la discipline. Dans le texte d'Al-Kindi, ce qu'on appelle aujourd'hui « chiffrer » s'exprime par « obscurcir », et « décrypter » par « extraire l'obscur ».

[3] Étudiants du master de cryptologie de l'Université Paris 8-Vincennes-Saint-Denis.

[4] NdE. Les titres des paragraphes n'existent pas dans le texte original.

[5] NdE. : Le mot « ruse » n'a pas ici de connotation négative, il correspond ici à l'idée d'astuce ou de procédé ingénieux.

un livre assez court mais complet. Louange à Dieu ! Des connaissances qui étaient encore négligées ont été découvertes, et tu as permis à beaucoup de gens de profiter des bienfaits de ce livre. Je l'implore de t'aider à accomplir toutes les bonnes actions, de te soutenir dans tes bonnes attentions, de t'accorder le succès pour atteindre tes buts et de t'offrir le bonheur autant dans ton existence terrestre que dans ta vie dans l'au-delà.

L'extraction de l'obscurité a des grands avantages, comme ce fut le cas pour bon nombre des anciens philosophes et savants qui ont utilisé des signes inconnus dans leurs livres. Mais ceux qui sont réticents à utiliser leurs connaissances pour découvrir les secrets de l'extraction de l'obscurité ne peuvent pas atteindre des niveaux élevés dans leur accomplissement savant. Cela n'était pas mon souhait mais mon sens du devoir de t'aider à atteindre tout ce que tu exiges avec moins d'efforts – que Dieu facilite tes actions et t'accorde toujours l'éloquence ! J'aurais préféré suivre la voie des savants qui m'ont précédé et qui pensaient à obscurcir les trésors de la signification plutôt que de les afficher et de les révéler. J'ai été encouragé par ma conscience, du fait qu'un grand nombre de livres écrits de philosophie qui sont pour toi d'un examen facile et dont tu sauras extraire les significations, sont très difficiles à comprendre dans un court laps de temps et fatiguent l'esprit de la majorité de ceux qui les consultent. Par conséquent, j'ai écrit sur ce sujet ce que je pensais être assez clair pour les fils de la sagesse, tout en restant hors de portée des personnes non informées. Que Dieu m'apporte le succès.

LES CHEMINS POUR EXTRAIRE L'OBSCUR

Ce que je dis, c'est que les lettres obscures sont, soit faites de rapport numérique, c'est-à-dire de poésie, soit ne sont pas faites ainsi. En ce qui concerne celles qui ne sont pas poésie, elles peuvent être dévoilées avec des méthodes soit quantitatives soit qualitatives.

La ruse quantitative consiste à connaître les lettres les plus fréquentes dans cette langue – la langue dans laquelle on veut extraire ce qui était obscur dans les livres – nous disons : les lettres sonores[6] sont comme la matière de n'importe quelle langue, et les non sonores[7] sont comme la forme, et de nombreuses formes peuvent être créées à partir de la même matière[8]. Cela peut être, de l'or, des couronnes, des diadèmes, des bracelets, des coupes, *etc*. Dans ces réalisations, l'or vaut plus que les formes qu'il a

[6] Ce sont les voyelles.
[7] Ce sont les consonnes.
[8] NdE. : La forme et la matière sont des concepts importants de la philosophie aristotélicienne.

constituées. De même, les lettres sonores, qui sont la matière de tout type de texte valent plus que les lettres non sonores. J'entends par sonores les lettres *alif*, *wow*, et *yāa*. Par conséquent, les [lettres] sonores sont inévitablement les lettres qui existent le plus dans n'importe quelle langue. Il arrive dans certaines langues que certaines lettres sonores soient plus nombreuses que certaines autres lettres sonores, tandis que les non-sonores peuvent être fréquentes ou rares selon leur utilisation dans chaque langue, comme le son *S* dont la fréquence d'occurrence est élevée en grec[9].

Une des ruses que nous utilisons pour extraire l'obscurité d'un livre, si la langue est déjà connue, est de trouver un texte qui contient autant [de lettres] qu'un livre, puis nous notons « première » les plus fréquentes, et « deuxième » les prochaines en abondance et « troisième » celles qui les suivent en abondance, et ainsi de suite jusqu'à avoir complété toutes les sortes de lettres. Puis, nous regardons dans le texte d'où nous voulons extraire [l'obscur] et nous classons aussi les sortes de ces lettres, et nous regardons les plus nombreuses. Nous les nommons « première lettre ». Et celles qui suivent en abondance, nous les nommons « deuxième lettre ». Et celles qui les suivent en abondance, nous les nommons « troisième lettre », et ainsi de suite jusqu'à épuiser tous les sortes de lettres de ce texte d'où nous voulons extraire [l'obscur].

Il peut arriver parfois que le texte obscur soit court et ne contienne pas toutes les lettres, ou que l'abondance et la rareté des lettres ne puissent pas être utilisées. En effet, l'abondance et la rareté des lettres ne peuvent être utilisées correctement que dans des textes longs, où l'abondance et la rareté des lettres peuvent être compensées. Ainsi, si l'une des sortes de lettres de ce livre est rare dans une partie, cela est compensé par son abondance dans une autre partie.

Mais si le livre est court il y a moins de compensation possible, et l'ordre de fréquence des lettres ne peut pas être appliqué. Alors tu devras utiliser une autre ruse que quantitative pour extraire les lettres. Elle consiste à connaître les lettres qui s'associent et celles qui ne s'associent pas dans la langue du texte dont on veut extraire l'obscur. Lorsque tu observes deux de ces lettres en utilisant l'ordre de la fréquence des lettres, tu te demandes : est-ce qu'elles s'associent ou non dans cette langue ? Si c'est le cas, tu cherches chacune d'entre elles à une autre place et tu observes en comparant avec la lettre avant et après elle, en utilisant aussi pour l'extraction les ordres des lettres, puis en te demandant : est-ce qu'elles peuvent être associées ou non avec cette lettre ? Si tu trouves que toutes ces lettres s'accordent avec cette lettre, alors tu regardes les lettres qui se combinent avec la deuxième

[9] NdT. : le mot arabe dans le texte est *Roumi*, qui littéralement signifie *Romain*, mais l'empire romain de l'époque est l'empire romain d'Orient, c'est-à-dire Byzance, où la langue des lettrés était le grec, langue dont al-Kindi lui-même était fortement imprégné.

lettre avant et après elle ; si elles s'associent vraiment, alors ce sont des lettres certaines, si ce n'est pas le cas, ce ne sont pas des lettres certaines. Si des lettres certaines sont vraiment trouvées, indiquées par la combinaison des lettres et aussi par leur ordre de fréquence, des syllabes surviennent jusqu'à ce qu'un mot apparaisse. Puis tu utilises la méthode à un autre endroit du livre de la même façon. Si les prononciations qui apparaissent s'accordent, tu utilises de la même façon la méthode à un autre endroit du livre, jusqu'à l'apparition complète.

Il est important de chercher dans toutes les langues les lettres qui s'associent le plus et de les utiliser comme indice, comme la combinaison en arabe de la lettre *alif* (أ) avec la lettre *lām* (ل) et *vice-versa*, comme dans le mot إلا (*illa*, sauf) et le mot الكتب (*al kotob*, les livres).

– et comme *mīm* (م) et *alif* (ا) dans ما (*ma*, exprime la négation),
– et comme *mīm* (م) et *lām* (ل) dans لم (*lam*, exprime la négation),
– et comme *nūn* (ن) et *mīm* (م) dans من (*mina*, de),
– et comme *'aīn* (ع) et *nūn* (ن) dans عن (*'an*, de),
– et comme *alif* (ا) et *wāw* (و) dans أو (*aw*, ou),
– et comme *lām* (ل) et *wāw* (و) dans لو (*law*, exprime le souhait),
– et comme *ṯāa* (ث) et *mīm* (م) dans ثم (*thomma*, ensuite),
– et comme *kāf* (ك) et *mīm* (م) dans كم (*kam*, combien),
– et comme *'aīn* (ع) et *lām* (ل) dans علّ (*'alla*, exprime le souhait),
– et comme *sīn* (س) et *mīm* (م) dans سم (*som*, poison),
– et comme *lām* (ل) et *'aīn* (ع) et *yāa* (ي) dans على (*'alaa*, sur).
– et comme *kāf* (ك) et *mīm* (م) et *alif* (ا) dans كما (*kamaa*, comme).

Et ainsi de suite. Utiliser cette méthode donne une précieuse indication sur l'extraction des lettres en employant ces deux sources : les ordres de l'abondance et de la rareté des lettres, et les lettres qui s'associent et qui ne s'associent pas.

Ce qui aide aussi à s'orienter, c'est de connaître dans chaque langue les déclarations d'ouverture d'honneur بسم الله الرحمن الرحيم [10] dans les livres arabes. Puis tu te serviras de ces lettres dans tout le livre. Et cet indice, qui est au début des livres n'apparaît pas dans chaque livre, parce que le livre peut être dépourvu de ce début, comme dans la langue arabe, la poésie est dépourvue de بسم الله الرحمن الرحيم. Par conséquent, si tous les indices indiqués ci-dessus semblent s'accorder sauf celui sur le début des livres, ce dernier peut être ignoré, mais si les indices s'accordent, alors cela confirme ce qui était attendu.

Nous pouvons penser que connaître chaque lettre parmi les lettres facilitera l'extraction du sens. En combinant les lettres sonores avec les lettres non sonores, et en combinant chaque lettre non sonore avec la plus

[10] NdT. : Au nom de Dieu le tout miséricordieux et le très miséricordieux.

proche des lettres sonores, puis en liant tout cela ensemble, les mots apparaissent et leur extraction devient facile.

Vient alors cette ruse qui extrait les lettres obscures – qu'elle soit poésie ou autre – selon laquelle les vers obscurs peuvent être rendus visibles par leurs rimes, puis en comptant le nombre de lettres dans un vers, puis en le présentant sur toutes les mesures poétiques connues en arabe, l'extraction des lettres survient ensuite par les ruses que nous avons indiquées, elles sont utilisées ici en les appliquant aux mesures du rythme. Si elles s'appliquent, tu présumes que ce sont les mots attendus, si ce n'est pas le cas, tu utilises un autre expédient, et tu l'appliques à nouveau aux mesures du rythme.

Ces méthodes sont ainsi les premières ruses pour extraire l'obscurité des lettres, et avec de la recherche et de la réflexion, d'autres idées que ces ruses, produites par ces ruses, peuvent apparaître, et qui servent à extraire l'obscurité des lettres.

Pour que cette question soit facile dans notre langue, nous dessinons dans notre livre les ordres de l'abondance et de la rareté des lettres, et celles qui s'associent et qui ne s'associent pas, avant ou après, cela facilite la méthode de résolution à ceux qui suivent ce chemin. Que Dieu leur apporte le succès !

LES CATEGORIES IMPORTANTES POUR L'OBSCURCISSEMENT

Et en premier lieu nous demandons : de combien de catégories disposons-nous parmi les catégories importantes pour extraire l'obscurité des lettres ? Nous répondons : cela se divise en deux grandes classes d'extraction de l'obscurité : soit simple, soit composée.

L'obscurité simple se divise en deux classes principales : soit simple avec changement du dessin des lettres, soit simple sans changement du dessin des lettres.

Et celle avec changement du dessin des lettres se divise d'abord en deux classes principales : l'une avec lien et interprétation [entre la lettre et sa signification], l'autre sans lien ni interprétation.

Et celle avec lien et interprétation se divise elle-même en deux classes principales : l'une par rapport au genre, et l'autre par rapport à l'espèce[11]. Et dans ces cas, l'indication donnée par la forme peut être soit unique, soit multiple. Par unique, je veux dire comme le changement de la lettre *ṭāa* (ط) par l'image d'un oiseau unique tel un pigeon. Et par multiple, je veux dire comme le changement de la lettre *ṭāa* (ط) par l'image de n'importe quel oiseau, étant donné que l'oiseau en général est une espèce pour tous les genres et toutes les formes d'oiseaux.

[11] NdE. : Le genre et l'espèce sont des concepts importants de la philosophie aristotélicienne.

Et l'autre catégorie qui est sans lien ni interprétation se divise en deux classes principales : l'une avec changement de la forme du dessin, et l'autre sans changement de la forme du dessin.

Le changement du dessin des lettres se divise en deux grandes classes : l'une échange le dessin des lettres en mettant le dessin des unes pour les autres, par exemple en mettant le dessin de la lettre *alif* pour la lettre *bāa* et le dessin de la lettre *bāa* comme indice de la lettre *alif* et ainsi de suite pour les autres lettres. Et l'autre change le dessin des lettres en mettant des dessins inventés qui ne sont pas liés aux lettres.

Et ce genre se divise en deux catégories : l'une en mettant les dessins pour plusieurs lettres qui s'associent le plus souvent :

لا ما أو لم من أن عن في

etc. pour chaque association de lettres, un seul dessin, et deux dessins rassemblés pour une seule lettre. Cette méthode peut être appliquée à toutes les lettres, ou bien à toutes les lettres associées, ou seulement à quelques-unes sans les autres.

L'obscurcissement sans changement dans la forme du dessin se divise en deux classes principales, l'une en modifiant la position, l'autre sans modifier la position.

La modification des positions [des lettres] se divise en deux classes principales, l'une en mettant une lettre à la position d'une autre, je veux dire avant ou après elle, et l'autre en formant la lettre autrement, en dessinant le haut en bas, ou à l'avant, ou à l'arrière, *etc*.

Pour changer la position de la lettre avant et après celle-ci, soit tu places une lettre à la dernière position des lettres du nom, et tu procèdes en inversant les autres lettres du nom, ou bien en plaçant la première lettre du nom à la position de la dernière lettre, la deuxième lettre à la position de la première lettre, et la troisième à la suite de la première lettre et la quatrième à la suite de la deuxième et ainsi de suite jusqu'à épuiser toutes les lettres du nom. Ou bien tu laisses la dernière lettre à sa position, et la deuxième à une autre position dans le nom, et la troisième après la dernière lettre du nom, et la quatrième après la deuxième lettre du nom, et ainsi de suite jusqu'à épuiser toutes les lettres du nom, ou bien en plaçant la première lettre à une certaine position dans le nom, et la deuxième à la position de la dernière lettre du nom, et la troisième après la première, et la quatrième après la deuxième. Et tu peux aussi commencer par la dernière lettre, ou par l’autre extrémité, puis ensuite la deuxième lettre, la troisième derrière la première et la quatrième derrière la deuxième et ainsi de suite jusqu'à épuiser toutes les lettres du nom. De même, cette composition s'applique dans l'ordre inverse, et toutes ces méthodes résident dans les différences de position.

L'obscurcissement sans modification de position se divise en deux classes principales : l'une avec rajout de dessins sans signification qui ne contiennent pas de lettre sonore, et l'autre, sans rajout de dessin sans signification qui ne contient pas de lettre sonore, et même en ôtant une ou plusieurs lettres.

Le rajout des dessins sans signification qui ne contiennent pas de lettre sonore se divise en deux classes : le non signifiant peut être un ou multiple.

Et l'autre [classe d'obscurcissement] simple sans changement du dessin des lettres se divise en deux classes principales : l'une du côté quantitatif et l'autre du côté qualitatif.

Et celle du côté quantitatif se divise elle-même en deux classes principales : l'une en mettant la forme de la lettre en double ou en triple ou tout autre dédoublement de celle-ci, comme à la place de *alif*, deux *alif*, ou trois *alif* ou tout autre dédoublement de celle-ci. Et cette méthode donne lieu encore à deux classes, selon que le dédoublement est pour toutes les lettres ou pour certaines lettres seulement.

L'autre classe du côté quantitatif consiste à mettre une seule figure pour indiquer plusieurs lettres, comme *bāa* (ب) et *tāa* (ت) et *ṯāa* (ث) qui sont, en calligraphie arabe, représentées par la même figure. Et ceci se divise encore en deux classes selon que toutes [les lettres] sont englobées, ou seulement quelques-unes sans les autres.

Du côté qualitatif, l'autre classe sans changement du dessin de la lettre se divise en deux classes : soit en reliant les lettres séparées, soit en séparant les lettres liées, et chacune de ces deux méthodes peut être soit pour certaines lettres seulement, soit pour toutes les lettres.

L'autre classe parmi les deux grandes classes d'obscurcissement des lettres peut être constituée de toutes ces [méthodes] simples, où l'on trouve deux ou plusieurs d'entre elles qui peuvent être combinées. L'application de chaque obscurcissement simple est utilisée pour construire un obscurcissement composé, et, afin d'éviter de trop allonger le livre par des choses inutiles, si tu connais les méthodes simples et l'abondance des méthodes composées, il n'est pas nécessaire de présenter toutes les images d'obscurcissement composé, et cela permet de se limiter à montrer ce qu'il faut faire pour cet ouvrage.

Nous allons visualiser ces classes par un arbre, de sorte que tous nos sens participent à la compréhension de cet ouvrage et facilitent son assimilation. Que Dieu t'apporte le succès !

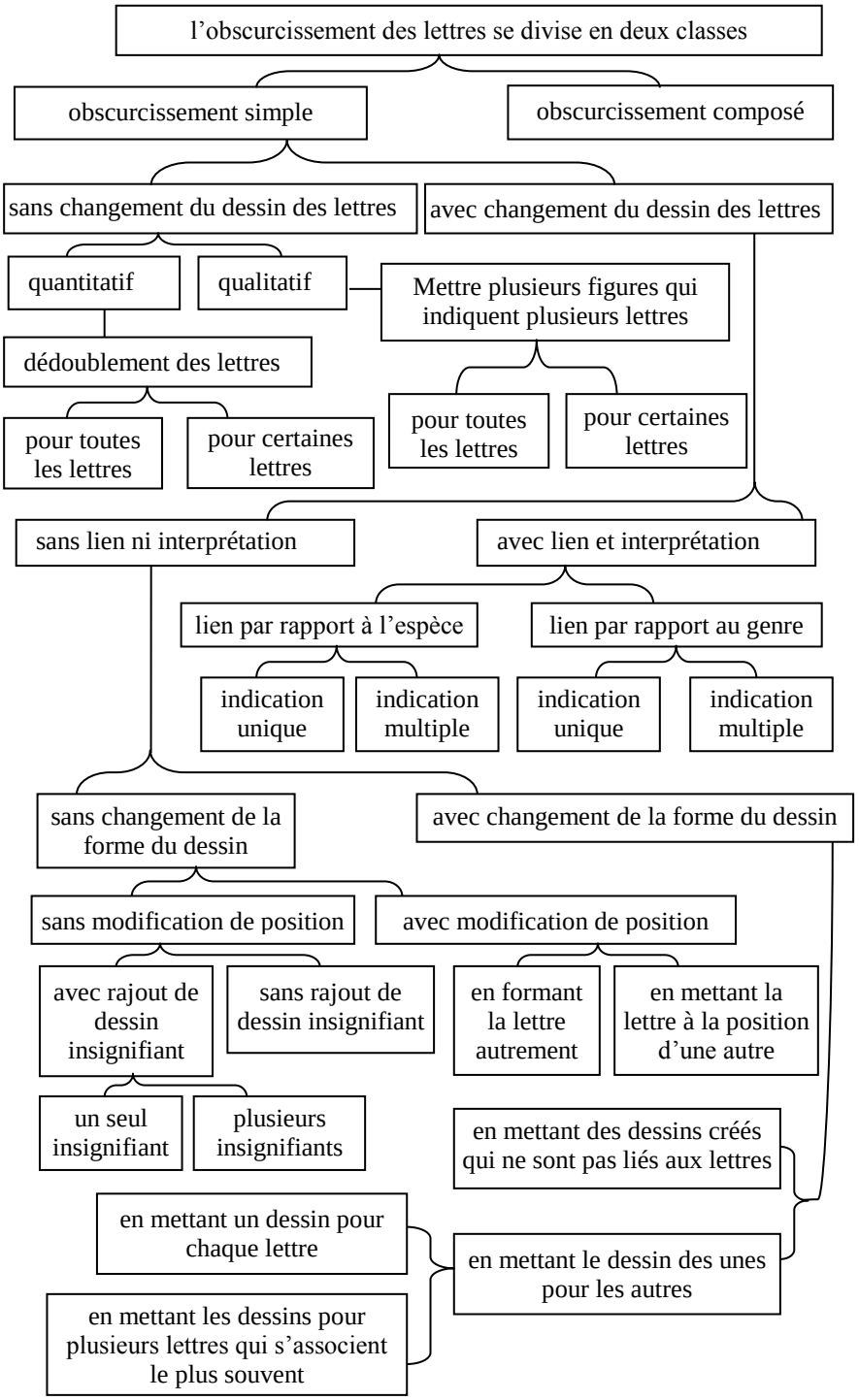

l'obscurcissement des lettres se divise en deux classes
obscurcissement simple
obscurcissement composé
sans changement du dessin des lettres
avec changement du dessin des lettres
quantitatif
qualitatif
Mettre plusieurs figures qui indiquent plusieurs lettres
dédoublement des lettres
pour toutes les lettres
pour certaines lettres
pour toutes les lettres
pour certaines lettres
sans lien ni interprétation
avec lien et interprétation
lien par rapport à l'espèce
lien par rapport au genre
indication unique
indication multiple
indication unique
indication multiple
sans changement de la forme du dessin
avec changement de la forme du dessin
sans modification de position
avec modification de position
avec rajout de dessin insignifiant
sans rajout de dessin insignifiant
en formant la lettre autrement
en mettant la lettre à la position d'une autre
un seul insignifiant
plusieurs insignifiants
en mettant des dessins créés qui ne sont pas liés aux lettres
en mettant un dessin pour chaque lettre
en mettant le dessin des unes pour les autres
en mettant les dessins pour plusieurs lettres qui s'associent le plus souvent

Fig. 1. Copie du diagramme original, significatif du travail de classification. M. Mrayati *et al.*, *Al-Kindi's Treatise on Cryptanalysis*, fig. 3.2 p.113.

METHODES D'EXTRACTION DE QUELQUES GENRES D'OBSCURCISSEMENT

Maintenant que j'ai présenté les classes d'obscurcissement, je vais présenter l'extraction de cet obscurcissement pour chaque classe.

Je dis d'abord : l'obscurcissement par changement des figures de lettres sans lien ni interprétation, qui peuvent être remplacées par des dessins qui ne sont pas des lettres, peut être accompli en remplaçant chaque lettre par une figure. L'extraction en est accomplie par les ruses mentionnées précédemment. Les figures qui se combinent fréquemment comme لا (*la*), إن (*inna*), ما (*mā*), أو (*aou*), لم (*lam*), أن (*an*), عن (*'an*), في (*fi*), لو (*lou*) *etc*. peuvent toutes être représentées par une seule figure.

La ruse pour extraire ce qui était masqué dans ce genre d'obscurcissement est d'utiliser les ruses indiquées précédemment, jusqu'à voir quelques-unes des lettres apparaître et, s'il en est apparu, les mots qui s'en suivent. Nous cherchons des positions où les lettres n'apparaissent pas, mais qui sont encadrées par les lettres qui viennent d'apparaître ; puis nous cherchons avec chacune des lettres connues, celles qui se combinent souvent avec elles. Nous conservons la lettre qui produit une séquence compréhensible ou un mot.

Si deux ou trois mots s'associent avec la figure de cette lettre obscure, par exemple si le mot قد (*qad*) se place entre إنه (*innaho*) et ذهب (*dhahaba*) tu obtiens : إنه قد ذهب (*innaho qad dhahaba*). Suppose maintenant que le mot لم (*lam*) se trouve à la place de قد (*qad*) alors tu obtiens إنه لم يذهب (*innaho lam yadhhab*). De même, le mot لن (*lan*) donne إنه لن يذ هب (*innaho lan yadhhaba*). S'il y a plusieurs mots qui ressortent, tu cherches les lettres déjà apparues dans un autre endroit du texte, y compris la lettre que tu veux extraire, qui est comparée à toutes les lettres associées. Si tu obtiens le mot juste, alors c'est bien la lettre recherchée. Si tu en obtiens plusieurs qui s'associent avec cette lettre, tu répètes le même travail jusqu'à trouver un seul mot lié à cette lettre. Après avoir testé cette méthode à un ou deux endroits du livre, et si l'apparition des mots significatifs se répète partout, tu peux penser que cette figure correspond bien aux deux lettres qui t'ont aidé à faire apparaître la signification. Une aide supplémentaire consiste à s'appuyer sur la fréquence ou la rareté des lettres.

Et nous allons écrire l'ordre de fréquence et de rareté des lettres associées dans la langue arabe lorsque nous écrivons l'ordre des lettres.

Un genre d'obscurcissement peut aussi consister à remplacer chaque lettre par la réunion de deux figures. Si tu penses que le livre est obscurci par ce genre [d'obscurcissement], c'est-à-dire que pour chaque lettre, il y a

deux figures réunies, alors tu comptes le nombre de figures des lettres de ce livre. S’il dépasse le nombre de figures de lettres de cette langue, alors cet excès est égal au nombre des figures réunies : tu peux alors penser que certaines lettres sont la réunion de deux figures.

Et si l'obscurcissement provient du changement de la figure, sans lien et avec ruse dans le changement de la figure, tu remplaces la figure des unes par celle des autres, par exemple la figure de la lettre *alif* pour montrer la lettre *bāa* et la figure de la lettre *bāa* pour montrer la lettre *alif*, et ainsi de suite pour les autres lettres.

L'obscurcissement résulte du désarroi face aux lettres et à l’absence de constitution d'un texte. Lorsque tu soupçonnes que seules les lettres sont utilisées pour en remplacer d’autres, tu essayes les possibilités de remplacer ces lettres non articulées par toutes les lettres qui n'ont pas été identifiées. En appliquant la recherche déjà utilisée pour les lettres dont la figure est remplacée par des figures créées qui ne sont pas liées aux lettres, les figures modifiées apparaissent. Si seulement une partie [de la lettre] est modifiée ou si toute la figure est modifiée, tu peux la considérer comme une figure créée, et la recherche se fait selon les premières ruses mentionnées précédemment.

Savoir si toutes les figures sont modifiées les unes par les autres provient de ce que la prononciation n'est pas facile. Si la prononciation est facile, ce qui est différent à un endroit du livre ne permet pas de trouver le sens à un autre endroit : c’est donc que le texte a été modifié.

Face à l'obscurcissement avec changement de figure des mots sans changement de la forme des lettres, mais seulement de leur position – je veux dire celle des figures – tu effectues une seule recherche pour toutes ces sortes. Et toutes les sortes [de changement de position] avant et après peuvent être appliquées aux lettres comme mentionné précédemment dans les méthodes d'obscurcissement.

L'obscurcissement avec changement des figures des lettres sans lien et sans changement de la forme du dessin s'effectue en changeant la position de la lettre, en mettant le haut en bas, ou l'avant, ou à l'arrière, *etc*. Son extraction est très facile. Tu peux savoir que ces lettres sont obscurcies par modification de la position lorsque le nombre des figures est le même que celui des lettres de cette langue, et que les figures sont les mêmes sauf qu'elles se différencient par leur position. Si une telle situation apparaît, tu fais tourner la figure dans tous les sens. Si une certaine mise en place donne une lettre qui est connue dans cette langue, alors tu prends cette figure comme représentation de cette lettre.

Le changement du dessin des lettres sans lien ni interprétation, sans changement de la forme du dessin, sans modification de la position, et avec rajout de dessins sans signification qui ne contiennent pas de lettre sonore, est indiqué en comptant les figures. Si cela dépasse le nombre des lettres de la langue, tu extrais quelques lettres du livre avec les ruses citées

précédemment. Tu examines ensuite quelques-unes des lettres qui ne sont pas encore apparues et tu essayes de trouver la ressemblance avec les lettres qui sont déjà apparues. Tu compares ces lettres avec le texte [extrait], en omettant celles que tu soupçonnes d'être des lettres sans signification dans plusieurs extraits du livre. Si le texte a un sens à ces endroits choisis, tu conclus que toutes les lettres omises ne sont pas signifiantes.

Si la condition est telle que nous l'avons mentionnée, je veux dire le changement de figure des lettres sans interprétation ni changement de la forme des figures, et sans changement des positions ni rajout de lettre insignifiante, mais avec omission d'une ou deux lettres du texte, tu peux le découvrir en trouvant des figures moins nombreuses que les lettres de l'alphabet dans cette langue. La ruse utilisée ici est la première de celles déjà mentionnées.

Si certaines lettres du texte sont apparues et si tu as trouvé celles qui lui ressemblent – si elles sont lues en une autre position – tu peux trouver un manque dans la lecture, comme dans *abdallah* (عبدالله), si le *dal* (د) est omis, nous lisons *aballah* (عباله). Tu cherches une lettre parmi celles déjà apparues ou une lettre associée avec *aballah* par l'une de ses extrémités : si le mot est privé de cette lettre dans deux ou trois endroits du texte, tu constates qu'une lettre est omise dans ce texte, tu consultes la position de cette lettre accolée à toutes les lettres de l'alphabet dans toutes les positions où est apparue une absence de lettre. Si tous les mots s'éclairent et donnent un sens en utilisant une seule lettre pour combler les vides, c'est donc que c'est cette lettre qui a été abandonnée. Le même travail est poursuivi si plusieurs lettres sont abandonnées.

Le changement de la figure des lettres avec lien et interprétation par rapport à l'espèce se divise en deux classes : l'indication donnée par la figure peut être soit unique, soit multiple. Par unique, je veux dire comme dans le changement de la lettre *ṭāa* (ط) d'un oiseau unique tel un pigeon ; par multiple, je veux dire comme le changement de la lettre *ṭāa* par l'image de n'importe quel oiseau ; et ceci peut être appliqué dans le changement de la forme de la lettre avec lien et interprétation par rapport au genre.

La distinction entre l'obscurcissement par rapport à l'espèce – s'il est l'image d'un oiseau unique ou de plusieurs – et par rapport au genre, c'est que l'image doit être celle d'un seul genre. Si tu peux savoir lequel, tu prends les premières lettres des genres. Dans ce cas, la prononciation s'éclaire. Sinon, les espèces et les genres sont remplacés par des dessins créés et modifiés qui ne sont pas liés aux lettres, et alors tu utilises la recherche citée pour la méthode mentionnée plus haut.

Ce genre d'obscurcissement indique une certaine ruse utilisée par certaines personnes, qui est de prendre pour chaque figure dessinée, la première lettre, ou la dernière lettre, ou encore la deuxième ou l'avant-dernière. Si le mot contient deux lettres, il peut arriver que la deuxième

lettre soit la même que la dernière, et que l'avant-dernière soit en fait la première lettre du mot.

L'extraction de ce type d'obscurcissement est très facile, et ne nécessite pas de recherche, puisque si tu examines l'obscur, tu prends les premières de ces lettres, ou les dernières, ou les deuxièmes, ou les avant-dernières. [La signification] apparaît si [le texte] était obscurci par ce type d'obscurcissement.

Du côté quantitatif, l'obscurcissement simple où les lettres conservent leur forme, est réalisé en doublant, triplant, *etc*. la forme des lettres : par exemple la lettre *a* en *aa*, la lettre *b* en *bb*, et cela pour toutes les lettres, ou seulement pour certaines. Tu reconnais ce type d'obscurcissement lorsque les lettres sont toujours repérées comme se répétant systématiquement.

Cette extraction est aussi très simple. Si tu soupçonnes que les lettres sont écrites dans une forme répétée, tu fusionnes les deux *a*, les trois *a etc*. en une seule lettre *a*, et tu appliques le même procédé pour les autres lettres.

Du côté quantitatif, l'obscurcissement simple, sans changement de figure des lettres, s'effectue en mettant une seule figure qui indique plusieurs lettres, comme les *bāa* (ب), *tāa* (ت) ou *ṯāa* (ث) qui sont indiquées comme une seule figure dans la calligraphie arabe. Si tu trouves que certaines lettres ont disparu, soit partout, soit en certains endroits – ce qui peut être soupçonné si le nombre des figures est inférieur au nombre des lettres de l'alphabet – les mots doivent être écrits différemment jusqu'à trouver le bon sens. Et tu appliques le même procédé au reste du texte jusqu'à ce que [les lettres] apparaissent toutes.

L'obscurcissement des lettres avec composition peut utiliser toutes les méthodes mentionnées précédemment, parce que la composition peut être infinie en raison de l'abondance des genres qui participent à la composition. Il n'en sera pas question ici, car notre but est la brièveté et la compacité.

La ruse utilisée pour trouver la composition réside dans l'utilisation de toutes les ruses mentionnées précédemment. Si le sens n'apparaît pas, sache qu'avec la composition, tu composes les méthodes avec lesquelles quelques parties sont apparues jusqu'à ce que l'obscurcissement soit levé. En fait la composition est la plus difficile à faire apparaître parmi tous les genres d'obscurcissement.

FREQUENCE ET ORDRE DES LETTRES DANS LA LANGUE ARABE.

Maintenant, puisqu'il en a déjà été question, qu'il me soit permis de mentionner l'ordre des lettres en abondance et en rareté dans la langue arabe. Je dis que *alif* (ا) est la lettre la plus utilisée dans la langue arabe, puis *lām* (ل), puis *mīm* (م), puis *hāa* (ه), puis *wāw* (و), puis *yāa* (ي), puis *nūn* (ن), puis *rāa* (ر), puis *'aīn* (ع), puis *fāa* (ف), puis *tāa* (ت), puis *bāa* (ب), puis

kāf (ك), identique en début, milieu ou fin, puis *dal* (د), puis *sīn* (س), puis *qāf* (ق), puis *ḥāa* (ح), puis *ǧīm* (ج), puis *ḏāl* (ذ), puis *ṣād* (ص), puis *śīn* (ش), puis *ḍād* (ض), puis *ḫāa* (خ), puis *ṯāa* (ث), puis *zāy* (ز), puis *ṭāa* (ط), *ḡīn* (غ), identique en début, milieu ou fin, puis *ẓād* (ظ).

Dans sept feuilles écrites en arabe, j'observe[12] :

alif ا 600	*lām* ل 437	*mīm* م 320	*hāa* ه 273
wāw و 262	*yāa* ي 252	*nūn* ن 221	*rāa* ر 155
'aīn ع 131	*fāa* ف 122	*tāa* ت 120	*bāa* ب 112
kāf ك 112	*dal* د 92	*sīn* س 91	*qāf* ق 63
ḥāa ح 57	*ǧīm* ج 46	*dal* ذ 35	*ṣād* ص 32
ḫāa خ 20	*śīn* ش 17	*ṭāa* ط 15	*ḡīn* غ 15

Je l'ai dit plus tôt : les voyelles sont les lettres les plus fréquentes dans toutes les langues, parce qu'elles sont la base de la parole. Dans ce tableau, nous remarquons que *lām* [consonne] est plus fréquente que *yāa* [voyelle] et *wāw* [voyelle], et aussi *hāa* [consonne], ce qui ne contredit pas ce que nous avons mentionné. C'est que les voyelles s'écrivent dans la calligraphie arabe lorsqu'elles sont longues, les voyelles courtes ne s'écrivent pas dans la calligraphie arabe, sauf lorsqu'elles se trouvent au début d'un nom, d'un adjectif ou de tout autre conjugué. Dans le mot *mohamed* (محمد) par exemple, il existe un *wāw* entre *mīm* et *hāa* qui n'apparaît pas dans l'écriture car c'est une voyelle courte. De même, le *alif* de *mohamed* qui est entre *hāa* et *mīm* et le *alif* qui est entre *mīm* et *dal*, sont courtes aussi. C'est pour cela qu'elles n'apparaissent pas dans l'écriture. Comme je l'ai montré dans mon livre *fi sina'ati achchi'ri* (في صناعة الشعر), « De la production poétique », les voyelles courtes sont toutes omises. C'est pour cela que les consonnes sont plus nombreuses dans la langue arabe.

LETTRES COMBINABLES ET NON COMBINABLES EN LANGUE ARABE

Je parle maintenant des lettres qui se combinent en langue arabe et de celles qui ne se combinent pas.

[12] Dans les statistiques d'al-Kindi, il y a trois lettres qui ont été omises, pour des raisons inconnues, ce sont *zāy* (ز), *ḍād* (ض) et *śīn* (ش).

Je dirais : les lettres qui ne se combinent pas sont les lettres fixes. Certaines d'entre elles ne se combinent ni avant, ni après, ou seulement avant, ou seulement après. Les lettres variables – je veux dire celles qui peuvent parfois être fixes, et parfois ajoutées, se combinent avec toutes les lettres avant et après, ou seulement avant, ou seulement après.

Je veux dire par lettres fixes celles qui se trouvent à la formation d'un nom ou à la racine d'un mot. Je veux dire racine quand je dis نُطْقٌ (*notqon* : résonne[13]) et mot [dérivé] quand je dis نَاطِقٌ (*naatiqon* : résonateur). Le mot dérivé peut dénoter un temps [conjugué], mais ici, dans le cas présent, il dénote un objet qui résonne toujours. Et le mot نَطَقَ (*nataqa* : il résonna) indique un objet qui était en train de résonner et يَنْطِقُ (*yantiqo* : il résonne) dénote qu'il résonne pendant un certain temps. Sauf que نَطَقَ (*nataqa*) et يَنْطِقُ (*yantiqo*) ne sont pas des mots [fixes] mais sont [des verbes,] conjugués à partir de mots. Seule la racine est composée des lettres fixes.

Dans la conjugaison du mot يَنْطِقُ (*yantiqo*), la lettre *yāa* (ي) ajoutée indique le futur où la résonnance aura lieu. Et également le *alif* (*ā*) court dans نَطَقَ (*nataqa*), situé entre *nūn* (ن) et *ṭāa* (ط), qui a remplacé la voyelle courte *wāw* (و) dans نُطْقٌ (*notqon*), indique un temps passé où la résonnance a eu lieu.

Et de même, dans le mot نَاطِقٌ (*naatiqon*), le *alif* (*a*) long situé entre *nūn* (ن) et *ṭāa* (ط) est ajouté et il remplace la voyelle courte *wāw* (و) dans نُطْقٌ (*notqon*).

Les lettres ajoutées sont donc celles qui sont attachées à un nom par conjugaison dans les temps, les nombres, le génitif, la comparaison, la cause, ou la succession, et ainsi de suite.

Les lettres fixes sont celles qui ne changent jamais et ne peuvent en aucun cas être des lettres ajoutées : *ṯāa*, *ǧīm*, *ḥāa*, *ḫāa*, *dal*, *ḏāl*, *rāa*, *zāy*, *śīn*, *ṣād*, *ḍād*, *ṭāa*, *ẓād*, *'aīn*, *ḡīn*, *qāf*.

Elles sont illustrées comme suit[14] :

ق	غ	ع	ظ	ط	ض	ص	ش	ز	ر	ذ	د	خ	ح	ج	ث

Les lettres variables qui peuvent être ajoutées ou fixes sont les suivantes : *alif* (أ), *bāa* (ب), *tāa* (ت), *sīn* (س), *fāa* (ف), *ka* (ك), *lām* (ل), *mīm* (م), *nūn* (ن), *hāa* (ه), *wāw* (و), *yāa* (ي).

Afin que tous nos sens participent à la compréhension des lettres, nous allons écrire ces lettres dans un tableau à deux lignes, chacune dans une ligne et nous écrivons les [lettres] fixes qui ne changent jamais dans la première ligne, et les [lettres] variables qui peuvent être ajoutées ou fixes

[13] NdT. : Le terme original a une signification proche de « prononcer ». Le terme « résonner » choisi ici est mieux adapté aux objets.
[14] NdT. : de droite à gauche.

dans la deuxième ligne. Les [lettres] fixes sont plus nombreuses, et certaines ne peuvent en aucun cas être combinées aux autres.

Lettres fixes	*ṯāa* ث	*Jim* ج	*ḥāa* ح	*ḫāa* خ	*dal* د	*ḏāl* ذ	*rāa* ر	*Zay* ز	*Sin* ش	*ṣād* ص	*ḍād* ض	*ṭāa* ط
	ẓād ظ	*gayn* ع	*ḡīn* غ	*qāf* ق								
Lettres variables	*alif* أ	*bāa* ب	*tāa* ت	*sīn* س	*fāa* ف	*ka* ك	*lām* ل	*mīm* م	*nūn* ن	*hāa* ه	*wāw* و	*yāa* ي

Les [lettres] variables peuvent se combiner avec toutes les lettres situées avant et après elles, sauf *sīn* (س) qui ne se combine pas avec *ṯāa, ḏāl, ṣād, ḍād, ẓād* ni avant ni après elle. En voici l'illustration :

sīn (س) ne combine pas avec	*ṯāa* (ث)	*ḏāl* (ذ)	*ṣād* (ص)	*ḍād* (ض)	*ẓād* (ظ)	
			ṣād (ص)	*ṭāa* (ط)	*ẓād* (ظ)	*Sin* (س)

Mais concernant les [lettres] fixes par nature, je veux dire celles qui se situent dans la première ligne :
– le *ṯāa* (ث) ne se combine pas avec les lettres *ḏāl* (ذ), *zāy* (ز), *ṣād* (ص), *ḍād* (ض), *ẓād* (ظ) et *sīn* (س) situées avant et après elle. En voici illustration :

ṯāa (ث) ne se combine pas avec	*ḏāl* (ذ)	*zāy* (ز)	*ṣād* (ص)	*ḍād* (ض)	*ẓād* (ظ)	*sīn* (س)

– le *ṯāa* (ث) ne se combine pas avec *śīn* (ش) s'il est situé avant. Il se combine avec si le *śīn* (ش) est situé avant. En voici illustration :

ṯāa (ث) ne se combine pas avec	*śīn* (ش)
ṯāa (ث) *śīn* (ش)	ششن *shathana* (grossir)

De même :
– le *ḏāl* (ذ) ne se combine pas avec les lettres *ṯāa* (ث), *zāy* (ز), *ṣād* (ص), *ḍād* (ض), *ṭāa* (ط), *ẓād* (ظ), *sīn* (س) ni avant ni après. En voici l'illustration :

ḏāl (ذ) ne se combine pas avec	*ṯāa* (ث)	*zāy* (ز)	*ṣād* (ص)	*ḍād* (ض)	*ṭāa* (ط)	*ẓād* (ظ)	*sīn* (س)

– le *ḏāl* (ذ) ne se combine ni avec *ṡīn* (ش), ni avec *ḡīn* (غ) s'il est situé avant. Il se combine avec si le *ṡīn* (ش) ou le *ḡīn* (غ) est situé avant le *ḏāl* (ذ). En voici l'illustration :

ḏāl (ذ) *ṡīn* (ش)	*ḏāl* (ذ) *ḡīn* (غ)
شذر *(shadhar,* pépite*)*	غذا *(ḡhaḏhan*, demain*)*

De même :
– le *zāy* (ز) ne se combine pas avec les lettres *ṯāa* (ث), *ḏāl* (ذ), *ṣād* (ص), *ẓād* (ظ), *sīn* (س) ni avant ni après. En voici l'illustration :

zāy (ز) ne se combine pas avec	*ṯāa* (ث)	*ḏāl* (ذ)	*ṣād* (ص)	*ẓād* (ظ)	*sīn* (س)

– le *zāy* (ز) ne se combine ni avec *ṡīn* (ش), ni avec *ḍād* (ض) s'il est situé avant elles. Il se combine avec si le *ṡīn* (ش) ou le *ḍād* (ض) sont situés avant le *zāy* (ز). En voici l'illustration :

zāy (ز) *ṡīn* (ش)	*zāy* (ز) *ḍād* (ض)
شزن (*shazan*, grossir)	ضوز (*Dawz*, mâcher)

– et le *zāy* (ز) ne se combine pas avec *ṭāa* (ط) si le *ṭāa* (ط) est située avant. Il se combine avec si le *zāy* (ز) est situé avant le *ṭāa* (ط). En voici l'illustration :

ṭāa (ط)	*zāy* (ز)
zāy (ز)	*ṭāa* (ط)

De même :
– le *ṣād* (ص) ne se combine pas avec les lettres *ṯāa* (ث), *ḏāl* (ذ), *zāy* (ز), *ḍād* (ض), *ṭāa* (ط), *ẓād* (ظ), et *sīn* (س). En voici l'illustration :

ṣād (ص) ne se combine pas avec	*ṯāa* (ث)	*ḏāl* (ذ)	*zāy* (ز)	*ḍād* (ض)	*ṭāa* (ط)	*ẓād* (ظ)	*sīn* (س)

– le *ṣād* (ص) ne se combine ni avec *ǧīm* (ج), ni avec *śīn* (ش) s'il se place avant eux. Il se combine avec si le *ǧīm* (ج) ou le *śīn* (ش) est situé avant le *ṣād* (ص). En voici l'illustration:

ṣād (ص) *ǧīm* (ج)	*ṣād* (ص) *śīn* (ش)
جص (*jass*)	شصيبة (*Shassībat*, le fond d'un puit)

– et *ṣād* (ص) ne se combine pas avec *dal* (د) si le *dal* (د) est situé avant, et se combine avec si le *ṣād* (ص) est situé avant. En voici l'illustration :

dal (د) *ṣād* (ص)	*ṣād* (ص) *dal* (د)
صدأ (*Sadaa*, rouille)	

De même :
– le *ḍād* (ض) ne se combine pas avec les lettres *ṯāa* (ث), *ḏāl* (ذ), *ṣād* (ص), *ṭāa* (ط), *ẓād* (ظ), *sīn* (س) et *śīn* (ش) ni avant, ni après. En voici l'illustration :

ḍād (ض) ne se combine pas avec	*ṯāa* (ث)	*ḏāl* (ذ)	*ṣād* (ص)	*ṭāa* (ط)	*ẓād* (ظ)	*sīn* (س)	*śīn* (ش)	Ni avant ni après

– le *ḍād* (ض) ne se combine pas avec *qāf* (ق) si *ḍād* (ض) se place avant *qāf* (ق). Il se combine avec si *qāf* (ق) se place avant *ḍād* (ض). En voici l'illustration :

ḍād (ض) *qāf* (ق)	*qāf* (ق) *ḍād* (ض)
قضأ (*qaddaa* = manger)	

– et le *ḍād* (ض) ne se combine ni avec *dal* (د), ni avec *zāy* (ز) si le *dal* (د) ou le *zāy* (ز) se placent avant le *ḍād* (ض). Le *ḍād* (ض) se combine avec le *dal* (د) et le *zāy* (ز) si le *ḍād* (ض) se place avant. En voici l'illustration :

dal (د) *ḍād* (ض)	*zāy* (ز) *ḍād* (ض)
ضد (*ḍid* = contre)	*ḍād* (ض) *zāy* (ز)

De même :
– le *ẓād* (ظ) ne se combine pas avec les lettres *ṯāa* (ث), *ḏāl* (ذ), *zāy* (ز), *ṣād* (ص), *ḍād* (ض), *ṭāa* (ط), *ǧīm* (ج), *dal* (د), *sīn* (س) ni avant ni après. En voici l'illustation :

ẓād (ظ) ne se combine pas avec	*ṯāa* (ث)	*ḏāl* (ذ)	*zāy* (ز)	*ṣād* (ص)	*ḍād* (ض)	*ṭāa* (ط)	*ǧīm* (ج)	*dal* (د)	*sīn* (س)	Ni avant ni après

– et le *ẓād* (ظ) ne se combine pas avec les lettres *ḥāa* (ح), *qāf* (ق), *śīn* (ش), *ḫāa* (خ) si *ẓād* (ظ) se place avant *ḥāa* (ح), *qāf* (ق), *śīn* (ش) ou *ḫāa* (خ). Il se combine avec si chacune de ces lettres se place avant le *ẓād* (ظ). En voici l'illustration :

ẓād (ظ) *ḥāa* (ح)	*ẓād* (ظ) *qāf* (ق)	*ẓād* (ظ) *śīn* (ش)	*ẓād* (ظ) *ḫāa* (خ)
ḥāa (ح) *ẓād* (ظ)	قظ (*qaddha* = stable, durable)	شظى (*shaddha*)	خظا (*khazza* = important, majeur)

De même :
– le *ǧīm* (ج) ne se combine pas avec les lettres *ṭāa* (ط), *ẓād* (ظ), *ḡīn* (غ) et *qāf* (ق) ni avant ni après. En voici l'illustration :

ǧīm (ج) ne se combine pas avec	*ṭāa* (ط)	*ẓād* (ظ)	*ḡīn* (غ)	*qāf* (ق)	ni avant ni après

– et le *ǧīm* (ج) ne se combine pas avec *ṣād* (ص) si *ṣād* (ص) se place avant *ǧīm* (ج). Il se combine avec si *ǧīm* (ج) se place avant *ṣād* (ص). En voici l'illustration :

ṣād (ص) *ǧīm* (ج)	*ǧīm* (ج) *ṣād* (ص)
جص (*jass*)	

De même :
– le *ḥāa* (ح) ne se combine pas avec les lettres *ẖāa* (خ), *'aīn* (ع) et *ġīn* (غ) ni avant ni après. En voici l'illustration :

ḥāa (ح) ne se combine pas avec	*ẖāa* (خ)	*'aīn* (ع)	*ġīn* (غ)

– et le *ḥāa* (ح) ne se combine pas avec *ẓād* (ظ) si *ẓād* (ظ) se place avant le *ḥāa* (ح). Il se combine avec si *ḥāa* (ح) se place avant *ẓād* (ظ). En voici l'illustration :

zāy (ز) *ḥāa* (ح)	حظ (*haz = chance*)

De même :
– le *ẖāa* (خ) ne se combine ni avec *ḥāa* (ح), ni avec *ġīn* (غ), ni avant ni après. En voici l'illustration:

ẖāa (خ) ne se combine pas avec	*ḥāa* (ح)	*ġīn* (غ)	Ni avant ni après

– et le *ẖāa* (خ) ne se combine pas avec *'aīn* (ع) et *ẓād* (ظ) si *'aīn* (ع) ou *ẓād* (ظ) se place avant le *ẖāa* (خ). Il se combine avec si *ẖāa* (خ) se place avant *'aīn* (ع) et *ẓād* (ظ). En voici l'illustration :

'aīn (ع) *ḥāa* (ح)	*ẓād* (ظ) *ẖāa* (خ)
نخع (*nakha'a*)	خاظ (*khazza*)

Et *dal* (د) ne se combine pas avec les lettres *zāy* (ز), *ṭāa* (ط), *ṣād* (ص), *ḍād* (ض) si le *dal* (د) se place avant *zāy* (ز), *ṭāa* (ط), *ṣād* (ص) ou *ḍād* (ض). Il se combine avec si *dal* (د) se place après *zāy* (ز), *ṭāa* (ط), *ṣād* (ص) ou *ḍād* (ض). En voici l'illustration :

dal (د) *zāy* (ز)	*dal* (د) *ṭāa* (ط)	*dal* (د) *ṣād* (ص)	*dal* (د) *ḍād* (ض)
الأزد (*alaazad*)	موطد (*mouttad*, confirmé)	صد (*ṣād,* empêcher)	ضد (*Did*, contre)

Et le *rāa* (ر), contrairement à toutes les autres lettres fixes, se combine avec toutes les lettres avant et après.

Et *śīn* (ش) ne se combine pas avec *ḍād* (ض) ni avant ni après. En voici l'illustration :

śīn (ش) ne se combine pas avec	*ḍād* (ض)

Et *śīn* (ش) ne se combine pas avec les lettres *zāy* (ز), *sīn* (س), *ṣād* (ص), *ṯāa* (ث), *ḏāl* (ذ) et *ẓād* (ظ) si le *sīn* (ش) se place avant le *zāy* (ز), le *sīn* (س), le *ṣād ṣād* (ص), le *ṯāa* (ث), le *ḏāl* (ذ) ou le *ẓād* (ظ), et se combine avec si le *śīn* (ش) se place après le *zāy* (ز), le *sīn* (س), le *ṣād* (ص), le *ṯāa* (ث), le *ḏāl* (ذ) ou le *ẓād* (ظ), et en voici l'illustration :

zāy (ز) *śīn* (ش)	*sīn* (س) *śīn* (ش)	*ṣād* (ص) *śīn* (ش)	*ṯāa* (ث) *śīn* (ش)	*ḏāl* (ذ) *śīn* (ش)	*ẓād* (ظ) *śīn* (ش)
شزب (*shazab*=s'éloigner)	شسع (*shasa'a*)	شص (*shass*)	شئن (*shaan*)	شذب (*shadhab*)	شظى (*shazza*)

De même :

– le *ṭāa* (ط) ne se combine pas avec lettres *ṣād* (ص), *ḍād* (ض), *ḏāl* (ذ), *ẓād* (ظ) et *ǧīm* (ج) ni avant ni après. En voici l'illustration :

ṭāa (ط) ne se combine pas avec	*ṣād* (ص)	*ḍād* (ض)	*ḏāl* (ذ)	*ẓād* (ظ)	*ǧīm* (ج)	Ni avant ni après

– et le *ṭāa* (ط) ne se combine pas avec *zāy* (ز) si le *ṭāa* (ط) se place avant le *zāy* (ز). Il se combine avec si le *zāy* (ز) se place avant *ṭāa* (ط). En voici l'illustration :

ṭāa (ط)	*zāy* (ز)
zāy (ز)	*ṭāa* (ط)

– et le *ṭāa* (ط) ne se combine pas avec la lettre *dal* (د), si le *dal* (د) se place avant le *ṭāa* (ط). Il se combine avec si le *ṭāa* (ط) se place avant le *dal* (د). En voici l'illustration :

dal (د)	*ṭāa* (ط)
موطد (*mouttad*)	

De même :
– le *'aīn* (ع) ne se combine pas avec les lettres *ḡīn* (غ) et *ḥāa* (ح) ni avant ni après. En voici l'illustration :

'aīn (ع) ne se combine pas avec	*ḡīn* (غ)	*ḥāa* (ح)

– et le *'aīn* (ع) ne se combine pas avec *ẖāa* (خ) si *'aīn* (ع) se place avant *ẖāa* (خ). Il se combine avec si *ẖāa* (خ) se place avant *'aīn* (ع). En voici l'illustration :

'aīn (ع)	*ẖāa* (خ)
بخع (*bakha'a*)	

De même :
– le *ḡīn* (غ) ne se combine pas avec les lettres *ḥāa* (ح), *ẖāa* (خ), *'aīn* (ع) et *ǧīm* (ج) ni avant ni en après. En voici l'illustration :

ḡīn (غ) ne se combine pas avec	*ḥāa* (ح)	*ẖāa* (خ)	*'aīn* (ع)	*ǧīm* (ج)

– et le *ḡīn* (غ) ne se combine pas avec les lettres *qāf* (ق) et *ḏāl* (ذ), si *qāf* (ق) et *ḏāl* (ذ) se placent avant *ḡīn* (غ), et se combine avec si *ḡīn* (غ) se place avant *qāf* (ق) et *ḏāl* (ذ). En voici l'illustration :

ḡīn (غ) *ḏāl* (ذ)	*ḡīn* (غ) *qāf* (ق)
غذا (*ḡhaḏhan* = *demain*)	نغق (*naghaq* = *croassement*)

De même :
– le *qāf* (ق) ne se combine pas avec *ǧīm* (ج) ni avant ni après. En voici l'illustration :

qāf (ق) ne se combine pas avec	*ǧīm* (ج)	Ni avant ni après

– le *qāf* (ق) ne se combine pas avec *ḡīn* (غ) si le *qāf* (ق) se place avant le *ḡīn* (غ) et se combine avec si le *ḡīn* (غ) se place avant le *qāf* (ق). En voici l'illustration :

qāf (ق)	*ġīn* (غ)
نغق (*naghaq* = c*roassement*)	

– et le *qāf* (ق) ne se combine pas avec *ḍād* (ض) si le *qāf* (ق) se place après le *ḍād* (ض), et se combine avec si le *ḍād* (ض) se place après le *qāf* (ق). En voici l'illustration :

qāf (ق)	*ḍād* (ض)
	قضم (*qaddam* = croquer)

Ainsi nous avons vu toutes les lettres qui ne se combinent pas. Les autres lettres se combinent entre elles. Pour que nous soyons plus clairs, nous allons illustrer ci-dessous les [lettres] combinables, comme nous l'avons fait ci-dessus lorsque nous avons répété pour chaque lettre celles qui ne se combinent pas avec elle.

J'ai déjà dit que les [lettres] variables se combinent avec toutes les lettres sauf *sīn* (س), et les lettres qui ne se combinent pas avec elles, ont été identifiées. Par contre, pour les lettres fixes que nous avons écrites quand elles se combinent entre elles et quand elles ne se combinent pas entre elles, j'écris également sa combinaison avec les [lettres] variables, à l'aide de Dieu, le bienfaisant et le protecteur contre les méfaits !

Et le *ṯāa* (ث) se combine avec *ṡīn* (ش) si *ṡīn* (ش) se place avant *ṯāa* (ث) et ne se combine pas avec sinon, et ne se combine pas avec les lettres *ḏāl* (ذ), *zāy* (ز), *ṣād* (ص), *ḍād* (ض) et *sīn* (س) ni avant, ni après. En voici l'illustration :

Nous disons que *ṯāa* (ث) se combine avec					*alif* (أ)	*bāa* (ب)	*tāa* (ت)	*ǧīm* (ج)	*ḥāa* (ح)	*ḫāa* (خ)	*dal* (د)	Avant et après
rāa (ر)	*'aīn* (ع)	*ġīn* (غ)	*fāa* (ف)	*qāf* (ق)	*kāf* (ك)	*lām* (ل)	*mīm* (م)	*bāa* (ن)	*hāa* (ه)	*wāw* (و)	*yāa* ي	

Et je dis que *ǧīm* (ج) se combine avec les lettres *yāa, wāw, tāa, ṯāa, ḥāa, ḫāa, dal, ḏāl, qāf, sīn, ṡīn, ḍād, 'aīn, fāa, ka, lām, mīm, nūn, hāa,* et se combine avec *ṣād* (ص) si *ǧīm* (ج) se place avant le *ṣād* (ص).

Et je dis que *rāa* (ر) se combine avec les lettres *ṯāa, ǧīm, ḫāa, ḥāa, dal, dhal, zāy, sīn, ṡīn, ṣād, ḍād, ṭāa, 'aīn, ġīn, fa, qāf, kāf, lām, mīm, nūn, hāa, wāw, yāa, alif, bāa, tāa* avant et après.

Et je dis que *zāy* (ز) se combine avant et après avec les lettres *alif, bāa, tāa, ǧīm, ḥāa, ḫāa, dal, rāa, 'aīn, ḡīn, fa, qāf, kāf, lām, mīm, nūn, hāa, wāw, yāa,* et se combine avec *śīn* (ش) et *ḍād* (ض) si *zāy* (ز) se place avant *śīn* (ش) et *ḍād* (ض). Il ne se combine pas avec sinon. Il se combine avec *ṭāa* (ط) si *zāy* (ز) se place avant *ṭāa* (ط). Il ne se combine pas avec sinon. Et *zāy* (ز) ne se combine ni avec *ṯāa* ni avec *ḏāl* ni avec *ṣād* ni avec *ḍād* ni avec *sīn*, ni avant ni après.

Et je dis que *śīn* (ش) se combine avant et après avec les lettres *alif, bāa, tāa, ǧīm, ḥāa, ḫāa, dal, rāa, ṭāa, 'aīn, ḡīn, fa, qāf, kāf, lām, mīm, nūn, hāa, wāw, yāa*. Il se combine avec les lettres *ṯāa, ḏāl, zāy, sīn, ṣād, ṭāa* si chacune de ces lettres se place après le *śīn* (ش). Le *śīn* (ش) ne se combine pas avec ces lettres sinon.

Et je dirai que *ṣād* (ص) se combine, avant et après, avec les lettres *alif, bāa, tāa, ḥāa, rāa, 'aīn, ḡīn, fa, qāf, kāf, lām, mīm, nūn, hāa, wāw, yāa*. Il se combine avec les lettres *ǧīm* (ج) et *śīn* (ش) si *ṣād* (ص) se place avant *ǧīm* (ج) et *śīn* (ش), et ne se combine ni avec *ǧīm* (ج) ni avec *śīn* (ش) sinon. Et *ṣād* (ص) ne se combine ni avec *ṯāa* (ث), ni avec *zāy* (ز), ni avec *sīn* (س), ni avec *ḍād* (ض), ni avec *ṭāa* (ط), ni avec *ẓād* (ظ), ni avant ni après.

[BIBLIOGRAPHIE]

(eds.) M. Mrayati, Y. Meer Alam, M.H. al-Tayyan, *Al-Kindi's Treatise on Cryptanalysis*, Riyadh, King Faisal Center for Research and Islamic Studies, 2003.

Rashed, R., *Œuvres philosophiques et scientifiques d'al-Kindi*, Leiden, E. J. Brill, 1997-98. Vol. I : *L'optique et la catoptrique d'al-Kindi*, vol. II : *Métaphysique et cosmologie* (avec J. Jolivet)

LES TRAVAUX DE LA SECTION DU CHIFFRE PENDANT LA PREMIERE GUERRE MONDIALE

Sophie DE LASTOURS[1]

La génération des combattants de 14-18 doit vous sembler bien lointaine : le dernier poilu français Lazare Ponticelli[2] est mort en 2008 à l'âge de 110 ans. Pour ma part, j'ai côtoyé cette génération, mes deux grands-pères ayant survécu à ce carnage, rescapés qu'ils étaient de Verdun, où 70 % de l'effectif des soldats français se sont trouvés engagés à un moment ou à un autre, la bataille ayant duré plusieurs mois.

Ayant eu la chance d'avoir été, en dehors des chiffreurs du monde de la Défense, la première à être autorisée à me plonger dans les archives françaises du Chiffre de 1914-1918, il me fallut bien admettre que la guerre s'était aussi déroulée à l'arrière, loin du front, et que les hommes qui l'avaient menée avaient pu tout autant en sortir meurtris, épuisés. Il fallut trois mois à Georges-Jean Painvin pour se remettre nerveusement de son intense travail intellectuel de concentration passé pour venir à bout du fameux « Radiogramme de la Victoire ». Il avait perdu quinze kilos.

Longtemps tenu secret, le rôle joué par le Chiffre lors de la guerre de 1914-1918 fut révélé en 1968, lors du cinquantenaire de l'armistice, au cours d'une rencontre historique entre le chiffreur allemand Fritz Nebel (1891-1977)[3], et le décrypteur français Georges-Jean Painvin (1886-1980), à l'occasion de l'inauguration d'une salle du musée des Invalides consacrée à la Première Guerre Mondiale. Dans la vitrine du Chemin des Dames furent placés deux documents concernant le « Radiotélégramme de la Victoire »,

---

[1] Historienne du renseignement, membre de l'Association des réservistes du chiffre et de la sécurité de l'information (ARCSI), membre du Conseil Supérieur de la Formation et de la Recherche Stratégique depuis 2010.

[2] On pensait jusqu'à tout récemment que les derniers combattants à avoir connu la Première Guerre Mondiale étaient le Britannique Harry Patch (1898-2009), le Canadien John Babcock (1900-2010), et l'Américain Franck Buckles (1901-2011), mais on a découvert depuis le Britannique Claude Choules, décédé le 5 mai 2011 à Perth en Australie, à l'âge de 110 ans. Il s'était engagé dans la Royal Navy à 14 ans en trichant sur son âge.

[3] La plupart des sites Internet le donnent pour mort en 1967.

ainsi commentés : « Pendant toute la durée de la Grande Guerre, les cryptologues français ont eu une supériorité incontestable sur leurs adversaires dans le domaine du décryptement des messages chiffrés ».

J'ai choisi de vous présenter les travaux de ces cryptologues français, menés dans un mouvement de fébrilité propre à la guerre, c'est-à-dire de manière non académique, dans une chronologie des événements où désorganisation, hasard, erreur, inconséquence de l'adversaire et compétence sont étrangement dépendants, et engendrent parfois de brillantes découvertes.

Je rappellerai d'abord ce qu'est le Chiffre, en présentant succinctement son vocabulaire. L'état des lieux de la cryptologie militaire à la veille de la Grande Guerre permettra de préciser cette supériorité cryptologique de la France en 1914 à travers les travaux de la Section du Chiffre, qui permettront de casser le système allemand UBCHI, puis le système ABC. Les deux exemples les plus manifestes de l'importance de la cryptologie lors de la Grande Guerre : le Télégramme Zimmermann et le Radiogramme de la Victoire, permettront de détailler le style de travail de décryptement.

Qu'est-ce-que le Chiffre ?

La cryptologie est la science des écritures secrètes. Elle étudie les méthodes, les procédés et les systèmes de chiffrement, et recherche les moyens de les décrypter. Comme toute technique, elle a son vocabulaire.

En voici quelques éléments de base :

Le *chiffrement* transforme un texte clair en un autre inintelligible, celui-ci devient un *cryptogramme.* Pendant la Première Guerre Mondiale, le chiffrement reste manuel, car on utilise le papier et le crayon, plus rarement des machines.

La *clé* est une convention orale ou écrite utilisée pour mener à bien les opérations de chiffrement et de déchiffrement.

Le *codage* est une transformation d'un texte en groupes de signes, de lettres, de chiffres, suivant des équivalences convenues.

Le *déchiffrement* est l'action de celui qui, recevant le message, connaît par avance les conventions fixées, et peut ainsi retrouver le message clair.

Le *décryptement* est l'action de celui qui, ignorant les conventions fixées, intercepte le cryptogramme par un moyen ou un autre et se livre à un travail d'investigation pour retrouver le message clair.

Le *cryptographe*, ou *chiffreur*, est un spécialiste qui se livre à un travail de chiffrement, ou de déchiffrement.

Le *décrypteur*[4] est un spécialiste qui se livre au travail de décryptement. Lorsque la clé n'est pas connue, il faut la trouver et se livrer pour cela à des recherches qui peuvent s'avérer longues et laborieuses.

Comment chiffrer ?

Le *système de transposition* change totalement l'ordre des lettres d'un message et le procédé de ce bouleversement n'est connu que par l'expéditeur et le destinataire. Par exemple PARIS devient ASPIR.

Le *système de substitution* est fondé sur le changement de la valeur des lettres. Chaque lettre du message en clair est remplacée par une autre lettre ou par un signe ou encore une image ou un nombre. Par exemple PARIS devient 12 4 45 7 89.

La substitution est simple si on utilise une unique échelle de chiffrement mais on peut compliquer les choses en ajoutant le chiffrement par code, c'est-à-dire que chaque mot du message en clair est traduit par un groupe de chiffres ou de lettres. On peut aussi combiner les deux méthodes, on parle alors de *surchiffrement.*

LA CRYPTOLOGIE EN FRANCE A LA VEILLE DE LA GRANDE GUERRE

Après la guerre de 1870 et la perte de l'Alsace-Lorraine, les militaires français comprennent qu'il faut protéger les communications dans tous les domaines : diplomatiques, militaires, commerciaux, *etc*.

Un curieux article nécrologique paru dans la presse allemande de 1879, lors du décès du capitaine Max Hering, chef du service télégraphique, avait appris aux militaires français quels services incontournables avaient été rendus à nos adversaires par l'absence d'un système de correspondance secrète fiable entre la partie de l'armée française à Paris et ses généraux en campagne hors de la capitale. C'est ce que relève Auguste Kerckhoffs[5] (1835-1901), linguiste et polyglotte, qui s'est intéressé à la cryptographie[6]. D'origine hollandaise, ce docteur ès lettres de l'université de Liège a publié en 1883 deux articles sur le sujet qui restent des références. Il y plaide

[4] C'est en 1943, par un décret signé de De Gaulle et Giraud, que l'on a officiellement séparé les fonctions de chiffreur et de décrypteur. Le Chiffre a été rattaché à l'Arme des transmissions en 1952. Le chiffrement est le chiffre de défense, et le décryptement est le chiffre d'attaque.

[5] Voir le chapitre « Du message chiffré au système cryptographique » p. 118.

[6] Kerckhoffs, « La cryptographie militaire ».

l'introduction de progrès indispensables qui vont contribuer à structurer ce domaine d'activités, et formule six règles de base dont la deuxième porte le nom officiel de « principe de Kerckhoffs ». Il y développe l'idée que la sécurité du système cryptographique ne doit dépendre que de la clé et non du secret d'une autre partie du système. Ces règles visent à obtenir un système matériellement incassable, la clé devant être facilement mémorisable, les cryptogrammes devant pouvoir être transmis par voie télégraphique par une seule personne[7]. Il faut absolument, selon lui, bannir la connaissance d'une longue liste de règles risquant de se révéler particulièrement délicates à utiliser lors d'une campagne militaire.

En 1872 a été créée la commission de télégraphie militaire, et en 1875, la Convention de Saint-Pétersbourg a reconnu l'emploi du chiffre dans les correspondances et les communications télégraphiques internationales. En 1881, le général Jules-Louis Lewal (1823-1908), ministre de la guerre n'hésitera pas à écrire : « La cryptographie est un auxiliaire puissant de la tactique militaire »[8].

En 1889, est créée la Commission du Chiffre, qui va avoir en charge la conception des codes et des systèmes de chiffrement. En 1890, le président de la Commission du Chiffre est le lieutenant-colonel Delanne. Lui succèderont en 1900 le général Pénel, puis de 1902 à 1912 le futur général Berteaux. Cette Commission est organisée en 1902 par le futur général Cartier[9], alors capitaine. C'est elle qui élabore les techniques de chiffrement et de décryptement, notamment par la mise au point de transpositions et de codes spécifiques. Le futur lieutenant-colonel Henry Olivari (1868-1955) en est membre de 1907 à 1912 et le futur général Marcel Givierge (1871-1931) de 1912 à 1914. Cartier, Olivari et Givierge vont constituer l'ossature du Chiffre en 1914. Georges-Jean Painvin les rejoint en cette année-là. Ils sont tous polytechniciens[10]. David Kahn, référence internationale de l'histoire de la cryptologie, préfaçant un ouvrage sur ce sujet, écrit que les années 1870-1914 sont celles où « la France domina toute la cryptologie du monde »[11]. Parallèlement, cette Commission est reconnue sur le plan gouvernemental :

> « Un renouveau des études cryptographiques […] devait permettre l'éclosion d'une véritable école cryptographique française particulièrement performante dans les années 1880-1900. Ainsi, deux des meilleurs spécialistes français de l'époque, le commandant Etienne Bazeries et le chef d'escadron Gaëtan Henri

[7] Voir le chapitre « Du message chiffré au système cryptographique » p. 107.
[8] Lewal, *Etudes de guerre*, tome 1. Le général Lewal fut ministre de la guerre en 1883 puis 1885. Cette citation figure également en exergue du texte de Kerckhoffs de 1883, « La cryptographie militaire ».
[9] Il recrutera également Paulier, Bessières, Latreille et Thévenin.
[10] Ribadeau-Dumas, « Chiffreurs et décrypteurs français de la guerre 14-18 ».
[11] Ollier, *La cryptographie dans l'armée française*, préface.

> Viarizio (de Viaris) di Lesegno, apportèrent-ils leur concours au succès du bureau du chiffre »[12].

Peu remarqués jusqu'ici, ces ingénieurs ont effectivement fait école auprès des membres de la Commission du Chiffre. Gaëtan de Viaris (1847-1901) « proposait de simplifier les vocabulaires télégraphiques composés de mots, de dictionnaires, en utilisant les mathématiques »[13]. Dans les années 1880, sur les traces d'Henry Mamy, il publie plusieurs articles sur la cryptographie dans la revue *Le Génie Civil*, où il cherche à synthétiser et à généraliser les méthodes de chiffrement polyalphabétique – à partir de Vigenère et Beaufort –, notamment par le recours à une écriture algébrique. Félix-Marie Delastelle (1840-1902), polytechnicien, qui, arrivé à la retraite, rédigea un *Traité élémentaire de cryptologie*, publié en 1902 chez Gauthier-Villars. Il y utilise une grille de chiffrement/déchiffrement semblable à celle du chiffre de Polybe : il repère les coordonnées de plusieurs lettres claires, mélange ces coordonnées, puis lit dans la grille des lettres chiffrées correspondant aux nouvelles coordonnées obtenues. Ce procédé est nommé tomogrammique[14]. C'est un mixage de codage par substitution et par transposition. Etienne Bazeries (1846-1931)[15] intervient, lui, dans les procédés de mécanisation. Il est connu pour avoir développé le cylindre qui porte son nom, version sophistiquée du cylindre de Jefferson[16]. L'*US Army* en fit bénéficier son appareil de chiffrement M-94.

Ainsi, « la période de la fin du XIX^{e} siècle fut sans doute une renaissance cryptologique pour la France qui s'inscrit dans l'optique d'une revanche de la défaite de 1870-1871 »[17].

La Commission du Chiffre devient officielle en 1912. Reconnue par le gouvernement, elle est rattachée au cabinet du ministre de la Guerre. Les ministères des Affaires étrangères et de l'Intérieur déploient également une activité cryptologique notable, la Commission interministérielle des Chiffres ayant été mise sur pied en 1909. L'historien Gérald Arboit affirme que :

> « Sur le plan international, [la cryptologie militaire française] dépassait les capacités allemandes et concurrençait celles de son allié britannique ; seules la Russie et l'Autriche la dominaient nettement »[18].

---

[12] Arboit, « La fin d'un monde : le bureau du chiffre du quai d'Orsay en 1904 ».
[13] *ibid.*
[14] Orancy et Pourroy, « Compte-rendu du T.I.P.E [...] : cryptage et problème de sac à dos ».
[15] Il a travaillé sur le fameux télégramme de Panizzardi qui joua un rôle clé dans l'affaire Dreyfus. Il fut rappelé lors du premier conflit mondial pour mettre ses qualités à contribution, ce qu'il fit avec succès. David Kahn le décrit comme « *the great pragmatist of cryptology. His theoretical contributions are negligible, but he was one of the greatest natural cryptanalyst the science has seen* ». Kahn, *The Codebreakers*, p. 244.
[16] Voir le chapitre « L'ancrage de la cryptologie dans les jeux d'écriture » p. 55.
[17] Hébrard, « La cryptologie dans l'histoire, Essai sur l'histoire secrète du chiffre », p. 137.

Une structure permanente devenait indispensable, notamment pour le décryptement des télégrammes étrangers que l'on archivait. Mais la nécessité d'une formation et d'une pratique systématiques ne s'imposera que progressivement. Le président de la Commission du Chiffre et ses membres avaient alors tous une autre affectation principale, et n'étaient appelés que pour la confection de codes et de dictionnaires de déchiffrement. Quelques spécialistes du chiffre et du décryptement avaient été toutefois formés. Ils suivaient en premier lieu un cours par correspondance avec exercices. En 1912, après plusieurs études et éliminations de méthodes jugées insuffisantes et trop compliquées, le système SD fut choisi, composé de transpositions avec diagonales. Des exercices furent aussi organisés pour des officiers chargés du Chiffre dans les états-majors des régions, les divisions et les places fortes, qui les pratiquaient régulièrement. Le Chiffre était également utilisé pendant les grandes manœuvres. À la veille de 1914, certains des meilleurs chiffreurs étaient pourtant employés ailleurs. On raconte que le colonel Mordacq (1868-1943), futur chef de cabinet de Clémenceau, retenait l'expert du Chiffre Paulier pour surveiller les leçons d'escrime ! Il n'empêche qu'à la veille de la guerre, le Chiffre français était techniquement prêt, même si le nombre d'officiers compétents restait insuffisant et que les états-majors ne comprenaient pas encore vraiment les enjeux de cette activité. Des réservistes furent aussi recrutés, dont plusieurs linguistes, à côté des mathématiciens.

On peut donc affirmer qu'à la déclaration de guerre, le 1er août 1914, la France jouissait d'une supériorité sur les autres puissances dans le domaine de la cryptologie. La Grande Guerre va exploiter cette discipline d'autant plus intensément que sont apparus de nouveaux outils de communication comme le téléphone, la télégraphie sans fil, la radio, et les premiers moyens de guerre électronique avec les écoutes et la radiogoniométrie. La multiplication des messages, amplifiée par la technique, l'étendue et la mobilité du front, oblige à employer le Chiffre.

La supériorité du décryptement sur les adversaires est avérée, ce qui, lié à des capacités d'interception radio efficaces, va permettre de prendre l'initiative dès le premier jour de la guerre. Le général Givierge, chef de la Section du Chiffre, parlera de « guerre cryptographique ». Le service des écoutes et celui des services de décryptement vont se développer de concert. Le renforcement progressif des précautions visant à conserver le secret va s'amplifier grâce au perfectionnement des systèmes de chiffrement et de la radiogoniométrie. Le général Louis Ribadeau-Dumas résume ainsi la situation :

[18] Arboit, « L'émergence d'une cryptographie militaire en France ».

> « Au déclenchement de la guerre, on a pu dire que le Chiffre français était techniquement prêt, mais d'une part les effectifs compétents dont il disposait étaient nettement insuffisants, d'autre part le décryptement n'était que virtuel. La mobilisation n'avait pas prévu d'affectation à la Section du chiffre et, au GQG et dans les grandes unités, un officier de l'état-major au plus avait été exercé au chiffre alors qu'il en aurait fallu deux ou trois (…). Ce n'est qu'en 1915, par persévérance et après des arrivées successives que Cartier et Givierge eurent les effectifs nécessaires à leur mission »[19].

LA SITUATION INTERNATIONALE AU DECLENCHEMENT DE LA GUERRE

En juillet 1914, les dépêches chiffrées donnant les instructions pour la mobilisation et la concentration des troupes avaient bien sûr été rédigées à l'avance et les clés correspondantes mises en place chez les destinataires. Mais le 26 juillet, au moment où on allait les envoyer, le gouvernement Viviani décida du recul des troupes à dix kilomètres en deçà de la frontière, espérant enrayer le processus de la guerre. L'état-major dut réviser ses instructions et le 27 juillet, tous les télégrammes durent être re-chiffrés et portés, non sans mal et en temps utile, aux PTT et à la Tour Eiffel !

La supériorité cryptologique de la France en 1914

En 1914, seul le chiffre austro-hongrois peut être comparé au chiffre français. Ce qui s'explique en partie par le nombre de langues utilisées en son sein.

La « clé anglaise » ou *Room 40*, nom donné à la suite du déménagement du service au Bureau 40 de l'Amirauté, va progresser à pas géants en peu de temps. Elle bénéficie de concours de circonstances comme celui-ci : au début de septembre 1914, le croiseur Magdeburg est coulé dans la Baltique. Le corps d'un officier de marine est repêché par les Russes quelques heures plus tard. Le cadavre tenait dans ses bras serrés, les documents du chiffre et des transmissions de la marine allemande, accompagnés des cartes de la mer du Nord et de la baie d'Heligoland. Laissons la parole à l'officier britannique concerné :

> « Le 6 septembre, l'attaché naval russe vint me voir. Il avait reçu un message de Petrograd, l'informant de ce qui s'était passé. L'amirauté russe avait pu, à l'aide de ces documents, déchiffrer, au moins partiellement certains messages de la marine allemande. Les Russes pensaient qu'en tant que puissance navale

[19] Ribadeau-Dumas, « Chiffreurs et décrypteurs français de la guerre 14-18 », p. 39.

> dominante, l'Amirauté britannique devait disposer de ces codes et de ces cartes. Si nous envoyions un navire à Alexandrovsk, les officiers russes qui détenaient ces documents les apporteraient en Angleterre »[20].

Les Russes sont traditionnellement de bons cryptologues, mais la rapidité de l'entrée en guerre va leur faire commettre de terribles erreurs dans ce domaine, en particulier la non-utilisation du chiffre à la bataille de Tannenberg en août 1914. Soljenitsyne[21] le décrit de façon poignante dans *La roue rouge : Premier nœud - Août 14*.

En 1914, le service du chiffre allemand dispose du même procédé de chiffrement pour toute l'armée, une uniformité pouvant se révéler n'être qu'une faiblesse.

Le système UBCHI

Fin novembre 1913, donc avant la guerre, le nouveau chiffre de l'armée allemande est l'UBCHI. Il s'agit d'un système assez simple à double transposition[22] avec changements de clés peu fréquents. Le 25 septembre 1914, Givierge envoie un cahier de chiffrement donnant trois clés permettant de déchiffrer un certain nombre de télégrammes anciens. Le système UBCHI est alors identifié et la première clé livrée entre les 27 et 30 septembre 1914. Il restera pourtant en service jusqu'en décembre 1914.

Les premières étapes conduisant à la solution avaient été franchies dès le 27 septembre par le commandant Olivari[23], extrayant les mots COMBLES [village de la Somme] et KAMPF [combat] de deux radiogrammes de quarante-quatre lettres provenant des écoutes de Reims. Un troisième radiogramme de quarante-quatre lettres provenant d'une autre source, arrivé dans la nuit du 27 au 28 septembre 1914, permit à l'interprète de réserve Schwab de vérifier par le mot SOFORT [aussitôt], l'exactitude des mots précédents. Le 29, Olivari ayant trouvé le mot ERCHEU [commune de la Somme], l'anagramme fut terminée à l'exception des lettres nulles[24].

Le 30 septembre, Schwab découvrit qu'un des chefs de section allemands s'appelait MEYDAN, nom relevé dans un annuaire d'officiers, ce qui lui permit d'identifier les lettres nulles de cet ordre chiffré. La clé fut alors

---

[20] Olivari, *Mission d'un cryptologue français en Russie*, p. 209.

[21] Les deux armées russes à Tannenberg ne disposaient pas du même code, car la rapidité de la déclaration de guerre ne leur avait pas laissé le temps d'harmoniser leur système.

[22] Rappelons qu'un système à double transposition produit un mélange de lettres d'un texte dans un ordre déterminé, de sorte que son rétablissement en clair donnait une anagramme du texte initial, laquelle nécessitait une deuxième transposition pour retrouver le code initial.

[23] De Lastours, *14-18, la France gagne la guerre des codes secrets*, p. 125.

[24] Les lettres nulles sont des lettres sans signification ajoutées au cryptogramme pour compliquer le décryptement.

reconstituée et de nombreux messages décryptés. On comprit alors qu'il y avait une clé unique pour toute l'armée allemande, que ce soient les états-majors d'armées, de corps d'armée, de divisions de cavalerie et d'infanterie ; restaient seulement à part quelques unités de cavalerie.

La deuxième clé trouvée avait demandé encore de longs tâtonnements et il avait fallu trente heures pour aboutir. Le fait d'avoir mis une fois quatre jours et une autre fois plus d'une journée pour terminer le décryptement, à partir de la connaissance d'une partie importante du texte clair, démontre qu'on ne possédait pas encore de méthode systématique complète de déchiffrement de l'UBCHI.

Du 20 au 24 octobre 1914, Olivari mit sur pied un procédé mécanique pour remonter automatiquement à la clé, à partir de la connaissance d'une portion du texte clair, l'opération se trouvant grandement facilitée par la connaissance des lettres nulles.

Le 22 octobre 1914, il y eut un changement de clé, mais Olivari, assisté de Schwab, la trouva en dix-neuf heures. Le 25, la nouvelle clé fut trouvée en une heure et demie, grâce à deux messages de vingt et une lettres. Dès lors, la méthode de décryptement se révéla au point.

Exemples de clés successivement découvertes :

1. MAGDEBURG AN DER ELBE [Magdebourg-sur-l'Elbe]
Cette clé a servi sur le front français du 2 au 9 août 1914. Elle fut relevée sur un cahier de chiffrement allemand, trouvé le 22 septembre à Fontenay-la-Joûte, et envoyée par le commandant Givierge de Paris à Bordeaux où elle parvint quelques jours plus tard.
2. SCHLACHT BEI SEDAN [bataille de Sedan].
Cette clé fut en service sur le front français du 9 au 13 septembre 1914.

Du système ABC à la dispersion des codes

Le 2 octobre, le journal « Le Petit Parisien » publia un reportage dans lequel des soldats affirmaient que les télégrammes allemands étaient lus. Il s'agissait là, en fait, de messages en clair parmi de nombreux autres ; mais quelques jours plus tard, ce fut au journal « Le Matin » de révéler que Thielt[25] en Belgique avait été bombardée à la suite du décryptement de messages annonçant la venue de Guillaume II dans cette ville.

En conséquence, les Allemands, ayant compris qu'on les lisait, changèrent le système de chiffrement UBCHI entre les 19 et 20 novembre

[25] Les troupes allemandes y avaient installé leur Quartier Général.

1914, et adoptèrent le système ABC, qu'ils utilisèrent jusqu'en janvier 1915, avant de le remplacer par un système ABCD, puis par divers autres codes.

Le colonel Olivari a rédigé, en 1921, des notes à l'intention du général Buat[26], lequel était alors chef d'État-Major général des armées françaises :

> « Il est à peine besoin d'indiquer que l'organisation et l'exploitation d'un service de renseignement sont aussi indispensables pour la préparation que pour la conduite de la guerre. Ce service de renseignement doit naturellement puiser à toutes les sources d'information possibles : ennemies, alliées, neutres, intérieures… »[27].

Dans ses mémoires écrits en 1932-33, baptisés *Souvenirs*, qui ont récemment été publiés après quelques modifications et avec de nombreuses notes sous le titre *Mission d'un cryptologue français en Russie* (1916), Olivari[28] précise les détails du chiffrement par code désigné sous le nom de « Havaube zwei »[29]. Il y donne à voir en détail l'aspect besogneux et les hésitations du travail de décryptement :

> « L'HAVAUBE ZWEI [...] devait être un code très général, peut-être à l'usage des consuls, que Paulier recopiait dans ses parties lisibles trouvées à Marseille ; mais il y avait des succédanés, si bien que la situation stratégique avait eu une répercussion cryptographique et, derrière le front stabilisé, les systèmes de campagne n'avaient plus la même importance ; il passait encore quelques UBCHI en retard et quant à l'ABC, c'était de la somme courante.
> Nous suivions Givierge de loin et nous en étions restés aux choses simples : la ponctuation, les météorologiques, la vitesse du vent, les DÄMPFER, les TRUPPEN, les PEILUNG.
> Bref, nous étions devenus un bureau secondaire, celui de l'« exploitation » et nous ne cesserons de répéter que si l'équipe numéro un, celle de l'« invention », a surtout besoin de posséder les caractéristiques et les particularités de la langue, l'équipe numéro deux, celle de l'« exploitation », doit avoir surtout une longue pratique et pouvoir perfectionner et élargir les résultats obtenus par la recherche, et nous méritions mieux.
> […] Comme dérivatif, j'avais la présence de Painvin qui me donna du courage. Le travail était tout de même passionnant, car c'était tous les jours du nouveau, en plus de cet HAVAUBE en quatre lettres, alors non encore éclairci.

---

[26] Ce général était persuadé qu'une autre guerre contre l'Allemagne serait à prévoir dans un délai de vingt à trente ans et qu'il fallait réorganiser l'armée française en favorisant les armes et techniques nouvelles.

[27] Olivari, *Mission d'un cryptologue français en Russie*, p. 387.

[28] Olivari a été envoyé en mission en Russie en avril 1916, afin « d'enseigner aux Russes certaines méthodes ».

[29] Il s'agissait d'un code diplomatique, un dictionnaire de chiffrement dont le « zwei » indique la deuxième édition, et que les décrypteurs travaillent à reconstituer.

> Ces communications avaient commencé à peu près en même temps que celles en trois lettres ; à partir de janvier, leur nombre s'égalisa, plus tard la vedette passa aux quatre lettres. Mes postes étaient toujours les mêmes : TQ et TH, l'un devait être voisin des exécutants : ANVERS ou BRUGES, l'autre BERLIN.
> On releva les groupes 1500 à 1800 ; cela ne donna rien ou à peu près. Le groupe le plus employé, AUDI, devait représenter PUNKT, STOP ou ABSATZ ; il n'y avait que treize lettres initiales.
> Le AN devait être dans les A, il n'y avait pas de D initial, donc pas de DÄMPFER et le destinataire qui se chiffrait dans les B pouvait être BERLIN. Il y avait en plus un paquet de AUDG, AUDM, *etc*. Sans doute des signes de ponctuation auxiliaires.
> Il fallait attendre la défaillance adverse.
> Vers le milieu de mars, j'étais de nuit, arriva un long radiogramme sous le chapeau HAVAUBE NORD ; les AUDI étaient remplacés par les AUNY et, en vertu de la convention internationale, les mots restaient prononçables.
> Dans le code de Givierge, nous lisions très bien les météorologiques ; la gaffe attendue se produisit : un météo fut passé en double, en trois lettres, et dans le Nord.
> Painvin s'attela au rapprochement, et presque en même temps Givierge nous communiqua un vieux météo en quatre lettres, dans lequel le groupe le plus fréquent était OABU. Je rétablis la concordance aussitôt, mais Painvin alla plus vite et il arriva aux constatations sensationnelles suivantes :
> - Le code devait avoir 100 000 lettres ou expressions, ce devait être le code des consuls.
> - La première partie, de A à N, correspondait à des radios et des noms géographiques.
> - Les signes OABU, UABU, *etc*. étaient des signes de ponctuation et leurs transposés.
> - Le code était ordonné à partir de O jusqu'à la fin.
> - Les chiffres étaient répartis en suivant le texte.
>
> On peut dire que par cette découverte, Painvin se plaçait du premier coup au premier rang »[30].

La cryptographie allemande va ainsi essayer les systèmes les uns après les autres : de systèmes de transposition, on passe à la transposition-et-substitution. Les Allemands procèdent logiquement, ce qui facilite les travaux des décrypteurs français. En avril 1916, Painvin décrypte l'un de leurs nouveaux systèmes de chiffrement à partir d'un message qu'un prince bavarois adresse à sa famille pour l'informer qu'il est blessé. En 1917, ils utilisent des grilles tournantes. Chaque grille de dimension différente porte un prénom : Anna, Berta, Clara, Dora, Emil, Franz. Ce procédé sera vite éclairci par les Français.

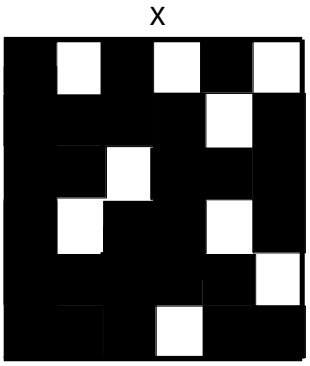
[30] Olivari, *Mission d'un cryptologue français en Russie*, p. 394-396.

La grille tournante, ou grille de Fleissner

Du nom du colonel autrichien Edouard Fleissner von Wostrovitz (1825-1888), qui l'a présentée en 1881 dans son ouvrage *Handbuch der Kryptrographie*, cette grille est un chiffrement par transposition. Ce procédé cryptographique est décrit dans les articles de De Viaris, ainsi que dans le roman de Jules Verne *Mathias Sandorf*[31] en 1885.

Le cryptogramme est disposé dans un carré, et en plaçant sur celui-ci une grille ajourée comprenant des trous convenablement placés, les premières lettres du message clair apparaissent. La suite du cryptogramme est lue de manière similaire en tournant successivement la grille d'un quart de tour.

L	L	T	E	A	S
I	L	E	I	S	S
B	Q	E	M	U	E
A	N	R	E	C	T
T	S	H	E	E	E
E	M	S	D	T	A



L'école allemande du Chiffre recrutait beaucoup par nomination et ne s'assurait pas toujours des meilleures compétences, ce que Fritz Nebel a expliqué quelques cinquante ans plus tard en 1968. Par manque d'expérience, les néophytes répétaient souvent les messages et multipliaient ainsi les possibilités de voir le système découvert. De plus, les radiogrammes parvenaient à leur destination avec beaucoup de retard.

Il n'existait pas en Allemagne d'école de cryptologie. La caste militaire avait été triomphante après la victoire de 1870, et croyait à une victoire en quelques semaines[32]. Le Grand-État-Major du Kaiser avait plutôt du mépris pour la cryptologie et pour les transmissions.

Le brouillage effectué par la Tour Eiffel contrariait le débit des messages allemands. Pour aller plus vite, certains messages cryptés étaient envoyés pour moitié en clair, ce qui fournissait des failles permettant de trouver le code utilisé.

[31] Voir le chapitre « l'ancrage de la cryptographie dans les jeux d'écritures » p. 55.

[32] Lors des journées d'études de Paris 8 sur « Les enjeux de la cryptographie », David Kahn a présenté sa thèse selon laquelle les vainqueurs d'une guerre tendent à minimiser l'importance de la cryptographie dans la stratégie militaire.

DEUX EXEMPLES DE L'IMPORTANCE DE LA CRYPTOLOGIE LORS DE LA GRANDE GUERRE

En dépit de l'absence de moyens de décryptement rapide, le travail des décrypteurs français a toutefois permis à la cryptographie de jouer un rôle effectif dans le déroulement de la guerre. Elle a notamment permis, sinon de gagner la guerre, au moins d'en abréger le cours et les dégâts. Deux cas sont tout à fait caractéristiques à cet égard vers la fin de la guerre : le télégramme Zimmermann et le fameux « Radiogramme de la Victoire ».

Premier exemple : Le télégramme Zimmermann

Le 16 janvier 1917, l'ambassadeur d'Allemagne au Mexique, le comte Johann Heinrich von Bernstorff, reçut un message chiffré constitué d'un paquet de mille groupes de nombres. Ce texte avait été chiffré avec le code diplomatique 0075, qui appartient à la famille des codes désordonnés. Il a été établi qu'il s'agissait du code affecté aux postes diplomatiques allemands de Vienne, Sofia, Constantinople, Bucarest, Oslo, La Haye, Lugano, Berne et Constantinople. Les cryptologues[33] n'arriveront qu'à une reconstruction du texte certes partielle, mais suffisamment édifiante pour avoir des conséquences radicales sur le déroulement de la guerre : cette reconstitution débouche finalement sur le basculement des États-Unis dans la guerre, ce dont ce télégramme tentait de prémunir l'Allemagne.

Comme le blocus anglais paralysait l'approvisionnement des Allemands, le Kaiser et ses généraux eurent l'idée de proposer une alliance militaire au Mexique, accompagnée d'un appui matériel pour qu'il entre en guerre contre les États-Unis, dans l'espoir de détourner leur attention de l'Europe, et d'éviter ainsi leur entrée en guerre aux cotés des Alliés. Les Mexicains avaient un contentieux important avec leur voisin du nord : l'expédition punitive du général Pershing contre Pancho Villa (1878-1923), restée dans les mémoires[34].

Le ministre allemand des Affaires étrangères, Arthur Zimmermann (1864-1940) – qui laissera son nom à ce télégramme historique – envoya une

[33] Notamment Nigel de Gray (1886-1951), issu de la société d'édition de William Heinnemann. Lors de la Seconde Guerre Mondiale, il sera affecté à Bletchley Park, ce manoir situé dans le nord de Londres qui accueillera à partir du 3 septembre 1939, une bonne partie des effectifs de la « Government Code and Cypher School », et où travaillera Alan Turing. Voir page suivante.

[34] John Joseph Pershing (1860-1948) est le seul général, avec George Washington, à avoir obtenu le grade de *General of the Armies*. En 1915, après la prise de pouvoir du général Huerta au Mexique – aidé par Pancho Villa –, Pershing reçut l'ordre de capturer ce dernier. Il fut également à la tête des troupes américaines engagées en France en 1917.

proposition en ce sens à son ambassadeur à Mexico. Afin de brouiller sa trace, le télégramme passa par la Suède neutre, puis par Buenos Aires. L'erreur allemande fut de ne pas prendre garde au fait que le câble reliant Stockholm à l'Amérique du Sud passait aussi par l'Angleterre.

Au sein de la section diplomatique britannique, le Bureau 40, service de l'Amirauté chargé du décryptement des codes ennemis, dirigé par l'amiral William Reginald Hall (1870-1943), constata que ce code était le code diplomatique habituel. Le théologien William Montgomery, qui était un cryptologue très reconnu, s'associa avec Nigel de Gray, éditeur de formation, pour parvenir à décrypter le fameux télégramme Zimmermann. Le télégramme partiellement décrypté sera transmis aux États-Unis dans cette version :

> « Nous déclencherons le premier février une guerre sous-marine totale. Malgré cela, nous essaierons que les États-Unis demeurent neutres. Au cas où cela serait impossible, nous proposerons au Mexique une alliance :
>
> > "Nous ferons la guerre ensemble, et nous ferons la paix ensemble. Nous accorderons notre appui financier au Mexique qui aura à reconquérir les territoires du Nord Mexique, du Texas et de l'Arizona. Vous superviserez tous les détails et en assumerez la responsabilité".
>
> Dès le commencement des hostilités avec les États-Unis, vous informerez le président (du Mexique) avec le maximum de secret et lui suggérerez qu'il doit de sa propre initiative, solliciter la participation immédiate du Japon et proposer sa médiation entre le Japon et nous-mêmes.
> Prière d'attirer l'attention que l'emploi de nos sous-marins donne maintenant la possibilité de pousser l'Angleterre à la paix en quelques mois.
>
> Zimmermann »

Le Secrétaire d'ambassade britannique fit parvenir ce brûlot au président des États-Unis, Woodrow Wilson (1856-1924). Certes, cela signifiait que les Allemands allaient tout de suite comprendre que leur code avait été cassé, mais c'était l'occasion attendue de faire entrer les États-Unis dans la guerre du côté des Alliés. L'attaque du paquebot britannique « Lusitania », torpillé par un sous-marin allemand en mai 1915 lors de la bataille de l'Atlantique, avait déjà eu un effet désastreux sur l'opinion. L'annonce de l'entrée en guerre des États-Unis aura lieu le 2 avril 1917.

Deuxième exemple : Le radiogramme de la victoire

Après la guerre, à la demande du général Mangin, alors ministre de la guerre, Painvin lui adressa, tout comme Olivari en 1921, un résumé de ses travaux[35]. Il y donne tous les détails sur l'A.D.F.G.V.X.

> « En mars 1918 apparurent des textes d'allure toute nouvelle, dont la principale caractéristique était d'être composée de groupes de cinq lettres, les différentes lettres employées se réduisant au nombre de 5 : A.D.F.G.X. et à partir du 1er juillet, au nombre de 6 : A.D.F.G.V.X.
> De mon côté, je me mis au travail dès son apparition, sans collaborateur, les officiers de mon service restant sur l'étude des codes de campagne. J'eus la très grande satisfaction dès le 5 avril, de reconstituer complètement le système en découvrant la clé utilisée par les Allemands le 1er avril.
> Je constatai rapidement que les clés changeaient chaque jour et j'eus l'occasion d'en reconstituer ainsi successivement une vingtaine environ. Ce système d'ailleurs ne fut employé par les Allemands que lors de leurs grandes offensives.
> J'ajoute que la découverte de la clé du 1er juin eut une importance toute particulière, car c'est par la traduction de l'un de ces télégrammes chiffrés à l'aide de cette clé, et qui fut déchiffré dans la nuit du 2 au 3, que l'on apprit le projet d'une nouvelle offensive allemande dans la région comprise entre Noyon et Montdidier[36].
> Cette offensive se déclencha le 10 juin, mais dans l'intervalle on avait pu prendre toutes dispositions pour y parer et elle fut un échec pour les Allemands »[37].

En 1918, les offensives de l'adversaire sur le front britannique, puis sur le front français de l'Aisne, respectivement le 21 et le 27 mai, menaçaient directement Paris. Nul ne savait alors où se produirait la prochaine offensive ennemie. Le travail de décryptement des messages allemands devait permettre de le faire savoir au commandement avec exactitude.

Parmi ces messages figure le fameux radiogramme adressé par le Haut commandement allemand à un état-major d'armée. Il fut repéré par la radiogoniométrie dans la région de Remaugies, à Tilloloy, à l'est de Montdidier, et décrypté par Painvin. Les divisions du général Mangin purent ainsi être concentrées dès le premier jour de juin face au point précis où se déclencha le 9 juin l'offensive allemande. Celle-ci échoua. La porte de Paris

---

[35] De Lastours, *14-18, la France gagne la guerre des codes secrets*, p. 225.

[36] Le texte clair du télégramme était « *Munitionierung beschleunigen punkt soweit nicht eingesehen auch bei tag* » (« hâter l'approvisionnement en munitions, le faire même de jour tant qu'on n'est pas vu »).

[37] Ce système correspond au maximum de complication des systèmes employés par les Allemands au cours de la guerre. Tous les états-majors alliés ont travaillé à sa reconstitution.

était définitivement fermée à l'ennemi. « Pour nous, celle de la victoire allait s'ouvrir », écrit Painvin.

LE QUOTIDIEN LABORIEUX DU DECRYPTEUR

Une caractéristique du travail des cryptologues est qu'il est mené anonymement dans le plus grand secret, de manière extrêmement laborieuse, voire obsessionnelle. Ils sont pourtant dans l'œil du cyclone et subissent un stress permanent. Leurs noms et leur travail restent la plupart du temps inconnus du grand public. N'oublions pas de mentionner que le chiffre fut fatal à Mata Hari, qu'un message allemand décrypté fit fusiller[38]. Il s'agit pour les principaux de Givierge[39], Painvin, Olivari, Paulier, Thévenin[40], Desjardins… Rendons leur hommage ici. Quant aux succès de la cryptologie française pendant la Grande Guerre, Painvin devait écrire quelques années plus tard : « J'ai la conviction que les Allemands, pendant la Première Guerre Mondiale, n'ont jamais déchiffré nos propres télégrammes dans une proportion comparable à celle où nous avons déchiffré les leurs »[41].

Un autre type de message allemand semble avoir joué un rôle important vers la fin des hostilités, qui témoigne bien des maladresses des services allemands. Alexis Tendil[42], opérateur d'écoute sur le front, transcrivait habituellement des messages chiffrés qui n'avaient pas de sens pour lui. Il n'avait pas à monter à l'assaut, comme tant de ses compagnons, mais, affecté au front, près du Chemin des Dames, il fut tout aussi exposé qu'eux aux effroyables bombardements et ne connut pas de bien meilleures conditions de vie. Jour après jour, il montait la garde sur les ondes, scrutant le spectre des fréquences à la recherche des émissions de l'ennemi. Il tomba un jour sur un message non chiffré. C'était une longue suite de caractères qu'il sut identifier comme de l'allemand. L'estafette à laquelle il avait remis le résultat de ses interceptions, revint de l'état-major en lui disant : « Bon sang ! Je ne sais pas ce que tu as pris, mais quand je leur ai donné ton papier, ils sont vite devenus comme fous.... ». Il apprendra un peu plus tard par son supérieur que ce message provenait de Max de Bade, le Chancelier de l'Empire allemand, s'adressant au Vatican. On y lisait que l'Allemagne

---

[38] De Lastours, « Le chiffre et les femmes ».

[39] Le Général Marcel Givierge, polytechnicien polyglotte, avait été mis, selon ses Mémoires : « par hasard par le ministre à la disposition du chef de la Sûreté pour des traductions secrètes », puis dans le décryptement. De Lastours, *14-18, la France gagne la guerre des codes secrets*, pp. 245-248.

[40] Général Ribadeau-Dumas, « Le général de division Louis Thévenin (1870- 1948) et la Commission de cryptographie militaire ».

[41] De Lastours, « Le chiffre et les femmes », p. 39.

[42] Alexis Tendil est mort à 109 ans.

allait demander l'armistice[43]. Cette nouvelle d'importance procura un avantage déterminant à notre état-major. On prétend que cette information permit d'économiser des milliers de vies.

Le Chiffre et l'ensemble des services de renseignement accompagnent ainsi les campagnes militaires comme les trois Parques. Elles commencent, se déroulent et se terminent avec lui. Le 11 novembre 1918, il aura le dernier mot.

Un contrôleur honoraire de la police est alors un témoin privilégié des pourparlers de Rethondes[44] puisqu'il voyage en tant qu'attaché au bureau des services spéciaux du Grand Quartier Général, dans le train qui conduit les plénipotentiaires allemands. Il consigne toutes ses observations du 6 au 11 novembre 1918 :

> « Le matin du 10 novembre, les deux trains se trouvent toujours immobiles et parallèles. Deux nouveaux officiers de l'armée impériale surviennent bientôt, deux lieutenants chiffreurs Rohde et Pistch ainsi que leur chef, le major Brinnkramm [NdA. sic ! Ce ne sont pas des noms chiffrés]. Les plénipotentiaires doivent être mis au courant de ce qui se passe en Allemagne. Une dépêche du Maréchal Hindenburg venant de lui être remise, la délégation allemande demande le temps nécessaire pour la faire déchiffrer : le repas du soir est le plus triste de tous. La fièvre monte à nouveau. Nous ne dormons plus. 11 novembre 1918 ! Vers 2 heures 15 les parlementaires, le col de leur manteau relevé, gagnent le train du Maréchal. 5 heures 10 : L'armistice a été signé ! »[45]

Les généraux vainqueurs oublièrent vite qu'ils avaient mobilisé jusqu'à cinquante-cinq mille sapeurs télégraphistes pour assurer leurs communications dans un conflit pourtant relativement statique. Ils ont tout autant oublié que la radio (TSF) avait rendu d'immenses services grâce au Général Ferrié auquel la tour Eiffel dût sa survie. La proposition de ce visionnaire, de constituer une arme dédiée à cette fonction, resta lettre morte.

En matière de cryptographie, les rivalités au sein de la Section du Chiffre[46], et la véritable guerre fratricide que se livraient d'un côté les Alliés, et de l'autre, les responsables français des écoutes et du décryptement, n'arrangèrent pas les choses. Mais nos spécialistes, malgré tous ces handicaps, participèrent à la formation des premières équipes américaines[47] en 1920.

---

[43] Desvignes, « Alexis Tendil, pionnier de la guerre électronique durant la Grande Guerre ».
[44] La fameuse clairière de Rethondes, de son nom officiel « Clairière de l'Armistice », se trouve dans la forêt de Compiègne.
[45] De Lastours, *La victoire à la clef*, p. 49-50.
[46] Olivari notamment eut à en souffrir en Russie, lors de sa mission aux contours mal définis.
[47] Blondé, *Historique des transmissions de l'armée de terre, des origines à 1940*, p. 112.

CONCLUSION

Le Chiffre de 1914-1918 fut donc une véritable clé du champ de bataille. N'a-t-on pas affirmé que l'on pourrait écrire une histoire des conflits par la seule étude des messages ou dépêches décryptés ? La cryptographie ne doit pas ses succès d'alors à ses seules capacités propres, dont la mise en œuvre reste, on l'a vu, laborieuse et délicate. Elle est surtout intégrée dans un ensemble plus vaste, celui des services du renseignement, dont le soutien est indispensable pour recevoir et entériner la validité des messages décryptés : il est vital que ces messages soient transmis rapidement au commandement, et suffisamment pris au sérieux pour que les informations reçues soient prises en compte. Le secret que cache un message chiffré doit s'emboîter, tel une poupée russe, dans l'autre secret que constitue le renseignement dans sa globalité. C'est autour du renseignement que sont coordonnés tous les moyens d'information alors à disposition : télégraphie, téléphone et TSF. La Première Guerre Mondiale va d'autant mieux exploiter la cryptographie que le progrès met de nombreux outils à la disposition des belligérants. Trente ans après l'énonciation des lois de Kerckhoffs, on peut donc considérer que la cryptographie a connu une première étape de sa mutation : elle s'est dotée de cette capacité que Kerckhoffs appelait de ses vœux, de traiter non plus seulement les échanges interpersonnels, mais les « systèmes cryptographiques ».

L'organisation existe bel et bien, même si les moyens techniques de la cryptographie, du « papier-crayon » au pigeon voyageur, restent en grande partie artisanaux. Pendant la Grande Guerre, la France a utilisé jusqu'à 130 000 de ces volatiles. On leur a avec justice consacré un monument à Lille… Le pigeon voyageur porteur de messages secrets sera en quelque sorte une arme de guerre[48] jusqu'aux lendemains de 1945.

En moins d'un siècle, la mutation de la cryptographie deviendra beaucoup plus manifeste, tant dans les moyens de chiffrement que dans le profil des chiffreurs. Chiffreurs et décrypteurs vont rapidement intégrer les mathématiques, et glisser du chiffre manuel « crayon-papier » de la Première Guerre aux machines de la Seconde Guerre. De l'*Enigma*, on passera alors à *Red*, *Purple*, à la KL 7 à rotors de l'OTAN puis, plus tard à *Myosotis* en France, pour arriver au chiffre électronique intégré dans les moyens de communication et les terminaux, et bientôt le chiffre quantique[49].

[48] De Lastours, « Petite histoire du pigeon voyageur ».
[49] Voir le chapitre « La cryptologie gouvernementale française » p. 153.

BIBLIOGRAPHIE

Arboit, G., « La fin d'un monde : le bureau du chiffre du quai d'Orsay en 1904 », *Centre Français de Recherche sur le Renseignement, Note historique n° 10,* janv. 2008. http://www.cf2r.org/fr/notes-historiques/la-fin-un-monde-le-bureau-du-chiffre-du-quai-orsay-en-1904.php.

— « L'émergence d'une cryptographie militaire en France », *Centre Français de Recherche sur le Renseignement, Note Historique n° 15*, juillet 2008. http://www.cf2r.org/fr/notes-historiques/lemergence-dune-cryptographie-militaire-en-france.php.

Bardin, E.-A. (Général), *Dictionnaire de l'Armée de Terre*, Paris, Perrotin, 1843.

Baud, J. (Colonel), *Encyclopédie du renseignement et des services secrets*, Paris, Lavauzelle, 1997.

Blondé, (Général), *Historique des transmissions de l'Armée de Terre*, Tome I : *des origines à 1940*, Versailles, Etablissement d'impression de l'Armée de Terre, s.d. (après 1995).

Cattieuw, A. (Colonel), « Rétrospective de la cryptologie de 1928 à nos jours », *Bulletin de l'ARCSI (Association des Réservistes du Chiffre et de la Sécurité de l'Information)*, n° 26, 1998-1999.

Delastelle, F., *Traité élémentaire de cryptographie*, Paris, Gauthier-Villars, 1902.

de Lastours, S., *14-18, la France gagne la guerre des codes secrets*, Paris, Tallandier, 1998.

— « La victoire à la clef », *Bulletin de l'ARCSI*, 1998, n° 26, p. 49-50.

— « La cryptologie et le renseignement », *Stratégique*, 1999/1, n° 73 (1), http://www.stratisc.org/strat_073_bDeLastourdoc.html.

— « Le chiffre et les femmes », *Bulletin de l'ARCSI,* 2008, n° 35, pp. 34-39.

— « Petite histoire du pigeon voyageur dans la Grande Histoire ou à quand le pigeon chiffreur ? » *Bulletin de l'ARCSI*, 2011, n° 38, pp. 67-81.

Desvignes, J.-L. (Général), « Alexis Tendil, pionnier de la guerre électronique durant la Grande Guerre », *Bulletin de l'ARCSI*, 2005, n° 33, pp. 89-91.

De Viaris, G., « Cryptographie », *Le Génie Civil*,1888, tome XXIII, pp. 24-2, pp. 38-39, pp. 55-56, pp. 72-75, pp. 84-88, pp. 104-107.

Hébrard, P., *La cryptologie dans l'histoire : essai sur l'histoire secrète du chiffre, de l'Antiquité à la Première Guerre Mondiale*, Paris, ARCSI, mars 2001, vol. 1.

Kahn, D., *The Codebreakers, The Comprehensive History of Secret Communication from Ancient Times to the Internet*, New York, Scribner, 1996.

Kerckhoffs, A., « La cryptographie militaire », *Journal des sciences militaires,* vol. IX, janv. 1983, pp. 5-38 ; vol. X, fév. 1883, pp. 161-191.

Lewal, J.-L. (Général), *Etudes de guerre : tactique des renseignements*, Paris, éd. Baudouin, 1881, 2 vols.

Mamy, H., « La Cryptographie », *Le Génie Civil*, 1886, tome IX, pp. 203-206, pp. 217-219, pp. 235-238,

Olivari, H. (Colonel), *Mission d'un cryptologue français en Russie (1916)*, Paris, L'Harmattan, 2009.

Ollier, A., *La cryptographie dans l'armée française 1881-1914*, Panazlo, Lavauzelle, 2002.

Orancy, S. et Pourroy, L., « Compte-rendu du T.I.P.E sur une étude bibliographique; sujet n° 14 : cryptage et problème de sac à dos », Site Internet : homepages.laas.fr/echanthe/doc/TIPE_ cryptage.pdf.

Porch, D., *Histoire des services secrets français*, Paris, Albin Michel, 1995-1997, 2 vols.

Ribadeau-Dumas, L. (Général), « Essai d'historique du Chiffre », *Bulletin de l'ARC*, 1974, n° 2, pp. 25-66.

— « Chiffreurs et décrypteurs français de la guerre 14-18 », *Bulletin de l'ARCSI*, n° 27, 1999, pp. 33-53.

— « Le général de division Louis Thévenin (1870-1948) et la Commission de cryptographie militaire », *Bulletin de l'ARCSI*, 2000, n° 8, pp 49-54.

Soljenitsyne, A., *La roue rouge : Premier nœud – Août 14*, Paris, Fayard, 1983.

Verne, J., *Mathias Sandorf*, Paris, J. Hetzel & Cie, 1885.

von Wostrovitz, E. B., *Handbuch der Kryptographie, Anleitung zum Chiffriren und Dechiffriren von Geheimschriften*, Wien, Selbsverlage des Verfassers, 1881.

DU MESSAGE CHIFFRE AU SYSTEME CRYPTOGRAPHIQUE

Marie-José DURAND-RICHARD[1]

Le décryptement d'un message chiffré en mode polyalphabétique par le mathématicien anglais Charles Babbage (1791-1871) en 1846 marque sans doute un premier rapprochement entre cryptologie et mathématiques. Et ce rapprochement peut paraître continu à la lecture des « lois de Kerckhoffs », telles qu'elles sont aujourd'hui présentées, sous forme mathématisée, pour introduire les systèmes de sécurité dans l'enseignement de la cryptologie. Pourtant, Auguste Kerckhoffs (1835-1901) ne faisait alors qu'énoncer en 1883, un ensemble de critères cherchant à caractériser un système cryptographique. Plaquer l'état de nos connaissances présentes sur l'histoire de la cryptologie des 19e et 20e siècles est donc un raccourci brutal qui ne permet pas de comprendre comment s'est opérée la rencontre entre cryptologie et mathématiques. Celle-ci n'est pas seulement le fruit d'une convergence technique ou opératoire. Elle a été marquée par une transformation profonde des significations épistémologiques et sociales, tant des conditions d'exercice de la cryptologie que de celles du calcul. Ainsi, au temps de César, le chiffre qui porte son nom[2] ne s'énonçait pas en termes d'addition modulo 26 sur l'ensemble des permutations dans un ensemble à 26 éléments ! Et l'énoncé de Kerckhoffs ne contient aucune référence à une quelconque écriture ensembliste ou fonctionnelle qui n'est pas encore advenue, et qui mettra du temps à pénétrer le milieu cryptographique. La référence à ces auteurs ne cherchera pas ici à repérer des précurseurs ou des anticipations fructueuses de la situation actuelle, mais à percevoir les enjeux spécifiques d'un tel rapprochement.

Au 19e siècle, les pratiques cryptologiques restent le fait de manipulations scripturales. Elles vont d'abord évoluer par le biais de pratiques matérielles nouvelles, suscitées par la mise en place de réseaux

[1] mjdurand.richard@gmail.com. Université Paris Diderot, Sorbonne Paris Cité, SPHERE-REHSEIS, UMR 7219, CNRS, F-75205 Paris, France.

[2] Voir le chapitre « L'ancrage de la cryptologie dans les jeux d'écriture » pp. 24-25.

techniques – télégraphe, téléphone, téléscripteurs, *etc.* – qui feront système bien avant que la théorie des systèmes ne s'empare des théorisations informatiques ou cybernétiques au milieu du 20e siècle. Or, l'existence de ces réseaux, qui relève de la raison d'être de cette cryptologie en voie de mathématisation, se trouve pour le moins masquée – ou reste pour le moins implicite – dans les présentations générales des dernières avancées de la cryptologie. Celles-ci préfèrent se référer aux échanges inter-individuels entre Alice et Bob[3]. Référence trompeuse s'il en est, qui traduit des échanges collectifs d'ordre commercial ou militaire en histoires personnelles ! Ce chapitre vise donc à expliciter les conditions de mathématisation de la cryptologie liées à l'existence de ces réseaux de communication.

Ainsi la mathématisation de la cryptologie se trouve-t-elle médiatisée par la nécessité de travailler matériellement sur des systèmes de codes liés à des systèmes techniques nouveaux. C'est bien la naissance du télégraphe qui modifie radicalement l'exercice de la cryptographie, entre les savantes recherches privées de Charles Babbage et l'article d'Auguste Kerckhoffs sur *La cryptographie militaire*. Lorsque Gilbert S. Vernam (1890-1960), ingénieur à la section télégraphique de *l'American Telephon & Telegraph Company* (AT&T) à Manhattan, conçoit son système à bandes chiffrantes au sortir de la Première Guerre Mondiale, il travaille à la sécurité des téléscripteurs. Il ne mobilise pas l'addition sur le groupe {0, 1} d'une théorie des groupes finis encore inexistante ! Il travaille sur des impulsions électriques et sur des rubans perforés dont les trous et les espaces correspondent aux signes du code Baudot[4], et c'est bien la matérialité technique qui constitue le support de ses pratiques et de sa réflexion. Claude E. Shannon (1916-2001) travaille initialement dans un tout autre contexte – celui de l'optimisation du fonctionnement d'une machine destinée à résoudre les équations différentielles[5] – lorsqu'il remarque, en 1937, que les connexions d'un circuit électrique peuvent s'exprimer dans les mêmes termes qu'une algèbre de Boole. Ingénieur et mathématicien, Shannon élabore un nouveau langage, exprimant le fonctionnement de ces circuits en

[3] De très nombreux manuels de cryptologie, y compris des exposés de chercheurs, ainsi que les ouvrages de vulgarisation, présentent les échanges cryptographiques comme devant préserver le secret (bien souvent amoureux) entre deux acteurs, nommés Alice et Bob, parfois Bernard, et laissent implicite la question de la sécurité du système tout entier. Voir par exemple Rémi, « La cryptographie à clé publique », p. 48 ; Misarsky, « Cryptanalyse et spécification des schémas de redondance RSA », p. 8.

[4] Ce code, dit code *Murray* par les Anglo-saxons, est aussi appelé code télégraphique ou alphabet international (AI) n° 2, ou code CCITT n° 2. C'est un des premiers codes binaires ainsi mis en œuvre sur une machine.

[5] L'analyseur différentiel a été conçu et construit au MIT (*Massachusetts Institute of Technology*) par Vannevar Bush (1890-1974) en 1927. Il a rapidement été reproduit en Angleterre, à Manchester, puis à Cambridge, par Douglas R. Hartree (1897-1958).

termes mathématiques. Mais c'est bien en tant que cryptologue qu'il élabore sa célèbre théorie de l'information au sortir de la Seconde Guerre Mondiale. Quant au cryptologue Horst Feistel (1915-90), il est déjà chargé d'élaborer des algorithmes cryptographiques chez IBM (*International Business Machines*) lorsqu'il conçoit ses algorithmes de chiffrement par blocs, qu'il exprime en termes d'algèbre binaire. Ce sont ces textes que j'ai retenus pour mieux cerner quelques moments décisifs de la mathématisation de la cryptologie associés à la maîtrise des réseaux de communication.

BABBAGE ET LE DECRYPTEMENT DU CHIFFRE DE VIGENERE

Charles Babbage est aujourd'hui surtout reconnu comme mathématicien. Il est souvent considéré comme un pionnier en matière d'ordinateur – une projection rétro-historique parmi tant d'autres ! – parce qu'il a conçu les plans d'une machine, *The Analytical Engine*, à la suite de sa *Difference Engine* partiellement construite. En effet, la « machine analytique » peut être assimilée à une calculatrice automatique à programme externe, dont la structure opératoire[6] est effectivement la même que celle d'un ordinateur classique d'architecture von Neumann, distinguant et isolant mémoire, organes de calcul, et organes de contrôle, organes d'entrée et de sortie. Mais Babbage est également l'auteur de recherches trop méconnues en cryptologie.

Les travaux de décryptement de Babbage

Le manuscrit aujourd'hui conservé à la *British Library*, « Philosophy of Deciphering »[7], témoigne d'une activité constante en ce domaine, et au moins reconnue par ses pairs, de 1831 à 1870. Il accumule des matériaux destinés à une publication, à laquelle il semble pourtant renoncer faute de temps[8]. Fondateur de la *Statistical Society* en 1834, il échange avec le célèbre astronome et statisticien belge Adolphe Quetelet (1796-1874) dès 1831 sur l'analyse des fréquences des différents langages[9]. Il établit des tableaux de fréquences des lettres en analysant d'importants ouvrages : pour

[6] Durand-Richard, « Charles Babbage : de l'école algébrique anglaise à la 'machine analytique' ».
[7] Babbage, Add. Mss 37 205.
[8] Babbage fait de nombreuses références à cet ouvrage qu'il voudrait publier, et au temps qui lui manque, trop absorbé sans doute par la conception et les tentatives de fabrication de ses machines. Babbage, Add. Mss 37 205, folios 211, 214.
[9] Babbage, « On the proportion of Letters Occurring in Various Languages ». Quetelet traduit cette lettre en français et la publie en 1831. Add. Mss 37 205, folio 230.

la langue anglaise, les *Sermons* de Hugh Blair (1718-1800) publiés en 5 volumes de 1771 à 1801, et pour la langue allemande, *Die Phosphorescenz der Körper* (1811-15) de Placidus Heinrich (1758-1825)[10]. Babbage offre la première trace du décryptement d'un message chiffré par une substitution alphabétique de type Vigenère, même si ce résultat reste en partie ignoré, au moins jusqu'à ses échanges avec un certain Mr Thwaites dans les colonnes du *Journal of the Society of Arts* en 1854-55. Cependant, bien que les idées de Babbage soient innovantes, aussi bien en cryptologie qu'en mathématiques, il reste un auteur charnière, un « gentleman amateur » qui élabore ses machines dans l'atelier qu'il a fait équiper dans sa propre demeure, un « polymath » qui se préoccupe de l'harmonie entre tous les aspects de la « philosophie naturelle », plutôt que de chercher la spécialisation des disciplines. S'il enquête longuement pour son *Treatise on the Economy of Machines and Manufactures* (1832), c'est avant tout pour mobiliser les hommes de pouvoir afin de coordonner les développements industriels, alors facteurs de profonds déséquilibres politiques et sociaux.

Ses travaux de cryptologie coïncident avec les débuts du télégraphe, dont il appréhende tout à fait l'importance socio-économique, tout comme il enquête en tant qu'expert pour s'assurer de la sécurité des chemins de fer. Charles Wheastone (1802-75), l'inventeur du télégraphe en Angleterre, est un de ses amis. Il invente aussi, en 1854, un procédé de chiffrement par substitution de digrammes, qui se trouve répertorié dans le manuscrit de Babbage[11]. Ce mode de chiffrement est communément appelé « carré de Playfair », du nom du baron Lyon Playfair (1818-98) qui le présentera aux autorités. Wheatstone, comme Playfair, a le souci d'éviter que les textes des télégrammes puissent être lus par tous, au moins pour certains sujets sensibles[12]. Cependant, contrairement à Wheatstone en 1854, contrairement aussi à John H. B. Thwaites au même moment, Babbage n'aborde pas la question du secret des correspondances télégraphiques. Il ne considère que les messages privés échangés au sein de cette élite cultivée qu'il veut convertir à la science et où il fait autorité[13]. La cryptologie reste pour Babbage une activité réservée à cette élite, une aristocratie proche du pouvoir, celle qu'il reçoit dans ses dîners mensuels et à laquelle il fait admirer sa « machine aux différences ». Auteur charnière entre les pratiques scripturales et le développement des réseaux, Babbage se considère lui-même comme un philosophe – au sens de la « philosophie naturelle » – selon le titre de son autobiographie[14].

[10] Franksen, *Mr Babbage's Secret*, p. 211.
[11] Babbage, Add. Mss 37 205, folio 80.
[12] Un appareil qui mécanise ce procédé, le cryptographe de Wheatstone, porte également son nom. Davies, « Wheatstone's Cryptograph ».
[13] Durand-Richard, « Le regard français de Charles Babbage ».
[14] Babbage, *Life of a Philosopher*.

C'est donc avec les érudits et aristocrates de ses amis et connaissances que Babbage se consacre à la cryptographie, une activité à laquelle il s'adonne tout à fait régulièrement, et qui semble le fasciner suffisamment pour qu'il entreprenne d'en répertorier les principales méthodes, qu'il puise essentiellement dans le traité de cryptographie du révérend John Wilkins, évêque de Chester, *Mercury or the Secret and Swift Messenger* (1641). C'est d'ailleurs à Wilkins – dont les œuvres viennent alors d'être rééditées – et non à Vigenère, que Babbage attribue le chiffrement polyalphabétique, signe de l'importance des traditions nationales en ce domaine. Les *agony columns,* ces messages du journal *The Times* où s'échangent soupirs et rendez-vous galants, sont une source importante d'exemples des modes de chiffrement élémentaires pour Babbage, qu'il utilise en deux exemplaires dans son manuscrit, l'un comme explication, l'autre comme exercice. Babbage et Wheatstone n'ont donc aucun mal à les décrypter, ce dernier allant jusqu'à s'immiscer dans ces correspondances pour mettre en garde les protagonistes ou s'en moquer[15]. Plus sérieusement, et très systématiquement, Babbage dresse un inventaire chronologique et conceptuel des systèmes de chiffrement, et accumule des matériaux d'aide au décryptement[16] : dictionnaires, inventaires, répertoires, analyse de fréquences sur des lettres et des mots courts, recherche d'équations simultanées. Il est régulièrement sollicité pour décrypter des correspondances, et insiste auprès de ses interlocuteurs sur les difficultés du décryptement en l'absence d'une bonne connaissance du contexte ou de la langue, surtout quand il s'agit d'analyses historiques. En 1835, il aide l'astronome Francis Baily (1774-1844) à reconstituer le sens d'une lettre datée de 1722, de l'assistant de l'astronome royal John Flamsteed (1646-1719), écrite comme une sorte de sténographie, afin de déterminer l'origine des erreurs constatées dans les observations de son arc mural[17]. En 1854, il intervient dans un procès, décryptant une abondante correspondance chiffrée afin de rétablir l'honneur de la famille du capitaine Childe[18]. Enfin, en 1858, il détermine pour Mrs Green[19] que les lettres qu'elle possède doivent être attribuées au roi Charles II plutôt qu'à Charles I. Dès le début des années 1830, Babbage innove dans ses échanges avec ses amis, Davies Gilbert (1767-1839) – président de la *Royal Society* de 1827 à 1830 – ainsi que le géologiste William H. Fitton (1780-1861) et sa sœur Mrs James, composant un système auto-clé, et discutant de ses possibilités et inconvénients selon que le mot-clé utilisé est soit le texte clair, soit le texte chiffré[20].

---

[15] Babbage, Add. Mss 37 205, folios 66, 80.
[16] *ibid.*, folios 211, 214.
[17] Franksen, *Mr Babbage's secret*, p. 18.
[18] Babbage, Add. Mss 37 205, folios 81 à 130.
[19] *ibid.*, folios 209 à 214.
[20] *ibid.*, folios 8-9. Babbage, *Life of a Philosopher*, p. 175-176.

Premier décryptement du mode polyalphabétique

C'est entre février et mars 1846 que Babbage va décrypter un message chiffré en mode polyalphabétique, à l'occasion d'un jeu avec son neveu Henry Hollier qu'il a initié à la cryptologie lorsqu'il était enfant, et qui l'aide à établir ses dictionnaires de déchiffrement – répertoires de mots et analyse de fréquences sur des mots courts. L'intérêt du manuscrit « Philosophy of Deciphering » est de rassembler ses nombreux essais, dont la collecte est malheureusement incomplète, et qui, à l'évidence, n'est pas rangée dans le bon ordre[21]. Le message chiffré est le suivant :

```
PYRI  ULOFV

POVVMGN  MK  UO  GOWR  HW  LQ  PGFJHYQ OJAV  MSN
WIJHEEHPR  BRVGRUHEGK, EFF WJSR  RVY
CPOY  VSP,  PX  OKLN  PI  XXYSNLA  SELF  XG
FEEWTALV  LJIU, WR  MOI  EGAP  HMFL  ML  YINZ
TNGDDG  YQIV  UYEAP-BQL
     WJQV  PGYK  STRITLMHFOFI EWTAWK
               TIEJC
```

Babbage découvre assez vite qu'il s'agit d'un mode de chiffrement polyalphabétique. Il fait à ce sujet de nombreuses analyses de fréquences à partir des mots courts, de 2, 3 et 4 lettres. La première difficulté de son travail provient du fait que le message a été chiffré à partir de trois clés différentes, difficulté que Babbage devra d'abord identifier avant de parvenir au texte clair. Après quelques tentatives infructueuses pour écrire et résoudre des systèmes d'équations simultanées – ces systèmes étant incomplets –, Babbage repère d'abord qu'il est possible d'associer, à chaque lettre de l'alphabet, le nombre qui correspond à son rang.

Alors, pour chaque lettre du chiffré, du clair et du mot-clé qui se correspondent, Babbage découvre l'existence d'une opération entre les nombres qui leur sont associés, à condition toutefois de soustraire 26 dès que ce nombre excède 26, ce qu'il écrit :

> « Take 26 from all the +s exceeding 26 »

Babbage met longuement en œuvre cette opération dans ses essais pour trouver les mots-clés, avant de l'exprimer pour la première fois par une formule mathématique :

[21] *ibid.*, folios 43 à 63.

Cypher = Key + Translation – 1 (1)
Translation = Cypher – Key + 1

Partant de cette constatation, sa méthode va consister à conjuguer la recherche des mots-clés avec celle de mots probables, comme « *affectionate* », « *nephew* », *dear uncle* », *etc*. Il écrit victorieusement : « *Decyphered completely, Thursday, March 19, 1846 – Friday morning 1 1/2 a.m.* »[22], et donne la solution obtenue avec les trois clés différentes MURRAY, CACOETHES et SUMMERSET :

```
  PYRI   ULOFV
  murr  aymur
  dear  uncle

POVVMGN  MK  UO  GOWR  HW  LQ  PGFJHYQ
cacoeth  es  ca  coet  he  sc  acoethe
nothing  is  so  easy  as  to  perform

OJAV  MSN  WIJHEEHPR  BRVGRUHEGK, EFF WJSR  RVY
scac oet   hescacoet  hescacoeth, esc acoe  the
what  you  perfectly  understand, and when  you

CPOY  VSP,  PX  OKLN  PI  XXYSNLA  SELF  XG
scac  oet,  he  scac  oe  thescac  oeth  es
know  how,  it  will  be equally   easy  to

FEEWTALV  LJIU, WR  MOI EGAP  HMFL  ML  YINZ
cacoethe  scac  oe  the scac  oeth  es  caco
decipher  this  in  the mean  time  it  will

TNGDDG  YQIV  UYEAP-BQL
ethesc  acoe  thesc-aco
puzzle  your  brain-box

       WJQV  PGYK  STRITLMHFOFI EWTAWK
       some  rset  somersetsome rsetso
       ever  your  affectionate nephew

                   TI EJC
                   me rse
                   hen ry
```

Sur la même page où Babbage donne cette solution se trouvent également les trois petits tableaux suivants :

[22] *ibid.*, folios 58-59. Ces feuillets sont datés du 24 février, élément qui témoigne du désordre de leur classement.

	Table 1			Table 2			Table 3	
	N°	Rem Substract		N°	Rem Substract		N°	Rem Substract
6)	0	24	9)	0	18	8)	0	19
	1	12		1	2		1	18
	2	20		2	0		2	14
	3	17		3	2		3	12
	4	17		4	14		4	4
	5	0		5	4		5	17
				6	19		6	18
				7	7		7	14
				8	4			

En face de chaque reste est ainsi indiquée la lettre de l'alphabet correspondante. Par exemple, pour la troisième clé :

0	1	2	3	4	5	6	7
T	S	O	M	E	R	S	E
19	18	14	12	4	17	18	4

Ces tableaux traduisent une étape supplémentaire dans la réflexion de Babbage concernant la correspondance entre nombres et lettres de l'alphabet. Cette fois, Babbage n'associe plus à chaque lettre son *numéro* d'ordre dans l'alphabet, mais un *nombre* de 0 à 25, c'est-à-dire leur reste dans la division par 26, à savoir les classes de résidus dans une relation de congruence modulo 26. Comme en témoignent les correspondances numériques qui se trouvent dans les feuillets de recherche de ce type :

19	20	18	9	20	12	13	8	6	15	6	9
S	T	R	I	T	L	M	H	G	O	F	I
18	14	12	4	17	18	4	19	18	14	12	4
A	F	F	E	C	T	I	O	N	A	T	E
1	6	6	5	3	20	9	15	14	1	20	5
S	O	M	E	R	S	E	T	S	O	M	E

et la présence constante du terme (+1) dans les formules (1), ce n'est pas au cours de sa recherche[23], mais seulement dans sa présentation finale, que Babbage fait le rapprochement entre son travail et la théorie des congruences de C. F. Gauss (1777-1855), dont il connaît par ailleurs les *Disquisitiones Arithmeticae* (1801).

[23] O. Franksen affirme que Babbage utilise les congruences de Gauss pour mener sa recherche, alors qu'il utilise seulement la correspondance entre numérotation et lettres de l'alphabet.

Le seul travail publié de décryptement : la controverse avec Thwaites

Par contre, Babbage utilise dans le détail cette théorie des congruences lorsqu'en 1854, il montre à Thwaites, chirurgien-dentiste à Bristol, que cette invention qu'il croît toute nouvelle n'est autre que le chiffrement polyalphabétique : on le trouve déjà chez Wilkins, il a déjà été décrypté – par Babbage lui-même –, et le système de règles coulissantes que Thwaites a fait breveté existe aussi déjà, en carton ou en bois, y compris sous d'autres formes, comme le système des disques concentriques. Thwaites avait envoyé son « invention » à la *Society of Arts,* pour qu'elle en fasse connaître l'intérêt, affirmant que ce système valait pour tout langage, et qu'il était très sûr, puisqu'il était, selon lui, impossible de décrypter le message sans connaître la clé. Il se référait même à l'*Essay on Probabilities,* publié par Augustus de Morgan (1806-71) en 1838 dans le *Penny Cyclopaedia*, pour affirmer que : « De par cette communication, je revendique la primeur de la découverte de la correspondance secrète utilisant le principe de permutation »[24]. Cette invention lui semble cruciale pour maintenir le secret dans les échanges télégraphiques, tant pour les établissements publics que dans les échanges commerciaux, donnant l'exemple d'une faillite qui aurait pu être évitée si une information confidentielle avait pu être envoyée chiffrée par télégramme.

Contacté comme expert, Babbage répond d'abord sarcastiquement que « il ne vaut pas la peine de considérer un chiffrement comme impénétrable, sauf si l'auteur a lui-même décrypté quelque chiffrement très difficile ». Mais il n'aura finalement d'autre recours pour convaincre Thwaites de sa méprise que de décrypter le message de sa seconde lettre, un extrait de *The Tempest* de Shakespeare, chiffré deux fois successivement avec deux clés différentes.

Le clair :

> Soft, sir, one word more,
> They are both in either's powers : but this swift business
> I must uneasy make, lest too light winning
> Make the pne word more, I charge thee
> That thou attend me, thou dost here usurp
> Upon this island as a spy, to win it
> From me, the lord on't.

[24] « *By this communication I claim precedence in the discovery of secrecy correspondence on the principle of permutation.* »

Le chiffré :

UTMU[25], DQV, UKS, LKZT, LRWN, FLHL, HPG,
SVUS, QR, KFHWAZI, ORBNDW, EHA, RJZZ,
THQJZ, YHIEVURV, N, VGWW, HUCCJF,
NLSI, RBGI, PWE, KLLQF, ALAUGPX, TBVM,
XNB, DGEHU, KLLQF, SQR, DMTU, TPCM, M
IEOGCM, JGHJ, CTEW, GOMW, RAUPVH, SB,
HWKC, TNVY, QQVH, HZSTG, BQZV, XNFG
XOTQMG, FB, M, WSL, AM, YZU, JE, NVUJ,
AT, PPU, KRWM, AR'W.

Babbage s'amuse alors de ce que Thwaites ignore : « [Il] ne semble pas connaître les principes sur lesquels sont construits de tels chiffrements, car il semble avoir employé deux chiffrements successifs, à savoir le mot TWO à partir de *p*, et le mot COMBINED à partir de *e*. Plus encore, il semble ignorer que l'ordre des chiffrements successifs est indifférent ». Ce que démontre Babbage sur le premier vers du texte, avec les deux clés trouvées : TWO et COMBINED, sans révéler pour autant comment il les a trouvées. Mais cette fois, il présente en détail comment, à partir de cette clé composée de 24 lettres (3 fois 8), il peut obtenir pour chaque lettre du chiffré, la lettre correspondante du clair. Partant d'un tableau du même type que ceux qu'il avait donnés pour les trois clés du message de son neveu :

Reste	Nb tabulaire	Reste	Nb tabulaire
0	24	12	22
1	2	13	8
2	17	14	16
3	7	15	25
4	1	16	3
5	11	17	5
6	8	18	9
7	4	19	12
8	6	20	4
9	23	21	3
10	14	22	13
11	15	13	7

Babbage « calcule » alors pour chaque lettre du chiffré la lettre correspondante du clair. Ainsi, pour le mot GOMW du chiffré :

w est la 145e lettre du chiffré et 145 = 6 fois 24 + 1

[25] Après avoir trouvé les deux clés avec lesquelles le message a été chiffré, Babbage corrigera la 2ème lettre du 1er mot du chiffré, qui doit être *v* et non *t*.

Dans le tableau, en face du reste 1 se trouve le nombre 2, et la lettre *w* est la 23e lettre de l'alphabet naturel. La différence 23 – 2 = 21 donne la place de la lettre du clair dans l'alphabet, soit *u*.

Babbage renvoie alors la balle dans le camp de Thwaites, le mettant au défi de décrypter à son tour un chiffré issu de la même pièce de Shakespeare, défi que Thwaites ne relèvera pas[26].

Le caractère privé des échanges de Babbage est essentiel pour appréhender à la fois ses méthodes et l'absence de diffusion de son travail. La non publication de « Philosophy of Deciphering » est souvent attribuée à la guerre de Crimée (1853-54), et au souci de ne pas rendre public ce qui aurait pu avantager l'adversaire russe. Mais outre la dispersion de Babbage lui-même entre tous ses travaux[27], l'écart entre les recherches savantes et l'état des pratiques sur le terrain peut également avoir été déterminant. Lorsqu'au même moment, Lyon Playfair propose le chiffrement de Wheatstone au Foreign Office, celui-ci juge son utilisation trop compliquée pour les praticiens de la cryptographie. Le fossé déjà signalé au chapitre « L'ancrage de la cryptologie dans les jeux d'écriture »[28], entre avancées conceptuelles et état de l'art est donc encore très prégnant au milieu du 19e siècle. Et Babbage cherche avant tout la reconnaissance de son milieu social. Lorsque Thwaites insiste sur les avantages commerciaux de sa proposition au moment où se développe l'utilisation du télégraphe, Babbage se contente de démontrer l'existence du décryptement, il ne renchérit pas sur la possibilité de lui donner une plus vaste audience.

C'est donc à Friedrich W. Kasiski (1805-81) qu'est en général attribué le décryptement du chiffrement de Vigenère, qu'il publie à Berlin en 1863 dans *Die Geheimschriften und die Dechiffrir-Kunst*. À juste titre d'ailleurs, puisque Kasiski donne cette fois une méthode générale de décryptement, un raffinement de l'analyse des fréquences. Pour l'appliquer, il faut au préalable découvrir la longueur de la clé, ce qui se fait en repérant, sur un texte assez long, des répétitions de groupes de lettres qui laissent supposer qu'un même mot a pu être chiffré à différents endroits avec les mêmes lettres-clé. La distance, en nombre de lettres, entre ces répétitions donne alors un multiple du nombre de lettres de la clé. Une fois ce nombre

[26] Tous ces échanges sont publiés dans le *Journal of the Society of Arts*, 1855, vol. 2, pp. 253-258, et compilés dans le manuscrit de Babbage sur la « Philosophy of Deciphering ». Add. Mss 37205, folios 133 à 179, avec les articles de ce journal, la correspondance avec le journal, et les essais de décryptement de Babbage.

[27] Babbage est également l'auteur d'une « Philosophy of Analysis », écrite dans les années 1820, et non publiée. Il en partagera cependant les idées dans sa correspondance avec George Peacock, l'auteur d'un *Treatise on Algebra* qui initie à Cambridge une conception purement symbolique de l'algèbre.

[28] Voir p. 24.

déterminé, il ne reste plus qu'à découper le message en sous-messages, formés des lettres chiffrées avec la même lettre de la clé.

L'ouvrage de Kasiski a été publié alors qu'il était officier d'infanterie prussien à la retraite. Il a travaillé en amateur sans mesurer tout l'intérêt de ses avancées. Sa démarche reste attachée au message, contrastant avec l'approche de Kerckhoffs qui énoncera ses lois dans une perspective plus globale liée au système de communication.

KERCKHOFFS ET LE SYSTEME TELEGRAPHIQUE

Dans la seconde partie du 19e siècle, les militaires s'emparent de l'usage du télégraphe. Leurs échanges secrets sont désormais transmis par ce nouveau support, ce qui change radicalement les conditions auxquelles la cryptologie se trouve confrontée. Là où Babbage continuait à traiter des messages entre individus, Kerckhoffs va examiner frontalement les nouvelles exigences qu'impose au secret l'utilisation d'un réseau télégraphique par les personnels militaires, du commandement aux exécutants.

Comme pour Kasiski, les renseignements sont rares quant aux biais par lesquels Kerckhoffs est arrivé au contact de la cryptologie. En particulier, il est difficile d'apprécier en quoi consistent ses relations avec le monde militaire. David Kahn[29] nous apprend seulement qu'il a eu des difficultés politiques après la défaite de 1870. Mais rien dans sa biographie n'indique spécifiquement comment il a été conduit à publier deux importants articles sur « La cryptographie militaire » dans deux numéros successifs du *Journal des sciences militaires,* en janvier et février 1883. Jean Guillaume Hubert Victor François Alexandre Auguste Kerckhoffs von Nieuwerhof (1835-1901), issu d'une riche famille flamande, diplômé en lettres et en sciences à l'Université de Liège, a beaucoup voyagé en Europe avant de s'installer en France où il va enseigner, d'abord essentiellement les lettres et les langues modernes en province – à Meaux et à Melun – puis l'allemand à l'Ecole des Hautes Etudes Commerciales et à l'Ecole Arago à Paris à partir de 1881. Il est l'auteur de divers ouvrages, qui vont du théâtre à des grammaires de langue étrangère. C'est après ses publications en cryptographie qu'il se fera propagandiste d'un nouveau langage, le *Volapuk*, qui vient d'être inventé par le prêtre catholique allemand Martin Schleyer (1831-1912), et qui se répand comme une traînée de poudre en France et dans le monde entier dès sa création en 1880. Kerckhoffs devient même président de l'*Académie Internationale de Volapuk* au 2e congrès de *Volapuk* tenu à Munich en 1887.

[29] Kahn, *The Codebreakers,* pp. 230-240.

Malgré ces débuts fulgurants, le *Volapuk* est moribond dès 1890 : il n'a pas résisté aux oppositions quant à la « nature » de cette nouvelle langue, entre l'idée d'une langue la plus littéraire possible envisagée par Schleyer et celle d'une langue la plus simple possible voulue par Kerckhoffs. L'érudition linguistique de ce dernier a sans aucun doute constitué une forme d'expertise tout à fait propice à penser une réorganisation des enjeux de la cryptographie militaire. Mais les éléments connus de sa biographie laissent néanmoins dans l'ombre le détail de son élaboration.

Les exigences de la cryptographie télégraphique

Dans les cours de cryptologie à l'université aujourd'hui, les lois de Kerckhoffs sont énoncées dans un cadre mathématisé, se référant à l'algorithme qui préside au secret des échanges. Elles apparaissent, du fait de cette dénomination, comme une sorte d'anticipation des critères de sécurité d'un système cryptographique transmis par voie électronique, alors qu'il n'y a bien sûr pas trace de référence à une quelconque notion d'algorithme chez Kerckhoffs, cette notion n'étant, à l'évidence, pas formalisée à son époque. Par contre, il a parfaitement perçu et explicité les conditions nouvelles imposées par la transmission télégraphique des messages, à la fois pour rendre applicable leur chiffrement, et pour adapter les services cryptographiques de l'armée à ce nouveau système de transmission. Analysant les conséquences organisationnelles de l'utilisation du télégraphe pour les services du chiffre, Kerckhoffs énonce ce qu'il appelle les « desiderata de la cryptographie militaire »[30] :

> « 1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable,
> 2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi,
> 3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants,
> 4. Il faut qu'il soit applicable à la correspondance télégraphique,
> 5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes,
> 6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer »[31].

[30] Guillot, « Auguste Kerckhoffs et la cryptographie militaire ».
[31] Kerckhoffs, « La cryptographie militaire », I, p. 12.

Kerckhoffs insiste sur le fait que ce mode de communication fait intervenir plusieurs niveaux de responsabilité et de très nombreux intervenants, dont les compétences sont très différentes. Il relève la difficulté qui a si longtemps bloqué l'utilisation des modes de chiffrement les plus élaborés : il serait vain d'exiger des personnels peu formés d'effectuer des manipulations trop compliquées. Il s'agit de rendre compatible le secret des informations avec cet usage collectif des échanges à l'extérieur comme à l'intérieur de la chaîne de transmission. C'est cette analyse qui conduit Kerckhoffs à distinguer pour la première fois sans doute entre deux types de difficulté : la difficulté matérielle et la difficulté mathématique. Et c'est aux difficultés matérielles et organisationnelles qu'il s'attache : le « système » dont il traite est celui qui régit la transmission télégraphique de l'ensemble des messages dans l'armée. On est loin des correspondances privées auxquelles Babbage appliquait ses recherches mathématiques :

> « Il faut bien distinguer entre un système d'écriture chiffrée, imaginée pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux. Ceux-ci, en effet, ne peuvent, à leur gré, et à un moment donné, modifier leurs conventions ; de plus, ils ne doivent jamais garder sur eux aucun objet ou écrit qui soit de nature à éclairer l'ennemi sur le sens des dépêches secrètes qui pourraient tomber entre ses mains […]. Un grand nombre de combinaisons ingénieuses peuvent répondre au but qu'on veut atteindre dans le premier cas, dans le second, il faut un système remplissant certaines conditions exceptionnelles »[32].

Ce sont ces conditions exceptionnelles, liées au mode de transmission télégraphique, qui constituent ce que Kerckhoffs nomme pour la première fois un « système cryptographique », et dont il énonce les « desiderata ». C'est bien dans ce domaine qu'il innove, et non en mathématiques. Il précise en outre que les messages chiffrés sont désormais écrits en séparant les lettres des messages chiffrés en tranches de cinq lettres, du fait de leur transmission télégraphique. S'il présente un inventaire érudit des méthodes et des instruments de chiffrement, il n'en produit pas de nouveau.

L'organisation de la cryptographie en tant que « système » n'est pas seulement une question de définition couchée sur le papier. Kerckhoffs accorde beaucoup d'importance aux différents systèmes de chiffrement utilisables sur le champ de bataille. Rendre ces « desiderata » effectifs impose tout un ensemble d'adaptations qui ne vont pas de soi au sein de l'armée, du moins en ce qui concerne les services du chiffre. Comment

[32] *ibid.*, I p. 12.

rendre compatible la hiérarchie du commandement militaire avec la circulation des messages chiffrés entre tous les niveaux de l'armée ? Exiger un secret absolu supposerait que dans un corps d'armée, toutes les instructions chiffrées émanent ou du moins passent dans les mains d'un seul, ce qui serait réduire la correspondance secrète à un rôle singulièrement modeste. Kerckhoffs attribue d'ailleurs, au moins en partie, la défaite de 1870 à un manque de communication entre les généraux de Paris et ceux de la province. Le procédé étant désormais commun à tous, le secret doit donc porter essentiellement sur la clé.

Corollaire de la mise en place de ce système de communications : l'extension de l'enseignement de la cryptologie dans les écoles militaires, dont Kerckhoffs souligne l'importance. Il en fait état en France depuis 1874, et en Allemagne au moment où il écrit en 1883. Le système cryptographique doit être également compatible avec les exigences du caractère public de cet enseignement :

> « L'administration doit absolument renoncer aux méthodes secrètes et établir en principe qu'elle n'acceptera qu'un procédé qui puisse être enseigné au grand jour dans nos écoles militaires, que nos élèves seront libres de communiquer à qui leur plaira et que nos voisins pourront adopter et même copier si cela leur convient »[33].

Au-delà de l'inventaire des méthodes cryptographiques, c'est bien l'enjeu principal des articles de Kerckhoffs : convaincre le système hiérarchique de l'armée de la nécessaire réorganisation des services du chiffre du fait de ce nouveau mode de transmission des messages.

Les débuts d'un enseignement de la cryptographie militaire

Conséquence du travail de Kerckhoffs ou de la défaite de 1870 : la France a considérablement renforcé son service cryptographique. Selon David Kahn en effet, il s'agit d'ailleurs d'une pratique manifeste dans les pays ayant connu une défaite militaire, ce que les vainqueurs négligent de faire en général. Le travail de Kerckhoffs structure ce que David Kahn appelle une véritable école de cryptographie[34], constituée pour beaucoup d'officiers issus de l'Ecole Polytechnique, et qui va assurer la suprématie de la France en ce domaine jusqu'à la Première Guerre Mondiale. Le marquis Gaëtan de Viaris (1847-1901) – Gaëtan Henri Léon Viarizio di Lesegno – réorganise le Service du Chiffre en 1890, conçoit quelques machines de chiffrement, et produit plusieurs articles dans *Le Génie Civil*, où il traduit en

[33] *ibid*., I, pp. 14-15.
[34] Kahn, *The Codebreakers*, pp. 240-242.

équations algébriques les relations entre les lettres du clair et du chiffré pour tous les chiffrements polyalphabétiques déductibles de celui de Vigenère. Paul-Louis-Eugène Valério publie une dizaine d'articles dans le *Journal des sciences militaires* dans les années 1890, ainsi qu'un ouvrage en deux volumes, *De la cryptographie, essai sur les méthodes de déchiffrement* (1893-96). Il interviendra dans le procès de Rennes qui condamne une seconde fois le capitaine Dreyfus, avant que ne lui soit accordée une grâce présidentielle en 1899. La tradition de la cryptographie comme activité érudite se poursuit également, comme en témoigne le *Traité élémentaire de cryptographie* (1901) de Félix M. Delastelle (1840-1902), administrateur des tabacs à Marseille, qui se consacre à une classification des modes de chiffrement au moment où il prend sa retraite. Et le lieutenant Etienne Bazeries (1846-1931) s'est initié par lui-même à la cryptanalyse, en décryptant les messages chiffrés parus dans les colonnes des journaux, avant de devenir si efficace au Bureau du Chiffre du Ministère des Affaires Etrangères. Il cassera le fameux « Grand Chiffre de Louis XIV », et publiera *Les chiffres secrets dévoilés* (1901), avant de travailler pour l'armée jusqu'après la Première Guerre Mondiale, ne se retirant qu'en 1924. N'oublions pas George-Jean Painvin (1886-1980) qui, s'il fut formé à l'Ecole Polytechnique, enseignait la géologie et la paléontologie avant de devenir LE cryptanalyste qui permit à l'armée française le succès que l'on sait dans les derniers moments de la Première Guerre Mondiale [35]. Au cours de cette guerre, le lieutenant Henry Olivari (1868-1955), polytechnicien, est envoyé à Petrograd (Russie) sous les ordres du général Maurice Janin (1862-1946), dans le cadre d'une mission militaire française chargée d'organiser un encadrement des services français insuffisamment dotés à l'ambassade, de recueillir des radiogrammes allemands sur le front de l'est, et aussi d'établir des liens avec l'état-major russe, et d'enseigner à la Stavka certaines méthodes, dont Olivari précise : « Étant mieux qui quiconque au courant de ce qui avait été fait à Paris, je savais fort bien ce qu'il convenait de dire et de cacher ». À son retour, il déplorera que cette collaboration n'ait pas été plus loin du fait de dissensions au sein du Service du Chiffre[36]. Tous ces travaux seront largement repris dans le *Cours de cryptographie* du colonel Marcel Givierge (1871-1931), qui servira longtemps de manuel aux cryptologues français, jusqu'après la Seconde Guerre Mondiale. Il connaîtra plusieurs éditions, et traversera l'Atlantique, puisque Shannon le cite comme une source importante[37] dans sa *Theory of Secrecy Systems* en 1949.

[35] Voir le chapitre « Les travaux de la section du chiffre pendant la Première Guerre Mondiale » p. 90.

[36] D'autres membres de la mission étaient polytechniciens ou normaliens. Certains d'entre eux resteront en URSS après la Révolution d'Octobre en 1917. Olivari, *Mission d'un colonel français en Russie 1916*, p. 36.

[37] Voir dans ce chapitre : « Mathématisation de la cryptographie ».

Quoi qu'il en soit, de part et d'autre de l'Atlantique, les militaires vont développer un enseignement de la cryptologie spécifique aux systèmes télégraphiques, sans que les manuels ne se montrent innovants pour autant[38]. À tel point qu'en 1915, le lieutenant Parker Hitt (1878-1971), instructeur en cryptologie de l'école du Signal de l'armée à Fort Leavenworth, est tellement conscient de la vulnérabilité des méthodes de chiffrement enseignées aux États-Unis qu'il demande – en vain – à ses chefs de partir – à ses frais ! – en France pour s'initier à des méthodes plus élaborées. L'autorisation lui en sera refusée, mais, devenu *Chief Signal Officier of the First Army* en 1918, il exercera ses talents sur le front en France au sein de l'*American Expeditionary Forces.* Il saura combler le fossé entre les pratiques de la cryptologie militaire et les avancées technologiques des nouveaux moyens de communication (télégraphe, téléphone, radio). Son *Manual for the Solution of Military Ciphers* (1916), premier livre de ce type outre-Atlantique, sera utilisé en particulier par le couple de cryptanalystes William F. Friedman (1891-1969) et Elizabeth W. Friedman (1892-1980) pour former des générations de cryptologues pendant l'entre-deux-guerres[39].

VERNAM ET LA PROTECTION DES ECHANGES PAR TELESCRIPTEUR

La façon dont l'armée investit le télégraphe pour son système de communications secrètes fait passer au second plan l'importance de la cryptologie dans les correspondances secrètes et les relations commerciales. À partir de la fin du 19e siècle, elle sera de ce fait le plus souvent référée aux échanges diplomatiques et militaires[40]. Pourtant, évoquée entre Babbage et Twaites pour les échanges commerciaux, elle se maintient aussi dans les milieux cultivés, comme en témoigne l'investissement d'un Edgar A. Poe (1809-49) sur le sujet dans ses *Histoires extraordinaires*[41]. L'introduction des téléscripteurs aux États-Unis, en faisant converger échanges privés, échanges commerciaux et mécanisation des moyens de transmission, correspond au moment du déploiement généralisé des communications, et à leurs besoins de confidentialité. La technique de chiffrement inventée par Gilbert S. Vernam, ingénieur chez AT&T (*American Telegraph and Telephon Company*) à Manhattan depuis 1915, contribuera d'ailleurs largement au développement du téléscripteur lui-même. Mais elle n'est le

[38] Slater, *Telegraphic Code* ; Hill, *Manual for the Solution of Military Ciphers.*
[39] Smoot, « Fighting the Damned Huns ».
[40] Il est en général ignoré que la machine *Enigma,* utilisée comme machine de chiffrement par les services allemands de la défense pendant la Seconde Guerre Mondiale, fut d'abord conçue pour le commerce et utilisée dans les banques dans les années 1920. Voir le chapitre « L'ancrage de la cryptologie dans les jeux d'écriture » p. 19.
[41] Voir le chapitre « L'ancrage de la cryptologie dans les jeux d'écriture » p. 19.

fait ni d'un mathématicien, ni d'un linguiste, et s'exprime dans le vocabulaire spécifique de l'ingénieur, en termes d'impulsions électriques.

Le chiffrement automatique des messages transmis par téléscripteur

Vernam est alors chargé de la sécurité des téléscripteurs à la section télégraphe du département *Develepment and Research*, et son invention est inscrite dans la nature même de ce type de transmission. Elle intègre le chiffrement et le déchiffrement au processus d'émission, de transmission et de réception des messages par voie télégraphique. Une fois de plus, il n'y a pas trace d'algorithme de chiffrement dans le brevet[42] qu'il obtient en 1919. Le texte de ce brevet décrit avant tout un dispositif technique, le « *printing telegraphic system* », formé d'électro-aimants et de commutateurs rotatifs, qui produit et contrôle automatiquement la façon de rendre inintelligibles les messages au cours de leur transmission. Il y est question de circuits ouverts ou fermés, de connexions et d'impulsions électriques. Les opérations dont traite Vernam sont celles qui caractérisent les différentes étapes de fonctionnement des parties du système : dispositifs d'émission, de transmission et de réception, et dispositifs de chiffrement et de déchiffrement. Les explications qui concernent le mode de chiffrement et de déchiffrement portent essentiellement sur la manière technique de le réaliser. Elles ne sont pas données en termes mathématiques.

Les signes du code Baudot
avec le mode de symbolisation de Vernam

A	+	+	−	−	−	B	+	−	−	+	+	C	−	+	+	+	−	D	+	−	−	+	−
E	+	−	−	−	−	F	+	−	+	+	−	G	−	+	−	+	+	H	−	−	+	−	+
I	−	+	+	−	−	J	+	+	−	+	−	K	+	+	+	+	−	L	−	+	−	−	+
M	−	−	+	+	+	N	−	−	+	+	−	O	−	−	−	+	+	P	−	+	+	−	+
Q	+	+	+	−	+	R	−	+	−	+	−	S	+	−	+	−	−	T	−	−	−	−	+
U	+	+	+	−	−	V	−	+	+	+	+	W	+	+	−	−	+	X	+	−	+	+	+
Y	+	−	+	−	+	Z	+	−	−	−	+	3	−	−	−	+	−	4	−	+	−	−	−
8	+	+	+	+	+	(+)	+	+	−	+	+	9	−	−	+	−	−	/	−	−	−	−	−

(3 = carriage return, 4 = line feed, 8 = letter shift, + = figure shift,
9 = space, / = null)

Les téléscripteurs représentent les lettres d'un message en utilisant le code Baudot, un codage binaire également appelé code télégraphique ou alphabet international, l'équivalent du code Morse pour ce type de transmission. Chaque lettre de l'alphabet y est codée par cinq unités qui, à

[42] Vernam présente son invention chez AT&T dans une note du 17 décembre 1917. Le brevet est daté du 22 juillet 1919, mais il est signé par Vernam en date du 08 septembre 1918.

partir de la frappe sur le clavier, vont se traduire par le passage du courant électrique ou par son absence. Les différentes combinaisons possibles de ces cinq unités permettent donc de transmettre 32 signes. Et le système dispose en outre de deux modes, qui permettent de distinguer minuscules et majuscules, et de représenter d'autres signes (ponctuation, chiffres). Dans une émission normale du message, pour chaque lettre transmise, les cinq impulsions correspondantes s'inscrivent sur le ruban de papier perforé, sous la forme d'un trou ou d'une absence de trou. Des ergots entrent dans ces trous pour faire contact et reproduire une impulsion. Ce codage sur ruban perforé peut alors être retranscrit au destinataire sous forme de lettres imprimées.

L'invention de Vernam utilise l'équipement du téléscripteur pour chiffrer ou déchiffrer automatiquement les messages. Elle associe au ruban du message un autre ruban qui fait office de clé. Lettre à lettre, les deux informations sont alors combinées électro-mécaniquement, afin de ne transmettre sur la ligne que le message chiffré. Cette clé n'est donc plus nécessairement un mot de la langue, elle n'est pas davantage un objet mathématique, elle n'est qu'un ruban de papier perforé dont les marques sont produites au hasard, même si Vernam précise qu'elles peuvent représenter une lettre de l'alphabet. Ce dispositif ouvre donc la voie au caractère aléatoire de la clé. Si la règle de combinaison est traditionnellement présentée dans les ouvrages comme une addition sur l'ensemble {0,1}, ou comme l'opération du connecteur logique « ou exclusif » sur ce même ensemble, le brevet la décrit comme une combinaison des signes « + » et « – », où « + » représente une impulsion électrique, et « – » l'absence d'une telle impulsion. Encore ne la décrit-il que sur un exemple :

> « Supposons que le premier caractère du message à transmettre soit un *A*. Le *A* est codé par les signaux « + + − − − », où « − » représente une impulsion ouverte ou « espace », et « + » représente une impulsion fermée ou « marque ». Dans le système décrit ici, il faut comprendre que des impulsions de courant positives et négatives peuvent être utilisées à la place de circuits fermés ou ouverts si il y a besoin. Pour chiffrer et déchiffrer le message aux deux bouts de la ligne, on utilise des bandes identiques où est enregistrée une série de signaux codés qui sont de préférence choisis au hasard, mais qui, si on le veut, peuvent représenter une série prédéfinie de lettres ou de mots. Supposons que la lettre *B* soit présente dans l'émetteur chiffrant en même temps que la lettre *A* est transmise dans l'émetteur normal. Le code de la lettre *B* est « + − − + + ». L'envoi du *A* par l'émetteur normal signifie que les contacts 25 et 26 seront fermés alors que les contacts 27, 28 et 29 seront ouverts. Par conséquent, les relais 14 et 15 seront alimentés et leurs contacts seront fermés, alors que les relais 16, 17 et 18 resteront non alimentés. La présence de la lettre *B* dans le code transmis signifie que les contacts 36, 39 et 40, représentant les impulsions positives du *B* seront en

> contact avec la ligne 32 qui est connectée à la batterie, et les contacts 37 et 38, représentant les impulsions négatives de ce caractère, seront en contact avec la ligne 33 qui est mise à la masse.
> Il résulte de cette combinaison de contacts dans les deux émetteurs, […] puisque le bras de distribution 10 tourne autour des contacts 1 à 5, qu'une impulsion sera transmise sur la ligne à partir des contacts 2, 4, et 5, et qu'aucune impulsion ne le sera à partir des contacts 1 et 3. Cela signifie que le signal «− + − + + » sera transmis sur la ligne, et cela représente la lettre *G*, et non pas la lettre *A* qui était le caractère du message à transmettre »[43].

Dans ce système cryptographique, le chiffrement et le déchiffrement sont des opérations identiques, ce que Vernam ne montre que sur le seul exemple précédent. Autrement dit, appliquer deux fois la clé sur un message redonne le message lui-même.

Cette propriété présente un double intérêt technique. Il n'y a qu'un seul type de réalisation électromécanique à mettre en place. Et les opérations de chiffrement et de déchiffrement s'effectuent automatiquement, sans aucune intervention humaine : elles font intégralement partie du processus de transmission. Le chiffre de Vernam signe en quelque sorte l'acte de naissance de la cryptographie automatique, le « chiffrement en ligne », en même temps que celui du caractère aléatoire de la clé.

En outre, et contrairement à bien d'autres systèmes ultérieurs – celui de l'*Enigma* par exemple –, le message clair parvient au destinataire

---

[43] *« Let us suppose that the first character of the message to be transmitted is* A*. The code signal of* A *is « + + – – – », where « – » represents an « open » or « spacing » impulse and « + » represents* a *« closed » or « marking » impulse in the system here illustrated although it will be understood that positive and negative current impulses may be used instead of closed and open circuit operation if desired. For ciphering and deciphering the message, the ciphering devices at the opposite ends of the line are provided with identical sections of tape upon which are recorded a series of code signals which are preferably selected at random but if desired may themselves represent a predetermined series of letters or words. Let us suppose that the letter* B *happens to be in the ciphering transmitter at the same moment that the letter* A *is being sent from the normal transmitter The code for the letter* B *is « + – – + + ». The sending of* A *from the normal transmitter means that the contacts 25 and 26 will be closed, while the contacts 27, 28 and 29 are open. Thus, relays 14 and 15 will be energized, and close their contacts, while relays 16, 17 and 18 remain unergized* [sic]*. The presence of the letter* B *in the code transmitter means that contacts 36, 39 and 40, representing the plus impulses for* B *will be in contact with the bus-bar 32, which is connected to battery and that contact 37 and 38, representing the negative impulses for this character will be in contact with bus-bar 33 which is grounded.*
As a result of this combination of contacts in the two transmitters, […] as the distributer arm 10 rotates over the contacts 1 to 5, impulses will be transmitted to the line from contacts 2, 4 and 5, and none from the contacts 1 and 3. This means that signal « – + – + + » will be transmitted over the line and this signal represents the letter G *and not the letter* A *which is the character of the message to be transmitted* ». Vernam, « Secret Signaling system ».

directement sous forme imprimée. Et si ce n'est pas là une totale nouveauté[44], cette impression directe à l'arrivée du téléscripteur se conjugue avec la vitesse de la frappe au clavier pour rendre particulièrement efficace ce mode de transmission chiffré. En tous cas, puisque le code Baudot est public, le secret du système de Vernam repose exclusivement sur celui du ruban-clé, ce qui correspond aux *desiderata* de Kerckhoffs.

Exemple de chiffrement d'un message utilisant le système de Vernam

Le mode de chiffrement de Vernam	Le chiffrement d'un message	
« + » associé à « + » donne « – »	Clair	+ + – – –
« + » associé à « – » donne « + »	Clé	+ – – + +
« – » associé à « + » donne « + »	Chiffré	– + – + +
« – » associé à « – » donne « – »		
	Le déchiffrement du chiffré	
	Chiffré	– + – + +
	Clé	+ – – + +
	Clair	+ + – – –

Vers le « one-time pad system »

Ce système est installé chez AT&T dès la note de Vernam du 17 décembre 1917. Et la *Navy* en est rapidement informée par le biais de la *Western Electric Company*, entreprise fabricante de AT&T. Il est adopté dès 1918 par le *Signal Armed Corps*, où le Major Joseph O. Mauborgne[45] (1881-1971), cryptologue et responsable du service des transmissions, en reconnaît immédiatement l'intérêt. Mauborgne a établi les premières liaisons radio aéroportées dès avant la guerre. Formé à l'école de Hitt, il dirigera la division *Engineering and Research* et le laboratoire du *Signal Corps* au Bureau des Standards après la Première Guerre Mondiale. Comme Hitt avant lui, il participe amplement à établir les conditions d'une cryptologie efficace avec les nouveaux moyens de communication mobilisés par l'armée. Impliqué dans la réalisation de l'invention de Vernam, il va en dégager les caractéristiques théoriques que son inventeur ne faisait qu'indiquer dans le texte de son brevet.

[44] Kahn, *The Codebreakers*, p. 397.

[45] Mauborgne a déjà publié en 1914 le premier décryptement connu du chiffre de Playfair, et en 1917, il a imposé à l'armée le cylindre de chiffrement élaboré par Hitt, qui sera intégré à la réalisation du M-94 en 1922.

Mauborgne se penche sur la question de la réalisation de rubans perforés de caractère erratique. Afin d'éviter la manipulation de rubans trop longs, il combine d'abord deux rubans, de 1000 et 999 marques respectivement, produisant ainsi une clé de 999 000 caractères sans répétition. Mauborgne établit, sinon formellement, du moins sur l'exemple de deux clés particulières, qu'une telle combinaison présente certaines faiblesses. Fidèle aux leçons de Hitt qui déclarait dès 1914 qu'une bonne clé devait être « comparable en longueur au message lui-même »[46], il conjugue les deux exigences susceptibles d'assurer l'inviolabilité du système : une clé « *endless and senseless* », c'est-à-dire aussi longue que le message et dépourvue de signification. Encore faut-il qu'elle ne soit utilisée qu'une seule fois. Mauborgne caractérise ainsi ce qui est aujourd'hui connu, depuis la démonstration formelle de Shannon de cette inviolabilité, sous le nom de « *one-time pad system* ».

Ce système de chiffrement automatique, en dépit de toutes ces qualités nouvelles, sera néanmoins très lourd à utiliser. En période de guerre, la quantité de messages transmis est colossale, et affecte tous les niveaux de l'armée, du commandement au soldat sur le champ de bataille. L'énorme quantité de clés à produire, à enregistrer et à distribuer est donc un obstacle majeur, auquel il faut ajouter la nécessité de contrôler la destruction des clés après leur première utilisation. Le volume du travail à produire déborde de beaucoup les moyens et les effectifs chargés de la transmission des messages.

> La réutilisation deux fois d'un ruban-clé peut être fatale, surtout en temps de guerre. Historiquement, il est arrivé que le décryptement de certains messages soit rendu possible par une telle erreur d'utilisation.
> Si on connaît déjà un autre message clair chiffré avec la même clé, on peut trouver le clair du second message. Il suffit pour cela de combiner les deux chiffrés. Puisque la combinaison de la clé avec elle-même annule toute impulsion, la combinaison des deux chiffrés est identique à celle des deux messages clairs. En combinant ce résultat avec le message clair connu, on obtient alors le message clair inconnu.

L'usage du « *one-time pad system* » ne sera donc pas généralisé, mais restera privilégié pour les communications particulièrement sensibles. La confection de clés réservées à un seul message sera ainsi proposée en Allemagne en 1921 par Werner Kunze (1908-86), Rudolf Schauffler et Eric Langlotz, et en 1926 par les Soviétiques à partir d'une indiscrétion d'un

[46] Cette condition n'est pas nouvelle. L'amorce d'une telle idée se trouve chez Vigenère et chez Babbage, conscients que plus la clé sera longue, plus le décryptement s'avérera difficile. Et Porta insistait déjà sur l'intérêt d'utiliser des clés longues et dénuées de sens. La réalisation matérielle du système de Vernam rend cette intuition efficiente et permet de l'expliciter.

Britannique du *Governement Code and Cypher Service* (GC&CS). Pendant la Seconde Guerre Mondiale, la machine de la compagnie Lorenz contre laquelle ce même service élaborera le premier ordinateur, le *Colossus*, utilisait des clés générées pseudo-aléatoirement à partir de roues codeuses. Elle était réservée au chiffrement des communications entre le quartier général de Hitler et ceux des différents groupes d'armées. Et le « téléphone rouge » n'est autre qu'une ligne réservée aux échanges directs entre Washington et Moscou, installée en 1963 après la crise de Cuba. Les bandes aléatoires étaient transmises par valise diplomatique et détruites après chaque utilisation.

L'invention de Vernam se cristallise donc en une réalisation technique impulsée par les nouveaux moyens de communication. La découverte récente d'un système de même type, élaboré par un banquier aux États-Unis dans les années 1880, mais resté lettre morte[47], illustre parfaitement cette nécessaire existence de besoins techniques et culturels pour que la nouveauté d'une idée se transforme en innovation investie socialement. Dans les années 1920, le travail de Vernam reste malgré tout dans le domaine de l'ingénierie. Pendant l'entre-deux-guerres, mathématiciens et ingénieurs travaillent et s'expriment – à quelques exceptions près – chacun dans leur milieu et leur langage. La restructuration des milieux scientifiques aux États-Unis pendant la Seconde Guerre Mondiale permettra leur convergence.

MATHEMATISATION DE LA CRYPTOGRAPHIE

Les travaux de Claude E. Shannon constituent une étape essentielle du basculement des pratiques matérielles vers la formalisation mathématique. Shannon est reconnu comme l'auteur d'une théorie nouvelle, la théorie mathématique de l'information, élaborée entre 1943 et 1949, et fondée sur une notion nouvelle qu'il appelle la « quantité d'information », reposant sur la théorie des probabilités. Mais dès 1937, la double formation technique et mathématique de cet ingénieur le conduit d'abord à élaborer un langage commun aux ingénieurs et aux mathématiciens, en traduisant en termes d'algèbre de Boole l'organisation logique d'une machine analogique : l'analyseur différentiel. Pendant la Seconde Guerre Mondiale, Shannon va investir la théorie des probabilités comme langage unificateur entre la cryptologie – qu'il utilise comme outil heuristique – et la théorie de l'information dont il élabore les concepts.

[47] Bellovin, « Frank Miller, Inventor of the One-Time Pad ».

Shannon n'est certes pas le premier, surtout à cette époque, à faire entrer les mathématiques dans le champ de la cryptologie. Déjà au cours des années 1930, Lester S. Hill (1890-1961) avait explicité le chiffrement en termes d'algèbre modulaire, et appliqué le calcul matriciel à la cryptographie[48]. Et William Friedman, déjà cité, utilise le calcul des probabilités en cryptologie pour élaborer son « indice de coïncidence »[49] en 1921. Dans ces deux cas, les mathématiques interviennent comme un outil ponctuel dans un corpus dont la présentation générale ne change pas. Parallèlement, d'autres auteurs ont abordé la mathématisation des circuits de téléphone : Paul Ehrenfest (1880-1933) en 1910 en Russie, Vladimir I. Shestakov (1907-87) en 1945 en URSS, et Akira Nakashima (1908-70) en 1935 au Japon[50]. Mais aucun d'eux n'a bénéficié d'un contexte aussi pluridisciplinaire que celui de Shannon, qui a assuré à la fois l'extension et la postérité de ses nouvelles théories. Le travail de Shannon va beaucoup plus loin : il excelle dans la formulation mathématique des problèmes qu'il rencontre en tant qu'ingénieur, et va restructurer parallèlement la cryptologie et la théorie de l'information à partir de leur reformulation analytique, précisant soigneusement la signification des théorèmes mathématiques pour l'une et l'autre de ces applications. Il produit ainsi une théorie mathématique de la cryptographie fondée sur la notion d'information.

[48] Hill, « Cryptography in an Algebraic Alphabet », « Concerning Certain Linear Transformations Apparatus of Cryptography ». Professeur de mathématiques à *New York City University*, il a beaucoup travaillé en cryptologie pour l'armée des États-Unis, la Marine et le Département d'Etat pendant l'entre-deux-guerres et la Seconde Guerre Mondiale. Il a enseigné à l'université américaine de Biarritz pendant sa courte existence en 1945-46. L'essentiel de ses recherches en cryptologie reste classé confidentiel.

[49] Friedman, *The Index of Coincidence.* S'il a commencé ses recherches dans le laboratoire privé d'un millionnaire états-unien à Riverbanks, il intègre le département de la Défense en 1921, et dirigera ensuite le *Signals Intelligence Service* (SIS) pendant plus d'un quart de siècle. Cryptanalyste de premier plan, il participe très activement à l'enseignement et à la mécanisation de la cryptologie pendant l'entre-deux-guerres et pendant la Seconde Guerre Mondiale. Il a brisé le code japonais *Purple* en 1939, qui utilisait une machine à chiffrer à rotors de même type qu'*Enigma.* Il a contribué à l'élaboration d'un vocabulaire spécifique, introduisant en particulier le terme « cryptanalyse ».

[50] Ségal, *Le zéro et le un*, pp. 76 et 261. Trogemann, Nitussov et Ernst, *Computing in Russia*, pp. 57-68. Stankovic et Ascoal, *From Boolean Algebra to Switching Circuits and Automata*, pp. 121-124 et 163-166. L'histoire des mathématiques regorge de semblables cas d'inventions simultanées – dont celle du calcul infinitésimal par Newton et Leibniz est sans doute la plus célèbre – et qui relativise grandement la notion de « génie ».

L'expression algébrique du montage de l'analyseur différentiel

La formation mathématique de Shannon comme ingénieur dans les années 1920 est tout à fait nouvelle. Il étudie à l'Université du Michigan, l'une des récentes universités d'état qui entrent alors en compétition avec les anciennes universités privées de l'est des États-Unis[51]. L'une des principales innovations est précisément l'introduction des mathématiques dans le cursus des ingénieurs. Et le *Massachussetts Institute of Technology* (MIT), où Shannon va travailler comme assistant-chercheur à partir de 1936, est un centre de recherches mathématiques tout à fait exceptionnel, où l'étude des mathématiques pures s'accompagne d'une philosophie utilitariste explicite. Entre 1927 et 1931, l'équipe de Vannevar Bush (1890-1974) y a conçu et construit une imposante machine, l'analyseur différentiel, qui permet d'obtenir graphiquement la solution d'équations différentielles dont les conditions initiales sont connues. Chargé de la maintenance de cet analyseur, Shannon va s'employer à optimiser son fonctionnement, en simplifiant l'organisation logique de ses circuits, qui connectent des intégrateurs analogiques à des organes d'opérations, et comportent de nombreuses boucles de rétroaction. Ces circuits sont spécifiques à différentes classes de problèmes, et leur montage nécessite la collaboration des ingénieurs, des physiciens et des mathématiciens[52]. Dès l'été 1937, Shannon fait un stage au *Bell Telephon Laboratories*, où il entrera pour quinze ans en 1941, et qui est alors le plus grand laboratoire privé du monde en matière de communications, avec plus de 1400 chercheurs dès les années 1920, travaillant sur les systèmes de contrôle automatiques et les analyses de stabilité. Dès avant la guerre, Shannon est donc déjà au cœur des meilleures institutions de recherche en mathématiques appliquées, dont le caractère stratégique au cours de la Seconde Guerre Mondiale va encore accroître l'importance. En 1956, le MIT créera spécialement pour lui une chaire de théorie de l'information au département du Génie électrique.

Comme il le confie lui-même, Shannon a étudié la logique symbolique et l'algèbre de Boole à l'université du Michigan, et c'est fort de cet enseignement qu'il a l'idée d'interpréter les circuits à relais et commutateurs en termes logiques, bien avant la conception et la mise au point des premiers ordinateurs. En notant $X_{ab} = 0$ le cas où le courant passe, et $X_{ab} = 1$ le cas où le courant ne passe pas entre deux points *A* et *B* du circuit, ainsi que (+) la combinaison de deux circuits en série et (•) celle de deux circuits en

[51] Créées à l'époque coloniale, elles sont regroupées sous le nom de *Ivy League.* Il s'agit des universités de Harvard à Cambridge, de Yale à New Haven, de Princeton, de Pennsylvanie à Philadelphie, Columbia à New York, Brown à Providence, de Darmouth à Hannover et Cornell à Ithaca.

[52] Bush, « The Differential Analyzer » ; Durand-Richard, « Planimeters and Integrpahs in the 19th century ».

parallèle, il établit une « parfaite analogie » entre l'étude des circuits et le calcul propositionnel, qui lui permet d'opérer sur les circuits en termes d'opérations algébriques[53]. Son mémoire, intitulé « A Symbolical Analysis of Relay and Switching Circuits », montre comment traduire un tel circuit en un ensemble d'équations logiques dont les termes, représentant les relais et les commutateurs, ne peuvent prendre que les valeurs 0 et 1.

Mais ce travail n'est pas une simple application des mathématiques. Shannon s'y réfère à l'ensemble des auteurs qui ont développé l'algèbre de la logique, non seulement George Boole (1815-64) et Edward Huntington (1874-1952), mais aussi Louis Couturat (1868-1914) et Alfred Whitehead (1861-1947). Il a parfaitement saisi l'approche symbolique de la logique mathématique et l'importance des analogies opératoires par lesquelles cette école de pensée s'autorise le transfert d'un système symbolique à un autre pour peu que les propriétés opératoires s'expriment avec les mêmes formules[54]. Il écrit :

> « Nous sommes maintenant en mesure de montrer l'équivalence de ce calcul avec certaines parties élémentaires du calcul des propositions. L'algèbre de la logique initialement développée par Boole, est une méthode symbolique pour étudier les relations logiques. Les symboles de l'algèbre booléenne admettent deux interprétations logiques. […] Si […] ses termes sont pris pour représenter des propositions, nous avons le calcul des propositions, dans lequel les variables sont limitées aux valeurs 0 et 1, […] »[55].

Pour sa part, Shannon procède par « induction parfaite », démontrant au cas par cas à partir des tables de vérité, la possibilité de simplifier les circuits en obtenant les formes normales des propositions logiques correspondantes. La détermination des formes normales permet d'optimiser le circuit correspondant.

Ce mémoire, soutenu en 1937 et publié en 1938 dans une revue technique d'électricité, recevra le prix Alfred Noble en 1940. Il sera immédiatement exploité aux *Bell Labs* et connaîtra une diffusion exceptionnelle pour un travail de Master. Howard Gardner le qualifie de « mémoire le plus important du siècle ». Ce langage commun aux ingénieurs

---

[53] Ségal, *Le zéro et le un*, pp. 72-88. Shannon, « A Symbolic Analysis of Relay and Switching Circuits », p. 475.

[54] Durand-Richard, « De l'algèbre symbolique à la théorie des modèles ».

[55] « *We are now in a position to demonstrate the equivalence of this calculus with certain elementary parts of the calculus of propositions. The algebra of logic originated by George Boole, is a symbolic method of investigating logical relationships. The symbols of Boolean algebra admit of two logical interpretations. […]. If […] the terms are taken to represent propositions, we have the calculus of propositions to which variables are limited to the values 0 and 1, […]* ». Shannon, « A Symbolical Analysis of Relay and Switching Circuits », p. 474.

et aux mathématiciens fait entrer un champ entier de l'ingénierie parmi les applications de la logique mathématique. Il débouche sur le basculement des préoccupations de l'ingénieur en communication, de l'étude des phénomènes physiques de propagation à l'analyse des circuits. Celle-ci pourra à son tour être transférée à l'analyse de toutes sortes de réseaux. Ce travail de Shannon sur l'analyseur différentiel ne s'arrête pas là. Il approfondit son propos en 1941 dans « A Mathematical Theory of the Differential Analyzer », qui sera de première importance dans la réalisation des grands calculateurs et des premiers ordinateurs au cours de la Seconde Guerre Mondiale[56]. Parallèlement, Shannon s'oriente plus directement vers des études de mathématiques[57] au MIT, préparant une thèse sous la direction de Bush, « An Algebra for Theoretical Genetics », soutenue en 1940, où il poursuit le travail de formulation mathématique qui lui permet de généraliser certaines lois connues de la dynamique des populations. Cette solide formation mathématique sera constamment mobilisée et enrichie dans ses travaux ultérieurs sur la théorie de l'information et la cryptographie.

Cryptographie et théorie de l'information

Dès 1940, Shannon est impliqué dans l'effort de guerre, qui se traduit aux États-Unis par un renforcement très structuré des relations entre la Défense, l'Industrie et les Universités au sein du *National Development and Research Committee* (NDRC), dirigé par Bush. Shannon travaille à l'élaboration d'une arme automatique anti-aérienne, le M-9, qui doit optimiser la trajectoire de tir[58], au sein de la section D2 du contrôle de tir, à laquelle sont associées les *Bell Labs* et le MIT. Le calcul prédictif des coordonnées de la position de la cible en vol, à partir de la transmission de ses coordonnées par radar, recourt à l'analyse statistique et au calcul des probabilités, ainsi qu'à la technique de lissage des données transmises. Il s'agit d'éliminer les fluctuations du signal et les effets du bruit. La voie est ainsi ouverte à Shannon pour mener de front l'analyse des processus de communication en termes discrets comme en termes continus. Le rapport commun rédigé en 1946 par Ralph B. Blackman (1904-90), Hendrik W.

[56] Au cours de la Seconde Guerre Mondiale, Bush, alors directeur du NDRC, a lancé un grand projet d'analyseur différentiel électronique, le *Rockfeller Differential Analyzer*, qui devait être un des plus grands instruments scientifiques des temps modernes » à la sortie de la guerre. Ce projet a été développé en collaboration avec Samuel J. Caldwell (1904-60), au département d'Ingénierie du MIT. Mais il a été supplanté par l'ENIAC (*Electronic Numerator Integrator Analyzer and Computer*) à l'issue de la guerre.

[57] Il suit à cette époque les cours de Norbert Wiener (1890-1964). Ségal, *Le zéro et le un*, p. 81.

[58] De nombreux exemplaires du M-9 seront fabriqués et joueront un rôle essentiel au moment de la bataille d'Angleterre et du débarquement allié du 6 juin 1944, *ibid*., pp. 93-99.

Bode (1905-82) et Shannon, « Data Smoothing and Prediction in Fire-control System », traite déjà du problème du contrôle de tir en termes de transmission, manipulation et utilisation du « renseignement » – « *intelligence* » en anglais –, terme qui se réfère alors au secret et à l'information. Aussi bien l'article sur ce sujet publié en 1950 par Bode et Shannon[59], que la contribution de Shannon à l'article collectif « The Philosophy of Pulse Code Modulation », publié en 1948, hériteront directement de cette ligne de recherche.

Mais l'étape la plus déterminante, et trop souvent ignorée, du travail de Shannon pour l'élaboration de sa théorie mathématique de l'information réside sans nul doute dans ses travaux de cryptologie menés aux *Bell Labs* pour la division D2 du NDRC de 1943 à 1945. En septembre 1945, Shannon rédige un rapport confidentiel, « A Mathematical Theory of Cryptography », qui sera déclassifié, et associé à des matériaux de 1946 pour être publié en 1949 sous le titre « Communication Theory of Secrecy Systems ». Entre temps, il aura publié en 1948 sa célèbre « Mathematical Theory of Communication », dont il a déjà conçu un mode de représentation dès 1939, sans toutefois introduire à cette époque le calcul des probabilités[60]. Même s'il présente le second texte publié comme une application du premier, leur élaboration a donc été menée en parallèle. Quiconque en douterait pourrait vérifier que le texte qui porte sur la théorie de l'information est beaucoup plus lisible après la lecture du texte qui traite des systèmes secrets. C'est à partir d'analogies opératoires désormais fondées sur la théorie des probabilités que Shannon peut identifier système crypté et canal de communication bruité, tous deux intervenant désormais aussi bien dans le domaine militaire que dans le domaine civil.

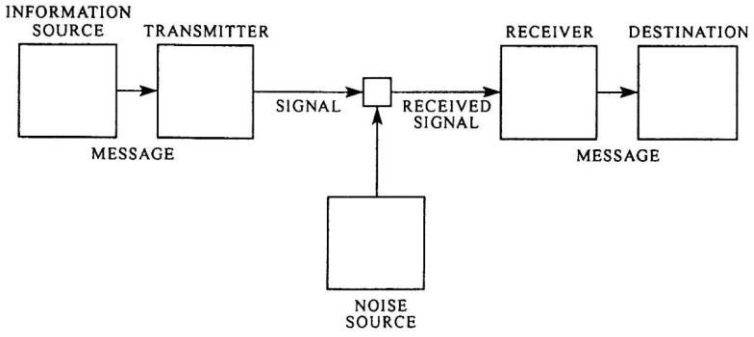


Fig. 1—Schematic diagram of a general communication system.

[59] Bode et Shannon, « A simplified Derivation ».
[60] Shannon, lettre à Vannevar Bush du 16 février 1939, *Collected Papers*, p. 455-456.

Le schéma devenu classique que donne Shannon d'un canal de communication présente la même structure pour ces deux types de systèmes : elle distingue la source, le transmetteur, le canal proprement dit, le récepteur, et le destinataire du message. Selon le cas, le transmetteur transforme le message en signal ou en chiffré et le récepteur effectue l'opération inverse.

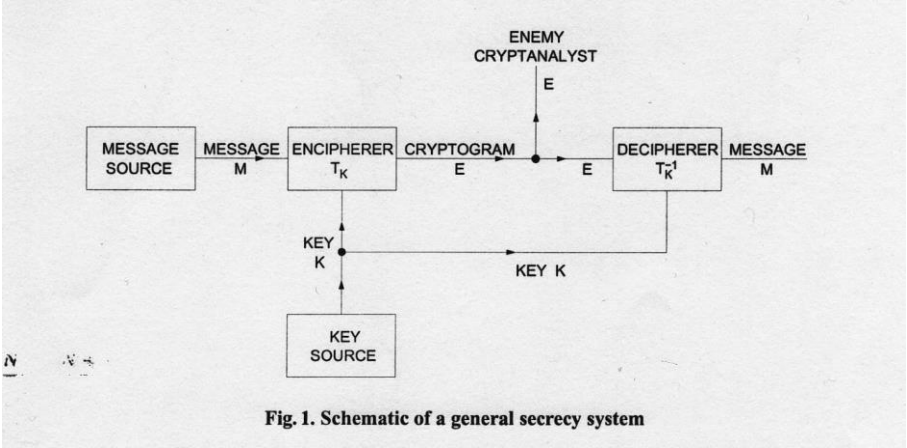


Fig. 1. Schematic of a general secrecy system

Dans ses deux articles, Shannon s'appuie sur les plus récents développements des mathématiques : théorie des ensembles, théorie des fonctions[61] et théorie moderne de la mesure, se référant directement à Andrei N. Kolmogoroff (1903-87), Maurice Fréchet (1878-1973), John von Neumann (1903-57) et Oskar Morgenstern (1902-77), ainsi qu'à Norbert Wiener (1894-1964)[62] lorsqu'il aborde les probabilités continues. La formulation mathématique qu'il propose concerne le système dans sa globalité :

> « L'aspect significatif est que le message présent est un, *sélectionné à partir d'un ensemble* de messages possibles. Le système doit être conçu pour opérer sur chaque sélection possible, et non pas seulement sur celle qui est présentement choisie, puisque celle-ci est inconnue au moment de la conception du système »[63].

[61] Shannon utilise abondamment les diagrammes de représentation des fonctions, où des flèches – les clés – relient les éléments de l'ensemble de départ – les messages clairs – aux éléments de l'ensemble d'arrivée – les cryptogrammes.
[62] Voir la note 57.
[63] « *The significant aspect is that the actual message is one selected from a set of possible messages. The system must be designed to operate for each possible selection, not just the*

Sa définition de la quantité d'information d'un système est d'abord explorée sur des exemples de « langages artificiels » que produit Shannon comme approximations de plus en plus raffinées du caractère stochastique du langage naturel. La cryptologie y intervient explicitement comme outil heuristique, permettant d'approcher cette formulation mathématique, puisque les approximations probabilistes produites pour les lettres, les digrammes et les trigrammes d'un message en anglais proviennent d'analyses cryptographiques[64]. Et la définition elle-même n'intervient qu'à la suite d'une longue discussion des conditions qu'elle doit remplir pour être opératoire pour l'ingénieur. C'est ainsi que Shannon parvient à la « seule définition qui satisfasse ces conditions » :

$$H = -K\sum_{i=1}^{n} p_i \log p_i$$

Dans cette formule, Shannon pose $K = 1$ pour pouvoir identifier cette définition à l'entropie d'un système donnée par le théorème de Boltzmann, telle qu'elle a été antérieurement définie en mécanique statistique[65]. Elle mesure aussi bien le choix que l'incertitude que représente un message parmi tous les messages possibles, les p_i représentant les probabilités d'occurrence de chacun d'entre eux. Elle est donc maximale lorsque la situation est la plus incertaine, à savoir dans le cas de l'équiprobabilité. Elle concerne aussi bien le cryptanalyste cherchant à retrouver le message clair à partir du cryptogramme, que l'ingénieur face au bruit perturbant la qualité de la transmission et que Shannon considère pour la première fois comme une variable aléatoire[66]. Dans les deux cas, il identifie la connaissance avec « un ensemble de propositions auxquelles sont associées des probabilités »[67].

De ce fait, un système secret est défini abstraitement comme un ensemble d'opérations ou de transformations T_i d'un espace – l'ensemble des messages possibles – dans un autre – l'ensemble des cryptogrammes possibles. Le cryptogramme E résulte de l'application à un message M d'une telle transformation T caractérisée par la clé i – devenue clairement aléatoire – de telle sorte que :

---

one which will actually be chosen since this is unknown at the time of design », Shannon, « A Mathematical Theory of Communication », p. 5.

[64] Pratt, *Secret and Urgent.* Dewey, *Relative Frequency of English Speech Sounds.*

[65] Shannon, « A Mathematical Theory of Communication », p. 11. Shannon se réfère ici à Tolman, *Principles of Statistical Mechanics.* Cette identification de la mesure de l'information à l'entropie d'un système donnera lieu à de très nombreuses interrogations philosophiques, notamment dans ses applications à l'informatique. Atlan, *Entre le cristal et la fumée*, pp. 5-129.

[66] Shannon, « A Mathematical Theory of Communication », p. 19.

[67] Shannon, « Communication Theory of Secrecy Systems », p. 657.

$$E = T_i\,(M)$$

Shannon prend soin de préciser que ces transformations doivent avoir un inverse unique, afin que le message clair puisse être retrouvé à partir du cryptogramme par la transformation :

$$M = T_i^{-1}(E)$$

Et les différents modes de chiffrement connus, de César à Vernam, sont alors réinterprétés dans cette formulation mathématique. À chaque clé et à chaque message sont associées des probabilités *a priori*, qui proviennent du caractère stochastique du langage, et qui sont donc connues du cryptographe et du cryptanalyste. Si par exemple, les messages possibles sont les suites de lettres de longueur *N* dans une langue, les probabilités *a priori* ne sont autres que les fréquences des occurrences des lettres de ces suites dans cette langue. Comme l'écrivait déjà Kerckhoffs, il faut penser que « l'ennemi[68] connaît le système utilisé »[69]. Celui-ci, ayant intercepté le message, peut alors calculer les probabilités *a posteriori* des messages et des clés susceptibles d'avoir produit ce cryptogramme. Toute l'étude de Shannon porte sur les relations entre ces probabilités *a priori* et *a posteriori*[70], et le problème général de la cryptanalyse n'est autre, pour Shannon, que le calcul de ces probabilités *a posteriori*.

Ces définitions marquent une mutation essentielle de la cryptologie, dans la mesure où elles permettent à Shannon – et à ses successeurs – de structurer son analyse de la cryptologie à partir des propriétés mathématiques des systèmes secrets, celles qui proviennent de cette définition ensembliste, comme celles qui découlent des probabilités associées à chaque message et à chaque clé, qui sont en général celles des suites possibles de lettres en anglais.

Analyse mathématique des systèmes secrets

La structure statistique du langage est donc au cœur de toutes les analyses de Shannon dans ces deux articles. Chaque message y est considéré comme une suite de lettres dont chacune est choisie dans un ensemble donné

[68] Tenant compte du contexte élargi dans lequel il travaille, Shannon prend soin de préciser que ce terme provient des applications militaires, et qu'il « est couramment utilisé dans le vocabulaire cryptographique pour dénoter quiconque est susceptible d'intercepter un cryptogramme ». *ibid* ., p. 657.

[69] Il peut même disposer d'un équipement spécial pour intercepter et enregistrer les messages.

[70] Elles font intervenir le théorème de Bayes, qui joue un rôle central dans la théorie des probabilités.

– l'alphabet en général – avec une probabilité donnée. Dans le cas le plus fréquent, celui du langage naturel, chacune de ces probabilités dépend des choix précédents, ce qui permet de caractériser l'ensemble des suites de lettres comme un processus de Markov discret, qu'il suppose ergodique, c'est-à-dire statistiquement homogène. Shannon utilise alors toutes les propriétés de l'entropie élaborées en mécanique statistique pour explorer celles de la quantité d'information. Dans le cas d'un canal bruité, l'entropie s'applique aux signaux transmis comme aux signaux reçus ; dans le cas d'un système secret, elle concerne l'ensemble des messages aussi bien que l'ensemble des clés. Dans les deux cas, Shannon caractérise l'ambiguïté du signal reçu par l'entropie conditionnelle du message transmis connaissant le message reçu, qu'il nomme l'équivocation[71] : c'est l'information additionnelle qui doit être fournie pour restituer le message reçu. L'incertitude correspondante – fortuite dans le premier cas et délibérée dans le second – peut être compensée en envoyant l'information sous une forme redondante, qui peut utiliser un encodage approprié ou la redondance propre au message, exprimant précisément « de quels éléments il peut être réduit sans perdre aucune information »[72]. La spécification mathématique de la redondance joue un rôle important dans ces travaux. Dans le domaine des télécommunications, Shannon a d'abord travaillé à réduire la bande de fréquence utilisée en s'appuyant sur le fait que la voix humaine est très redondante. Et c'est à partir de cette recherche d'une réduction de la redondance qu'il a envisagé que la quantité d'information transmise soit d'autant plus grande que la redondance est plus faible.

Quant aux transformations de l'espace des messages possibles dans l'espace des cryptogrammes possibles, elles sont susceptibles d'être combinées, en tant qu'opérations sur les systèmes, soit afin d'engendrer de nouveaux types de systèmes secrets, soit d'en fournir de possibles décompositions, donc de contribuer à la résolution de cryptogrammes. La plupart du temps, ces deux espaces étant identiques, ces transformations sont des endomorphismes, dit Shannon, et les systèmes secrets ont une structure d'« algèbre associative linéaire », dont toutes les propriétés peuvent donc être attribuées aux systèmes secrets. Shannon intègre à cette approche théorique l'ensemble des systèmes connus, dont il renvoie l'étude pratique aux ouvrages de cryptographie existants[73]. Cette analyse débouche notamment sur une classification théorique des systèmes secrets qui permet

[71] L'équivocation est un indice théorique du secret, théorique en ce sens qu'elle ne tient aucun compte de la limitation de temps dans laquelle travaille le cryptanalyste. Elle donne une approximation de la quantité de messages à intercepter pour obtenir une solution cryptanalytique.

[72] Par exemple, la lettre *u* suivant toujours la lettre *q*, elle peut être omise sans perdre aucune information.

[73] Notamment Givierge, « Cours de cryptographie », et Gaines, « Elementary Cryptanalysis ».

d'optimiser le travail du cryptanalyse, et qui s'accompagne d'une analyse pratique de la quantité de travail requis pour le décryptement, ce qui garde une grande importance pour Shannon. Il distingue :
– le secret pur, pour lequel toutes les clés sont équivalentes, au sens où elles conduisent toutes au même ensemble de probabilités *a posteriori*. Il forme un groupe et se décompose en sous-systèmes fermés disjoints, stables dans les opérations de chiffrement. Un cryptogramme intercepté ne permet de spécifier qu'une sous-classe de messages clairs.
– les systèmes semblables, dont les cryptogrammes se correspondent terme à terme avec les mêmes probabilités *a posteriori*.
– le secret parfait, où les probabilités *a posteriori* sont égales aux probabilités *a priori* et pour lequel intercepter un message ne donne donc aucune information au cryptanalyste[74]. Un tel système est particulièrement utile pour les correspondances entre les plus hauts niveaux de commandement, mais il requiert une énorme quantité de clés. C'est par exemple le cas du chiffrement de Vernam.
– le système idéal, pour lequel l'équivocation de la clé et celle du message ne s'annulent pas quand le nombre de lettres interceptées augmente, laissant le cryptanalyste dans l'impossibilité théorique de déterminer une solution unique pour un cryptogramme intercepté.

Le travail de Shannon, essentiellement connu pour avoir fondé la théorie mathématique de l'information, est donc tout aussi déterminant pour la cryptologie. Celle-ci a manifestement une fonction heuristique considérable pour inciter Shannon à penser la quantité d'information en termes de probabilités, et indépendamment de la signification des messages. Mais au-delà de cette fonction heuristique, elle s'est trouvée elle-même totalement renouvelée par la restructuration qu'opère Shannon en y introduisant les concepts dégagés en théorie de l'information. Cette reformulation mathématique de la cryptologie permet de synthétiser l'ensemble des méthodes existantes[75]. Mais surtout, elle offre aux successeurs de Shannon un vaste champ théorique, structuré par l'ensemble des possibles, et qui conjugue les préoccupations de l'ingénieur à celles du mathématicien.

Information et signification

Historiens et enseignants insistent de manière récurrente sur le fait que le travail de Shannon autorise un abandon de toute référence à la signification

[74] Shannon, « Communication Theory of Secrecy Systems », pp. 679-683.
[75] Le lecteur est souvent impressionné par le niveau d'abstraction de ces articles. Or, non seulement Shannon était à la fois ingénieur et mathématicien, mais surtout, il n'a pas été autorisé à montrer dans ses articles les éléments qui auraient pu permettre au lecteur d'en déduire les usages applicatifs. Roch, *Claude E. Shanon, spielzeug, leben*, p. 136.

des messages échangés. Et cette question fait l'objet de discussions réitérées autour de l'idée selon laquelle la transmission des messages sur les canaux de communication est indépendante de toute signification. Tout se passe comme si l'existence de ces systèmes de communication rendait superflue la référence au sens. Cette affirmation soulève un problème philosophique majeur, dès lors qu'est prise en compte l'importance de la fonction signifiante pour l'humain, aussi bien au plan individuel que collectif

Il est vrai qu'en 1948, dans « A Mathematical Theory of Communication », Shannon affirme d'emblée que les « aspects sémantiques de la communication ne sont pas pertinents pour le problème de l'ingénieur »[76]. Ce qui ne signifie pas pour autant qu'il s'en détourne totalement. La rédaction même de ses articles témoigne au contraire du soin qu'il prend à préciser pour l'ingénieur la signification des mathématiques qu'il introduit. Il adopte une démarche tout à fait constructive en examinant soigneusement les conditions que doit remplir la quantité d'information pour constituer une grandeur mesurable, sur laquelle l'ingénieur pourra pratiquer des opérations mathématiques conformes à sa propre expérience. C'est en cherchant la fonction mathématique qui va lui permettre d'exprimer le mieux cette notion qu'il définit l'unité de mesure correspondante, le fameux *binary digit* (bit)[77]. Quand il traite des probabilités *a priori* et *a posteriori*, il prend soin de discuter des enjeux épistémologiques attachés à l'intervention du théorème de Bayes et aux relations entre probabilités objectives et probabilités subjectives[78]. Et surtout, de manière tout à fait caractéristique, tous les théorèmes énoncés sous forme mathématique sont suivis d'un énoncé spécifique, significatif pour l'ingénieur dans son travail. Par exemple, ayant défini la redondance D_N pour N lettres d'un message par la formule :

$$D_N = log\ G - H(M),$$

où G est le nombre total de messages de longueur N, et $H(M)$ l'incertitude attachée au choix du message M, Shannon établit la formule :

$$H(K) - H_E(K) \leq D_N,$$

[76] « *These semantic aspects of communication are irrelevant to the engineering problem* », Shannon, « A Mathematical Theory of Communication », p. 5.

[77] Si ses prédécesseurs aux *Bell Labs*, Ralph V.L. Hartley (1888-1970) et Harry Nyquist (1889-1976), avaient déjà envisagé l'introduction d'une mesure logarithmique de la quantité d'information, Shannon est le premier à dégager l'intérêt d'une mesure probabiliste lorsqu'il traite de front cryptologie et communication.

[78] Shannon, « Communication Theory of Secrecy Systems », p. 646.

où $H(K)$ est l'incertitude attachée à la clé, et $H_E(K)$ l'incertitude conditionnelle attachée à la clé connaissant le cryptogramme. Il précise alors :

> « Ceci montre que, dans un système fermé par exemple, la diminution de l'équivocation de la clé après l'interception de *N* lettres n'est pas plus grande que la redondance de *N* lettres du langage »[79].

Shannon fait suivre le théorème :

> « Une condition nécessaire et suffisante pour avoir un secret parfait est que :
>
> $$P_M(E) = P(E)$$
>
> pour tout *M* et tout *E*, où *M* est le message, *E* le cryptogramme, [$P(E)$ la probabilité *a priori* du cryptogramme, et $P_M(E)$ sa probabilité conditionnelle si *M* est choisi, c'est-à-dire la somme des probabilités de toutes les clés qui produisent *E* à partir de *M*.] C'est-à-dire que $P_M(E)$ doit être indépendant de *M* ».

de l'explication suivante :

> « Dit autrement, la probabilité totale de toutes les clés qui transforment M_i en un cryptogramme donné *E* est égale à celle de toutes les clés qui transforment *Mi* en un même cryptogramme *E* pour tous les M_i et *E* »[80].

En fait, le travail de Shannon permet de renouveler fondamentalement la question de la signification d'un énoncé. Il pose clairement, d'un point de vue technique, la question du lieu de l'énonciation, là où d'autres que lui la poseront d'un point de vue philosophique. En tant qu'ingénieur, et comme il l'écrit à plusieurs reprises : « Le problème fondamental de la communication est celui de reproduire un message sélectionné en un point, soit exactement, soit approximativement, en un autre point »[81]. De fait, la formule par laquelle il définit la quantité d'information – the « *amount of*

---

[79] « *This shows that, in a closed system, for example, the decrease in equivocation of key after* N *letters have been intercepted is not greater than the redundancy of* N *letters of the language* ». *ibid.*, p. 689.

[80] « *A necessary and sufficient condition for perfect secrecy is that* $P_M(E) = P(E)$ *for all* M *and* E. *That is,* $P_M(E)$ *must be independent of* M.
Stated in another way, the total probability of all keys that transform M_i *into a given cryptogram* E *is equal to that of all key transforming* M_j *into the same* E *for all* M_i, M_j *and* E ». *ibid.*, p. 680.

[81] « *The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point* », Shannon, « A Mathematical Theory of Communication », p. 5.

information » – traduit bien le changement de point de vue qu'engage la conceptualisation mathématique de la notion de système. Avec cette définition, qui prend en compte l'ensemble de tous les messages et de toutes les clés possibles, Shannon ne se situe pas à l'intérieur du système, mais totalement à l'extérieur de ce système, cherchant à expliciter les conditions qui vont lui permettre d'en maîtriser l'ensemble des communications. Il insiste abondamment sur le fait qu'un système secret ne signifie pas une transformation, mais un ensemble de transformations – les clés possibles étant aussi importantes que les clés effectivement choisies – et qualifie de « vrais systèmes secrets » les systèmes cryptographiques définis par Kerckhoffs, ceux qui, par opposition aux « systèmes privés », sont destinés à être utilisés collectivement et publiquement[82]. La signification n'a donc pas disparu du champ des préoccupations de Shannon. Mais ce qui signifie pour Shannon ingénieur diffère radicalement de ce qui signifie pour Alice et Bob, simples acteurs du système parmi d'autres. Son travail est hautement significatif pour les développements des communications, du point de vue de l'ingénieur certes, mais plus généralement du point de vue des praticiens des systèmes de communication, et plus encore du point de vue de tous les pouvoirs pour lesquels ils sont mis au point et organisés. Shannon rend donc tout simplement manifeste le fait que la signification d'un énoncé dépend du point de vue de celui qui l'énonce.

Au sortir de la guerre, la production naissante des ordinateurs hérite largement de ce langage commun, forgé par Shannon pour les ingénieurs et les mathématiciens, qui conservaient encore des approches distinctes au moment de leur collaboration autour de l'analyseur différentiel. Ce langage commun contribuera très efficacement à la mutation de l'approche analogique vers l'approche digitale dans la conception et la réalisation des grands calculateurs. À partir des années 1950, la mise en réseau des ordinateurs se heurte à la nécessité de garantir la confidentialité des échanges informatiques, ouvrant de nouveaux défis et de nouvelles perspectives pour la cryptologie.

CRYPTOLOGIE ET INFORMATIQUE

Dans la course aux armements inaugurée par la guerre froide dans les années 1950, l'ordinateur a été une des clés du système de défense, investie dans les recherches sur l'armement nucléaire et dans la surveillance des territoires[83]. La transition des besoins militaires vers le domaine civil sera

[82] Shannon, « Communication Theory of Secrecy Systems », p. 656.

[83] Mis au point au début des années 1950, le programme SAGE (*Semi Automatic Ground Environment*) est un réseau de défense anti-aérienne automatisé qui couvre l'ensemble du territoire des États-Unis. Les ordinateurs en constituent le centre nerveux. Le *Whirlwind*,

grandement favorisée par la collaboration entre défense, universités et industrie, inaugurée aux États-Unis pendant la guerre. L'amenuisement des budgets militaires à la fin de la guerre a conduit les entreprises commerciales à chercher de nouveaux débouchés. Cette évolution a concrétisé l'ancrage de l'informatique dans le monde civil[84] dès le début des années 1970.

Conjugué à l'algébrisation de la logique et au travail de Shannon, l'architecture von Neumann des ordinateurs[85] ouvre la possibilité d'identifier données numériques et instructions, et installe la notion d'algorithme au cœur de la production des logiciels, qui délivrent sous forme abstraite ce que réalisait initialement le montage des calculateurs sous forme câblée.

L'enjeu du secret change une fois de plus de dimension. Comme l'écrit Horst Feistel en 1973, du fait de leur fonctionnement en réseaux : « Les ordinateurs constituent, ou vont constituer, une menace pour la liberté individuelle. Ils contiennent des données personnelles et sont accessibles à partir de terminaux très éloignés »[86]. Contrairement à la formulation de Feistel, il ne s'agit d'ailleurs pas tant de liberté individuelle, celle que recherchent « les amoureux et les voleurs », mais de la sécurité des échanges internationaux et des libertés commerciales, qui ne concernent plus seulement les militaires et les diplomates, mais constituent une « affaire publique ». Sous la pression d'une demande civile de normalisation de plus en plus forte, émanant en particulier du monde bancaire, la NSA (*National Securité Agency*), créée[87] en 1952 aux États-Unis pour assurer le développement et la sécurité de tous les moyens de chiffrement du gouvernement et de l'OTAN, va promouvoir la publication d'algorithmes cryptographiques. Une nouvelle étape est ainsi franchie quant à la nature du secret : l'accroissement de la puissance du chiffrement, et donc, sa résistance à la cryptanalyse, réduisent la part secrète, concrétisant ainsi les principes de Kerckhoffs.

---

premier ordinateur à travailler en temps réel, sera réalisé au MIT dans ce cadre. La firme IBM fut alors chargée d'analyser le *Whirlwind* afin d'en produire industriellement pour les besoins de la défense. Ses modèles IBM 701 et IMB 702, respectivement destinés à des fins militaires et civiles, s'en inspireront directement.

[84] Breton, *Une histoire de l'informatique,* pp. 115-137.

[85] L'architecture Von Neumann est caractérisée par une mémoire unique pour les données et les programmes.

[86] « *There is a growing concern that computers now constitute, or will soon constitute, a dangerous threat to individual privacy* ». Feistel, « Cryptography and Computer Privacy », p. 15.

[87] Son existence est restée secrète jusqu'en 1957. Les journalistes la surnomment alors la *No Such Agency*. Elle est à l'origine du système mondial d'espionnage des communications commerciales ECHELON, élaboré par les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle Zélande, et installé en 1980. Voir l'introduction de cet ouvrage page 17.

Le chiffrement par blocs

C'est dans ce contexte que Feistel va inventer un nouveau dispositif de chiffrement symétrique qui mobilise pleinement la notion d'algorithme et le codage en écriture binaire. D'abord utilisé dans l'algorithme *LUCIFER*[88], en 1973, ce mode de chiffrement est qualifié de chiffrement par blocs, par opposition au mode traditionnel de chiffrement, dit chiffrement par flots. Il alimentera de nombreux algorithmes cryptographiques dont une variante de *LUCIFER* qui sera immédiatement utilisée pour la banque en ligne, et surtout le DES (*Data Encryption Standard*), premier algorithme public de chiffrement symétrique, qui sera homologué par le *National Bureau of Standards* des États-Unis au terme d'une compétition remportée par IBM (*International Business Machines*) à la suite d'un appel d'offres lancé en 1977 pour produire un système cryptographique utilisable par les entreprises.

Emigré d'Allemagne en 1934, et citoyen des États-Unis depuis 1944, Horst Feistel a fait des études de physique au MIT avant de travailler pour l'AFCRC (*Air Force Cambridge Research Center*) sur la mise au point du dispositif IFF (*Identification Friends and Foes*), puis à la conception du chiffrement au *Thomas Watson Research Center* de la firme IBM. Il est un des premiers chercheurs non gouvernementaux à travailler sur la théorisation des modes de chiffrement. Son premier article sur le sujet, « Cryptography and Computer Privacy », est publié en 1973 dans le *Scientific American.* Il analyse d'emblée l'évolution des enjeux : il s'agit désormais de protéger les systèmes informatiques eux-mêmes, ainsi que les banques de données. Feistel écrit notamment :

> « Le système lui-même doit être tel qu'il soit invraisemblable qu'une personne non autorisée mais habile et subtile puisse soit y entrer, soit y supprimer, soit en altérer des commandes ou données »[89].

Une question nouvelle émerge donc : il s'agit d'authentifier l'origine de tout message, et au-delà, de toute instruction informatique, ceci afin d'assurer la sécurité des opérations effectuées par ordinateur. Le problème est donc ici beaucoup plus vaste que la seule protection du secret des messages. Il concerne également les risques de panne et le fait que les réseaux d'ordinateurs sont très ouverts à la corruption délibérée des échanges, car la moindre altération peut fausser tous les résultats ultérieurs

---

[88] Ce nom proviendrait du mot « Demon », obtenu par troncature du mot « Demonstration », qui était alors trop long pour pouvoir être traité par le système d'exploitation.

[89] « *The system itself must make it extremely unlikely that an unauthorized but clever and sophisticated person can either enter, withdraw or alter commands or data in such a system* ». Feistel, « Cryptography and Computer Privacy », p. 15.

des opérations du système. Une nouvelle exigence entre en jeu : si le cryptanalyste dispose d'un laps de temps non négligeable pour travailler, dans un système informatique au contraire, les corrections doivent intervenir en temps réel pour que sa fiabilité soit garantie à ses utilisateurs.

Le travail de Feistel s'inscrit dans le prolongement direct de l'article de Shannon de 1949 sur les systèmes secrets. Il présente toutes ses analyses, à commencer par celle du système de Vernam, en termes d'opérations sur les symboles 0 et 1 en arithmétique modulaire : le chiffrement et le déchiffrement ne sont autres qu'une seule et même opération, l'addition en base 2. Feistel insiste sur l'intérêt d'une clé aléatoire pour le chiffrement polyalphabétique en arithmétique binaire, qui détruit toute régularité d'ordre syntaxique susceptible de servir d'indice au cryptanalyste : toute possibilité de s'appuyer sur la signification des messages se trouve ainsi éliminée, et le cryptogramme produit devient potentiellement indéchiffrable, puisque la recherche d'un mot clair à partir de toutes les substitutions possibles donne tous les mots ayant le même nombre de caractères, sans pouvoir en privilégier aucun.

Outre la difficulté de produire des clés pseudo-aléatoires de longueur suffisante, et en très grand nombre, le système de Vernam souffre d'un autre grave défaut. Dans un environnement d'ordinateurs, où sont transmises beaucoup de données numériques, la moindre erreur de chiffrement peut provoquer une avalanche d'erreurs de calcul. Pour surmonter ce nouveau handicap, Feistel reprend l'idée de fractionner le message, qu'il trouve déjà dans le mode de chiffrement ADFGVX utilisé par les militaires allemands[90] pendant la Première Guerre Mondiale, et celle de chiffrement-produit, théorisée par Shannon dans son article de 1949 alors que son intérêt s'était estompé pendant l'entre-deux-guerres avec le développement des machines à rotors. Dans la section de son article consacrée à la pratique du secret, Shannon envisageait également différents procédés possibles pour renforcer la puissance des systèmes de chiffrement, selon les principes de confusion et de diffusion, que Feistel va s'employer à réaliser concrètement dans le chiffrement par blocs. Ces méthodes visent à contrarier l'analyse statistique menée sur la propagation de certaines propriétés du clair et du chiffré. La diffusion doit disperser les probabilités associées aux lettres du message, tandis que la confusion doit brouiller la relation entre les probabilités associées aux lettres du cryptogramme et à celles de la clé.

Dans l'algorithme *LUCIFER* que décrit Feistel dans son article de 1973, la force du système est obtenue par une combinaison de chiffrements successifs, qui alternent substitutions et permutations. Les substitutions bouleversent le nombre et la répartition des 0 et des 1, et assurent la

[90] Voir le chapitre « Les travaux de la Section du Chiffre pendant la Première Guerre Mondiale » p. 87.

confusion des probabilités qui sont associées aux lettres initiales du message. Quant aux permutations, elles ne font que mélanger les symboles, et engendrent la diffusion de ces probabilités. Ces transformations sont effectuées électroniquement par des dispositifs nommés respectivement boîtes S et boîtes P, qui alternent en plusieurs couches à travers lesquelles passe le message. Le système décrit en 1973 – mais qui n'est pas le premier établi par Feistel et ses collègues – travaille sur des blocs de 128 symboles binaires. Il utilise une clé de même longueur, qui sélectionne les substitutions à mettre en œuvre sur des blocs de 4 symboles binaires. À la sortie, les chiffres sont devenus des fonctions très sophistiquées, et surtout non linéaires, de tous les chiffres d'entrée. Le but du concepteur est évidemment « d'empêcher un adversaire de retracer le processus inverse »[91]. Ces produits de transformations ouvrent, selon Feistel, des possibilités presque illimitées d'invention, de conception et de recherche.

Le message transmis est complété par plusieurs éléments : un mot de passe pour garantir l'authenticité du message, un code correcteur pour juguler les éventuels brouillages de transmission, et un autre mot de passe pour restreindre l'échange des messages à un groupe prédéterminé de destinataires. Le chiffrement par blocs mélange judicieusement les chiffres du message initial et de ces ajouts, de telle sorte qu'un adversaire ne puisse les distinguer.

Ainsi le chiffrement par blocs conjugue-t-il la force du système de chiffrement à une bonne résistance à la corruption – fortuite ou intentionnelle – des messages. Feistel est donc très confiant dans ce nouveau système de chiffrement, investissant la cryptographie d'origine militaire pour assurer la confidentialité des échanges civils.

La publication du DES en 1977 marque un nouveau tournant : c'est le premier algorithme à clé secrète rendu public. La possibilité de rendre public les modes de chiffrement est désormais reconnue par tous. Cette publicité n'est d'ailleurs pas sans risque : elle ne correspond à un choix raisonnable que si l'algorithme sur lequel repose le mode de chiffrement est sûr. Or, l'intervention de la NSA dans la conception ultime du DES a conduit ses utilisateurs à soupçonner l'existence de trappes qui lui auraient permis de décrypter les échanges[92]. Le DES a cependant été le système de chiffrement à clé secrète le plus utilisé pendant une vingtaine d'années. L'augmentation considérable de la puissance des ordinateurs a cependant rendu possible, dès 1997, la recherche de la clé par calcul exhaustif. Pour y

[91] Feistel, « Cryptography and Computer Privacy », p. 21.

[92] Ce soupçon n'est pas totalement gratuit, puisque la NSA a continué à fournir à ses allés des machines *Enigma* pendant la guerre froide, sans révéler que son système avait été décrypté en Grande-Bretagne et aux États-Unis pendant la guerre précédente. Voir l'introduction p. 17.

pallier, la NSA a standardisé un triple DES, puis le système AES en 2000, à la suite d'un appel d'offres cette fois international.

CONCLUSION

Si la cryptologie traite toujours de messages chiffrés, les conditions et l'extension du chiffrement ont donc connu des mutations profondes depuis le début du 19e siècle. L'écriture des cryptogrammes a abandonné la technique du papier-crayon pour s'effectuer au moyen d'instruments et de machines, devenues électroniques au 20e siècle. Mais surtout, les principes propres à l'exercice de la cryptologie ont renoncé au secret des messages particuliers, pour s'attacher aux conditions qui garantissent le secret de l'ensemble des messages susceptibles d'être échangés par le biais d'un système technique donné : système télégraphique et téléphonique au 19e siècle, télégraphie sans fil, téléscripteurs et ordinateurs au 20e. Le développement de ces nouveaux systèmes de communication a été déterminant dans cette mutation de la cryptologie, tout comme les techniques d'écriture avaient présidé à ses balbutiements. L'analyse des conditions de sécurité susceptibles de garantir le caractère sinon privé, du moins réservé, des communications, a présidé à la mathématisation du domaine, et la cryptologie a finalement joué un rôle capital dans l'extension des réseaux d'ordinateurs. Et au fur et à mesure que la puissance des méthodes cryptographiques se renforçait, le secret s'est de plus en plus restreint à la question des clés de chiffrement, la méthode elle-même pouvant s'exposer publiquement.

Il n'empêche que la publicité faite au système ne concerne pas la société civile dans son ensemble. Qu'il s'agisse du système télégraphique ou des réseaux d'ordinateurs, seul un cercle restreint d'utilisateurs initiés est susceptible de s'approprier la connaissance du procédé de chiffrement. Il s'agit des militaires dans le texte de Kerckhoffs, des techniciens du téléscripteur dans le système de Vernam, et des praticiens de l'informatique aujourd'hui. La publicité faite aux systèmes de chiffrement témoigne en fait de l'extension du spectre des personnels concernés par le fonctionnement de ces systèmes. En dépit des déclarations fracassantes sur l'universalité du mode de communication qu'autorise l'informatique aujourd'hui, les modes d'échanges reproduisent de fait les rapports sociaux existants dans la société, tout en décuplant la puissance des détenteurs d'information.

Avec l'extension qu'a connue la théorie de l'information depuis les années 1950, l'importance prise par la notion de système dans ce mode d'échanges a dépassé de très loin le point de vue de l'ingénieur qu'était Shannon. Dans cette perspective nouvelle, il serait pourtant réducteur d'ignorer toute caractérisation du sujet autre que son appartenance à un

quelconque système, ou de considérer tout élément extérieur au système comme « ennemi ». Si la question de la signification des messages n'est pas pertinente pour l'ingénieur, elle reste hautement pertinente, d'un point de vue philosophique, pour le sujet pris dans le fonctionnement de multiples systèmes. Réduire le sujet à l'état d'élément communicant de tels systèmes va à l'encontre de la conception humaniste soucieuse de l'autonomie du sujet, et pour laquelle la signification est centrale dans les échanges humains. En ce sens, il est essentiel pour le sujet de porter un regard extérieur sur ces systèmes de communication. Tels qu'ils sont organisés par la cryptologie, ils ne fonctionnent pas *ex nihilo*. Ils ont une fonction sociale déterminée pour les organisateurs du système lui-même, auxquels il offre toute la puissance de son réseau d'échanges instantanés. Et il devient donc particulièrement urgent de penser cette fonction sociale des systèmes dans leur ensemble.

BIBLIOGRAPHIE

Atlan, H., *Entre le cristal et la fumée, Essai sur l'organisation du vivant.* Paris, Seuil, Points Sciences, 1979.

Babbage, Ch., *The Works of Charles Babbage*, (dir.) M. Campbell-Kelly, London, William Pickering, 11 vols, 1989.

— *Life of a Philosopher, in Works,* vol. 9.

— « Philosophy of Deciphering », Add. Mss. 37205, *British Library, Manuscript Room.*

Bellovin, S. M., « Frank Miller : Inventor of the One-Time Pad », Columbia University, Academic Commons, 2011, http://hdl.handle.net/10022/AC:P:10665.

Bode, H. W. et Shannon, C. E., « A simplified Derivation of Linear Least Squares Smoothing and Prediction Theory », Decimal Classification : R 150. Reprinted *in Shannon's Collected Papers,* pp. 628-656.

Breton, Ph., *Une histoire de l'informatique,* Paris, Seuil, 1990.

Bush, V., « The Differential Analyzer. A New Machine for Solving Differential Equations », *Journal of the Franklin Institute,* 1931, vol. 212, pp. 447-88.

Davies, D. W., « Wheatstone's Cryptograph and Plett's Cipher Machine », *Cryptologia,* 1985, vol. 9, n° 2, pp. 155-160.

Dewey, G., *Relative Frequency of English Speech Sounds,* Boston, Harvard University Press, 1923.

Durand-Richard, M.-J., « Charles Babbage (1791-1871) : de l'Ecole algébrique anglaise à la "machine analytique", *Mathématiques, Informatique et Sciences Humaines,* 1992, 30° année, n° 118, 5-31 ; et n° 120, 79-82.

— « Planimeters and integraphs in the 19th century, before the differential analyzer », *Nuncius*, 2010, vol. XXIV, n° 1, pp. 101-124.
— « Le regard français de Charles Babbage (1791-1871) sur le déclin de la science en Angleterre », *Documents pour l'histoire des techniques*, numéro thématique sur « Les techniques et la technologie entre la France et l'Angleterre XVIIe-XIXe siècles », (dir.) P. Bret, I. Gouzévitch et L. Perez, n° 19, 2e sem. 2011, pp. 287-304.
— « De l'algèbre symbolique à la théorie des modèles : structuration de l'analogie comme méthode démonstrative », *in Le statut de l'analogie dans la démarche scientifique, Perspective historique* (éd.) Marie-José Durand-Richard, Paris, L'Harmattan, 2008, pp. 131-169.
Feistel, H., « Cryptography and Computer Privacy », *Scientific American*, 1973, vol. 128, n° 5, pp. 15-23.
Franksen, O. I., *Mr Babbage's Secret, the tale of a cypher and APL,* Vedbaek (Denmark), Strandberg Forlag, 1984.
— « Babbage and Cryptography. Or, the mystery of Admiral Beaufort's cipher », *Mathematics and Computers in Simulation*, 1993, n° 35, pp. 327-367.
Friedman, W. F., *The Index of Coincidence and its Applications to Cryptolgraphy,* Laguna Hills, California, Aegean Park Press, 1921.
Fréchet, M., *Méthode des fonctions arbitraires, théorie des événements en chaîne dans le cas d'un nombre fini d'états possibles*, Pairs, Gauthier-Villars, 1938.
Givierge, M., *Cours de cryptographie,* Paris, Herman, 1939.
Guillot, P., « Auguste Kerckhoffs et la cryptographie militaire », 2012, http://www.bibnum.education.fr/calculinformatique/cryptologie/la-cryptographie-militaire#.
Hill, L. S., « Cryptography is an Algebraic Alphabet », *American Mathematical Monthly*, 1929, n° 36, pp. 306-312.
— « Concerning Certain Linear Transformations Apparatus of Cryptography », *American Mathematical Monthly*, 1931, n° 38, pp. 135-154.
Hitt, P. *Manual for the Solution of Military Ciphers*, Fort Leavenworth, KS, Press of the Army Service School, 1916.
Kolmogoroff, A., *Grundbegriffe der Wahrscheinlichkeitsrechnung*, Berlin, Springer, 1933.
Minarsky, J.-F., « Cryptanalyse et spécification de schémas de signature RSA avec redondance », *Thèse de l'université de Caen,* Spécialité : Mathématiques et leurs applications, Caen, Université de Basse-Normandie, 1999.
Olivari, H., *Mission d'un colonel français en Russie (1916),* Paris, L'Harmattan, 2009.

Pratt, M. F., *Secret and Urgent, the Story of Codes and Ciphers*, Garden City New York, American Cryptogram Association, Blue Ribbon Bookds, 1939.

Rémy, F., « La cryptographie à clé publique », *Pour la Science*, dossier « L'art du secret », juillet/octobre 2003, n° 36, pp. 44-51.

Roche, A., *Claude E. Shannon, Spielzeug, Leben und die gheime Geschichte seiner Theorie der Information*, Berlin, Gegenstalt Verlag, 2, Auflage, 2010.

Segal, J., *Le zéro et le un, histoire de la notion scientifique d'information au 20e siècle*, Paris, Syllepse, 2003.

Shannon, C. E., *Collected Papers of C.E. Shannon*, (eds.) Sloane, N. J. A. et Wyner, A. D. New York, IEEE Press, 1993.

— « A Symbolical Analysis of Relay and Switching Circuits », *Transactions of the American Institute of Electrical Engineers*, 1938, n° 57, pp. 713-723, *in Shannon's Collected Papers,* pp. 471-495. http://paradise.caltech.edu/CNS188/shannon38.pdf.

— A letter from Shannon to Vannevar Bush, dated : 16th February 1939, *in Shannon's Collected Papers*, pp. 455-456

— « An algebra for Theoretical Genetics », Ph. D. Doctoral mathematical Dissertation, 1948, *in Shannon's Collected Papers,* pp. 891-920.

— « Mathematical Theory of the Differential Analyzer », *Journal of Mathematics and Physics*, 1941, vol. 20, pp. 337-354, *in Shannon's Collected Papers*, pp. 493-513.

— « Communication Theory of Secrecy Systems », *The Bell System Technical Journal*, 1946-49, vol. 28, pp. 656-711, *in Shannon's Collected Papers*, pp. 656-711.

— « The Philosophy of PCM », *Decimal Classification* : R 148.6. Original manuscript received by the Institute may 24, 1948, *in Shannon's Collected Papers*, pp. 151-176.

— « A Mathematical Theory of Communication », *The Bell System Technical Journal*, july-october 1948, vol. 27, pp. 379-423 et 623-656, *in Shannon's Collected Papers*, pp. 5-82.

Slater, R., *Telegraphic Code, to Ensure Secrecy on the Transmission of Telegrams*, London, W. R. Gray, 1870.

Smoot, B. R., « Pioneers of US Military Cryptology : Colonel Parker Hitt and his wife Genevieve Young Hitt », *Federal History*, 2012, pp. 87-100.

Stankovic, R. S. et Ascola, I., *From Boolean Logic to Switching Circuits and Automata*, Berlin Heidelberg, Springer Verlag, 2011.

Tolman, R.C., *Principles of Statistical Mechanics*, Oxford, Clarendon Press, 1938.

Trogemann, G., Nitussov, A. et Ernst, W., *Computing in Russia, The History of Comuter Devices and Information Technology revealed*, traduction anglaise par A. T. Nitussov, Wiesbaden, Vieweg & Sohn Verlag, 2001.

Vernam, G. S., « Secret Signaling System », *United States Patent Office*, patented July 22, 1919.

Von Neumann, J. et Morgenstern, O., *Theory of Games and Economic Behavior*, Princeton, Princeton University Press, 1944.

Wilkins, J., *The Mathematical and Philosophical Works*, London, Vernor and Hood, 1802, 2 vols.

LA CRYPTOLOGIE GOUVERNEMENTALE FRANÇAISE ET SES RELATIONS AVEC LES MATHEMATIQUES

André CATTIEUW[1]

On entend souvent dire que la cryptologie était l'affaire des militaires avant l'apparition, au milieu des années 70 dans la société civile, des algorithmes de cryptologie comme le DES et des systèmes à clé publique tels que le RSA, conçus pour satisfaire les besoins de sécurité de la société informatisée qui émergeait. La cryptologie était perçue comme une chasse gardée des militaires car, jusque dans un passé récent, les moyens de la cryptologie étaient considérés et traités comme des matériels de guerre par les grandes puissances. C'est une demi-vérité. Depuis bien longtemps, elle était plutôt l'affaire des diplomates et des policiers. De fait, les militaires ne s'y sont intéressés et n'ont acquis une prééminence dans le domaine qu'à partir de la Première Guerre Mondiale, quand l'emploi de la radio s'est généralisé et que la protection des communications militaires par radio s'est révélée indispensable.

On s'efforce ici de décrire comment la cryptologie s'est développée dans les armées françaises et dans les instances gouvernementales en tentant de donner un aperçu du rôle des mathématiques dans ce développement, sachant qu'aujourd'hui la cryptologie tend à devenir une branche nouvelle des mathématiques appliquées. La cryptologie, grâce aux possibilités des nouvelles technologies de l'information et des communications, offre aux mathématiciens l'occasion d'applications concrètes et de débouchés jusqu'ici insoupçonnés à des mathématiques bien abstraites comme la théorie des nombres par exemple. Cela n'a pas toujours été le cas et les mathématiques utilisées aujourd'hui ne pouvaient pas l'être auparavant. Imagine-t-on un instant demander à un militaire en campagne d'effectuer à la main avec un papier et un crayon des opérations arithmétiques sur des

[1] Ancien chef du Service Central du Chiffre et de la Sécurité des Télécommunications (SCCST). Ancien Adjoint du Délégué Interministériel pour la Sécurité des Systèmes d'Information (DISSI).

nombres de 150 chiffres ou des exponentielles modulaires ? En fait, la cryptologie est à l'image de la technologie de son temps. L'application des mathématiques à la cryptologie aujourd'hui n'est possible que parce que nous disposons des moyens de calcul adaptés qu'offrent l'informatique et l'électronique actuelles (processeurs performants, microcircuits des cartes à puce, *etc.*).

C'est surtout à partir de la Première Guerre Mondiale que la cryptologie a été prise en compte dans les armées de tous les belligérants. Les services rendus, au cours de la guerre 1914-18, par le renseignement radioélectrique et le décryptement des communications chiffrées, tout comme les conséquences désastreuses résultant des négligences en matière de sécurité des communications radio, furent parmi les enseignements les plus inattendus qu'ont pu tirer les états-majors du déroulement du conflit. Longtemps couvertes par le secret chez les anciens belligérants, les informations concernant le Chiffre ne furent connues que peu à peu, à mesure qu'ont pu être publiés mémoires, livres ou articles, sur la guerre.

Qu'on se souvienne en effet :

– de la bataille de Tannenberg : deux armées russes sont battues par une seule armée allemande bien renseignée des intentions des généraux russes qui transmettent en clair, par radio, leurs intentions de manœuvres[2],

– du fameux télégramme Zimmerman décrypté par les Britanniques qui fut un des éléments qui amena l'entrée en guerre des États-Unis[3] en 1917,

– et du radiogramme de la victoire dont le décryptement a été déterminant pour l'issue de la guerre[4].

LES CRYPTOLOGUES POLYTECHNICIENS DANS LA PREMIERE GUERRE MONDIALE

Avant la Première Guerre Mondiale, deux pays seulement ont prévu les conséquences de l'emploi militaire de la radio, découverte en 1895, et ont créé un Service du Chiffre pour protéger leur communications et intercepter les communications radio adverses : la France et l'Autriche-Hongrie qui, ayant observé le conflit italo-turc de 1911, crée le *Dechiffrierdienst*[5].

---

[2] Kahn, *The Codebreakers,* pp. 622-627.

[3] Voir le chapitre « Les travaux de la section du chiffre pendant la Première Guerre Mondiale » pp. 99-100.

[4] *ibid*., p. 100. Le décryptement de ce radiogramme a entre autres permis à l'État-Major français, en juin 1918, de connaître les intentions de l'adversaire et de stopper net la dernière grande offensive projetée par les Allemands sur Paris, de contre-attaquer et de l'emporter. Cet événement est longuement évoqué par Sophie de Lastours dans son ouvrage, *La France gagne la guerre des codes secrets.*

[5] Service du déchiffrement.

La France crée une « Section du Chiffre » auprès du Cabinet du Ministre de la Défense en 1912. Jusqu'alors la cryptologie était une affaire d'officiers qui la pratiquaient comme un *hobby* en dehors de leur activité principale. À la Section du Chiffre va se constituer, autour d'un noyau de polytechniciens de talent, et sous la conduite du Colonel Cartier – lui-même polytechnicien – une équipe d'officiers compétents et passionnés par la cryptologie, qui placera la France au premier rang lors de la guerre 1914-18. L'un d'eux, le capitaine Painvin, major de Polytechnique et 1er prix du conservatoire de Nantes, se révèlera un véritable génie du décryptement qui étonnera nos Alliés[6].

Sont ainsi décryptés pendant la guerre[7] :

– tous les systèmes manuels de campagne allemands au fur et à mesure de leur mise en service, alors qu'ils changent souvent à cause des indiscrétions françaises émanant la plupart du temps du Cabinet du Ministre, et reprises par les journaux,

– les codes de la marine allemande en relation avec les Britanniques qui nous demanderont de cesser toute activité dans ce domaine par crainte de nos indiscrétions,

– les codes autrichiens dans le cadre de l'aide technique du Chiffre fournie aux Italiens,

– les codes diplomatiques allemands, autrichiens et bulgares : c'est le décryptement des messages de l'attaché naval allemand à Madrid adressés à Berlin qui permet de confondre la fameuse espionne Mata Hari qui le paiera de sa vie.

Les officiers de la Section du Chiffre se sont montrés opérationnels dès le début des hostilités en août 1914. Au cours des deux années précédentes, ils avaient pu se former et mettre au point leur savoir-faire. L'un d'entre eux, le Capitaine Marcel Givierge (1871-1931), sorti dans les premiers de Polytechnique et parlant cinq langues, avait été mis à disposition du Ministère de l'Intérieur pour apporter son aide, grâce à ses connaissances linguistiques, à l'équipe du commissaire Haverna de la Sureté Générale. Celui-ci, depuis 1905, quand il était parvenu à décrypter les messages diplomatiques japonais pendant le conflit russo-japonais, dirigeait, au ministère de l'Intérieur, une équipe d'une grande efficacité qui avait à son actif le décryptement d'autres chiffres (Turquie, Espagne, Monaco, agents financiers russes, serbes et roumains installés en France, *etc*.). À son contact, le capitaine Givierge va devenir un « as » du décryptement et pourra communiquer son savoir-faire à ses camarades de la Section du Chiffre qui, de leur côté, avaient travaillé les ouvrages bien connus de cryptologie de

[6] Voir le chapitre « Les travaux de la section du chiffre pendant la Première Guerre Mondiale » pp. 102-103.

[7] Cattieuw et Hébrard, « L'origine des codes secrets », p. 17.

leurs prédécesseurs (Kerckhoffs, commandant Bazeries, De Viaris, capitaine Valerio, Hermann, Delastelle)[8] et dressé les tableaux des caractéristiques statistiques des principales langues. Ils avaient aussi commencé à s'attaquer au trafic radio militaire allemand chiffré au cours de manœuvres, et découvert les premières brèches conduisant au décryptement de quelques procédés.

Il faut bien voir qu'à cette époque, tous les systèmes de chiffrement étaient manuels. Aux niveaux élevés de la hiérarchie, on utilisait des dictionnaires ou des codes de chiffrement sur-chiffrés par un moyen manuel. Sur le plan tactique, c'étaient des systèmes dits « papier-crayon ». Il fallait qu'ils soient faciles d'emploi et donc peu sophistiqués : la recherche d'un procédé – on dirait aujourd'hui d'un algorithme – manuel, simple, rapide et sûr, était à l'ordre du jour, mais on constatait que c'était un objectif impossible à atteindre pour les cryptologues. C'était d'autant plus inexplicable qu'on ne connaissait pas, à cette époque, la théorie de la complexité qui en aurait vraisemblablement donné l'explication.

Le décryptement reposait sur une analyse statistique et linguistique des cryptogrammes en nombre plus ou moins élevé selon l'ampleur du trafic des messages chiffrés interceptés. Ce travail demandait beaucoup de patience, un esprit d'observation toujours en éveil prêt à repérer la moindre anomalie dans les cryptogrammes, une excellente mémoire eidétique capable de mémoriser presqu'inconsciemment des suites et des combinaisons de lettres incompréhensibles : toutes qualités qui n'exigent pas de connaissances mathématiques bien approfondies mais une sympathie intellectuelle pour le mystère et les énigmes. Bien sûr, après une phase d'examen des textes chiffrés au cours de laquelle était relevées les fréquences des éléments du cryptogramme et les répétitions de lettres caractéristiques, il fallait avoir le talent ou l'intuition qui permettait de poser les bonnes hypothèses à partir desquelles, en suivant une analyse rigoureuse, il était possible « d'entrer » dans le cryptogramme, c'est-à-dire de commencer le décryptement proprement dit. Si l'analyse n'aboutissait pas, il fallait savoir revenir en arrière, réviser les hypothèses, entamer une nouvelle analyse… Tout était bon pour parvenir au résultat, y compris les hasards heureux. Cette intuition, plus ou moins développée chez les uns ou les autres, était une sorte de faculté de sentir, portant sur un savoir et une expérience accumulés, impossibles à formuler explicitement comme le serait un savoir mathématique.

Le choix des bonnes hypothèses était guidé aussi par les circonstances car un lot de messages interceptés à un moment donné dans un contexte opérationnel bien connu suggérait tel ou tel « mot probable » par exemple. Les habitudes rédactionnelles des correspondants, les messages stéréotypés,

[8] Voir le chapitre « Du message chiffré au système cryptographique » p. 122.

les erreurs d'opérateurs, *etc*., étaient aussi des aides précieuses. Pour les cryptologues chevronnés, cette analyse était plus ou moins rigoureuse. L'entraînement, l'expérience les amenaient à subodorer les bonnes hypothèses et à pratiquer bien des raccourcis dans l'analyse. Si on leur demandait comment ils avaient fait, ils répondaient assez fièrement : « ... mais c'est évident, ça se voit ! » ; le raisonnement et l'analyse avaient été court-circuités par leur intuition. Comme il existe des cruciverbistes chevronnés, des joueurs de bridge astucieux, et des joueurs d'échecs redoutables, il y avait des décrypteurs plus ou moins doués, plus ou moins talentueux ou géniaux. Pour l'observateur peu expérimenté ou pour le débutant, leur façon de faire pouvait paraître étonnante et même déroutante, le « ça se voit » pouvait les faire passer pour arrogants. Il faisait penser aussi à quelque magie ou sorcellerie et c'est en cela que l'analyse cryptologique passait pour un art.

En revanche, concevoir un procédé de chiffrement solide, du moins assez solide eu égard à l'usage qu'on voulait en faire, relevait d'une autre démarche car il fallait, pour éviter de concevoir un procédé faible, bien connaître toutes les recettes de la cryptologie d'attaque, ainsi que les procédés qui avaient été percés, ainsi que leurs faiblesses ; tout ce savoir constituait la science cryptologique que devait posséder le cryptologue de conception, science assez loin des mathématiques en tout état de cause.

L'ENTRE-DEUX GUERRES : LES POLYTECHNICIENS SE DETOURNENT DU CHIFFRE

Les enseignements de la Première Guerre Mondiale sont évidents.

L'indiscrétion de la radio s'est révélée manifeste, le chiffrement est nécessaire pour assurer la sécurité des communications mais, effectué manuellement par des officiers, il est trop lent. Doit-il rester le monopole des seuls officiers ? Il faut moderniser et mécaniser le Chiffre pour gagner du temps, et sous-traiter les opérations de chiffrement et déchiffrement à des exécutants.

Le décryptement est apparu comme une source précieuse de renseignements. Cette source est fiable mais très précaire car la moindre indiscrétion peut la tarir. Faut-il investir dans cette voie très (trop ?) technique et complexe aux résultats incertains, souvent longs à obtenir, alors que le rétablissement de procédés codiques à base de dictionnaires de chiffrement surchiffrés peut demander plusieurs années d'effort, sauf si on recourt à des moyens extérieurs à la cryptologie ?

Il faut orienter les interceptions radio et la radiogoniométrie pour aider à l'analyse du trafic et au décryptement car il vaut mieux intercepter le trafic

chiffré que l'on sait décrypter ou que l'on espère bientôt percer, plutôt qu'autre chose.

Enfin, la place du Chiffre dans l'organisation militaire pose problème : la Section du Chiffre a souffert des multiples indiscrétions des politiques du Cabinet du Ministre, il faut lui trouver un autre point d'ancrage.

La restructuration de la Section du Chiffre

Le Chiffre étant chargé de chiffrer et de déchiffrer les messages, certains le verraient volontiers relever du Service du courrier. Chargés de percer les chiffres adverses, d'autres le verraient plutôt au Deuxième Bureau, chargé du renseignement. Mais si le Deuxième Bureau le revendique, il ne veut pas assurer les tâches d'exécution – chiffrement et déchiffrement des messages. Quant au Chiffre lui-même, il souhaite continuer à orienter les interceptions pour optimiser ses travaux d'analyse, mais les responsables des interceptions se montrent jaloux de leurs prérogatives et insistent sur l'importance des interceptions claires pour les préserver.

En tout état de cause, les structures sont modifiées en 1921. La Section du Chiffre du Cabinet du Ministre, qui avait si brillamment trouvé toutes les solutions de décryptement des procédés allemands pendant la Grande Guerre, est rattachée au Chef de l'État-Major, en réalité à un Sous-Chef, lequel s'en débarrasse vite auprès d'un Directeur qui la confie à un Sous-Directeur. Au cours de ce transfert, elle perd donc tout son prestige ainsi que son rôle stratégique et politique. Elle devient, en pratique, un élément de l'État-Major sans grande influence, caché derrière un rideau de secret.

Lors de ce transfert, ses effectifs sont passés d'environ soixante officiers à, à peine, quinze. Elle n'a aucune possibilité d'orienter les interceptions et doit travailler sur celles qu'on lui donne. Elle est chargée de chiffrer et déchiffrer les messages de l'État-Major – 80 à 100 messages par jour –, de former les 250 officiers du chiffre de réserve convoqués par périodes, de confectionner les codes et dictionnaires de chiffrement de l'Armée ainsi que les procédés et les clés de surchiffrement, de rechercher les moyens de mécaniser les opérations de chiffrement mais sans crédit alloué pour ce faire. Elle doit, en outre, rechercher les solutions de décryptement c'est-à-dire les clés des systèmes adverses pour le Deuxième Bureau qui les exploite dans une Section D – décryptement – distincte, et qui sera bientôt chargée de guider les interceptions.

La Section du Chiffre travaille donc en vase clos, s'attaquant à ce qu'elle sait décrypter sur les interceptions qu'on lui fournit. Elle cultive surtout la cryptanalyse des procédés manuels. Elle s'intéresse bien sûr aux matériels de chiffrement qui apparaissent sur le marché, mais se montre très prudente au plan de leur analyse cryptologique. Elle saura néanmoins décrypter

l'*Enigma* commerciale utilisée par les nationalistes lors de la guerre d'Espagne. En revanche elle se montrera très sceptique sur les possibilités de décrypter l'*Enigma* I de la *Werhmacht*, mais n'aura pas communication des messages chiffrés interceptés laissant apparaître les erreurs d'exploitation commises par les Allemands, et qui conduiront les Polonais au décryptement de cette machine[9].

Mais les études de cryptanalyse s'adaptent mal au milieu militaire environnant de l'État-Major. Elles demandent du temps, de la patience, et ne sont pas compatibles avec la mobilité exigée du personnel militaire. En outre, l'éthique militaire est fondée sur l'action et le panache, le héros militaire français est un « baroudeur ». On n'admire pas un analyste ou un chercheur de génie, même s'il a été capable de fournir des informations décisives pour la victoire. Là-dessus, la maréchal Foch (1851-1929), selon la doctrine officielle qu'il édicte après la Grande Guerre, décide que le renseignement relève, en priorité, de la reconnaissance confiée à la cavalerie et à la toute jeune aviation, et ne prend pas en compte le décryptement. Dans ces conditions, la plupart des officiers ayant servi à la Section du Chiffre se plaindront amèrement de la modestie de l'avancement qui leur sera réservé, et les polytechniciens qui avaient été l'âme de ce service s'en écarteront en lançant la formule : « on ne fait pas carrière au Chiffre ». Givierge, devenu général, alors chef de la Section du Chiffre de l'État-Major, s'élève avec véhémence contre cet état de choses mais n'est pas entendu.

Les premiers pas de la mécanisation de la Section du Chiffre

Il n'en demeure pas moins que les officiers de la Section du Chiffre de l'État-Major sont des personnels de qualité, plutôt littéraires de formation, tournés vers les langues. Ils maintiendront le savoir-faire cryptologique de la section à un niveau élevé. Ils vont s'attaquer à la mécanisation du chiffre, devenue indispensable compte tenu de l'ampleur du trafic des messages à chiffrer, et qui ne fait que croître. En 1934, ils accueillent chaleureusement un jeune ingénieur, Boris Hagelin (1892-1983), patron d'une petite entreprise suédoise de mécanique qui s'est spécialisée dans les machines à chiffrer. Boris Hagelin a conçu une machine à chiffrer, la B 21, en vue de concurrencer l'*Enigma* dont l'armée suédoise souhaitait s'équiper. Les militaires suédois ont refusé sa B 21, et il vient la présenter à l'État-Major français – tentative de la dernière chance en quelque sorte, puisque son entreprise est au bord du dépôt de bilan.

La B 21 intéresse beaucoup les officiers de la Section du Chiffre qui l'étudient de près au plan cryptologique bien sûr, mais aussi et surtout au

[9] Cattieuw et Hébrard, « De la mécanique à l'ordinateur ». pp. 19-23.

plan de la mise en œuvre et de l'exploitation. Cette collaboration permet de définir la B 211, machine à clavier la plus légère du marché – 15 kg. –, avec imprimante, et pouvant fonctionner sur la batterie d'un véhicule, mais aussi avec une manivelle – à la main – en cas de secours. Le clair est frappé au clavier – lettres, chiffres et signes de ponctuation –, et le chiffré est imprimé sur une bande de papier. Cinq cents exemplaires sont commandés pour l'Armée Française et fabriqués par l'entreprise Ericson à Colombes. Les Soviétiques, de leur côté, en feront réaliser un modèle avec l'alphabet cyrillique, et en équiperont leurs forces jusqu'en 1952.

Les militaires français souhaitaient aussi un matériel de campagne léger avec imprimante. Hagelin leur propose en 1936 une petite machine de 1,125 kg répondant à leur vœu, la C 36. La France en commandera 5 000 exemplaires pour ses petites unités et Hagelin en vendra plus de 50 000 exemplaires à différentes armées de par le monde (Italie, Suède, Finlande, Japon, *etc*.). Les États-Unis s'y intéresseront en l'améliorant, et en fabriqueront 140 000 exemplaires pendant la Seconde Guerre Mondiale sous le nom de *Converter M 209*.

Ces machines sont mécaniques ou électromécaniques, leur fonctionnement repose sur des mécanismes à base de roues dentées et d'engrenages qu'on peut aisément observer à l'œil nu. Le succès de ces matériels s'explique par le fait que Hagelin laissait toujours le choix à son client d'apporter des modifications et de fixer certains paramètres, ce qui lui garantissait une machine quasiment sur mesure et en tout cas personnalisée.

Nul besoin d'études sophistiquées faisant appel aux mathématiques pour évaluer la valeur cryptographique de ces équipements. Ils relèvent de procédés cryptographiques bien connus en cryptographie manuelle : les procédés dits « à double clé » ou encore « polyalphabétiques » comme le « Vigenère »[10]. Une machine telle que la C 36 produit de longues séquences dites « incohérentes » d'éléments-clés qui sont des nombres de l'ensemble des entiers modulo 26 ($\mathbb{Z}/26\mathbb{Z}$), les 26 lettres claires de l'alphabet sont considérées aussi comme des éléments de $\mathbb{Z}/26\mathbb{Z}$. Le chiffrement s'effectue selon la variante dite à « l'allemande » où le clair est soustrait modulo 26 à la clé. Au déchiffrement c'est la lettre chiffrée qui est soustraite a l'élément-clé, autrement dit c'est la même opération qui intervient au chiffrement et au déchiffrement, c'est une opération idempotente qui permet de simplifier le matériel : on chiffre comme on déchiffre et inversement, c'est tout le contraire des systèmes à clé publique d'aujourd'hui.

Les améliorations qui seront apportées pour réaliser les machines réservées à la France seront d'ordre purement cryptologique et non mathématique. La machine C 36 est emblématique de toute une famille de machines qui seront produites jusque dans les années 1950. Elle réalise

[10] Voir le chapitre « L'ancrage de la cryptologie dans les jeux d'écriture » pp. 37-49.

mécaniquement, à l'aide de roues-clés portant des ergots pouvant prendre deux positions « actifs » ou « passifs » (matérialisant des bits « 0 » ou « 1 ») et avançant toutes régulièrement d'un pas à chaque lettre, un algorithme de production d'une suite d'éléments-clés de $\mathbb{Z}/26\mathbb{Z}$ combinés avec les lettres claires selon le procédé de chiffrement polyalphabétique « à l'allemande »[11]. La production de cette suite est obtenue par le jeu des ergots des roues-clés sur les tétons, curseurs ou cavaliers solidaires de réglettes mobiles agissant sur une roue des types afin de fournir un alphabet décalé dit de « Jules César » pour chaque lettre à chiffrer ou à déchiffrer.

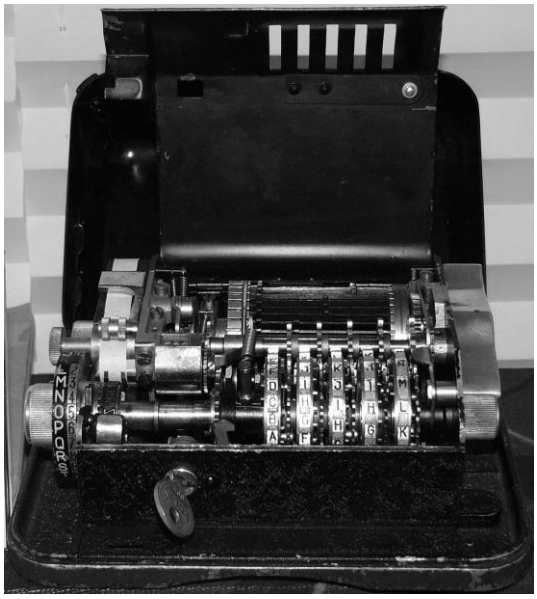


Fig. 1. Machine C36. Autorisation de Matt Crypto, Domaine public.

La machine ne pouvant prendre qu'un nombre fini d'états, la suite-clé produite est périodique et sa période, produit de la longueur des roues-clés à ergots (25, 23, 21, 19, 17), vaut 3 900 225 avec une entropie de la clé de 105 bits. Ce sont des valeurs très élevées pour l'époque, s'agissant surtout d'une cryptologie de campagne devant offrir une sécurité de quelques heures et non d'un système de chiffrement de haut niveau.

On se préoccupe peu du caractère pseudo-aléatoire de la suite-clé produite, ou de sa prédictibilité. Son incohérence apparente satisfait les experts, heureux de constater que la machine fournit à chaque message une séquence d'éléments-clé aussi longue que le texte à chiffrer, ce qui empêche

[11] *ibid.*, p. 49.

toute analyse basée sur une quelconque périodicité de la suite-clé combinée au texte. Mais les cryptologues de la Section du Chiffre s'aperçoivent bien vite que deux messages clairs chiffrés avec la même portion de la suite-clé, erreur souvent commise par les chiffreurs, conduisent au rétablissement des textes clairs et, s'ils sont assez longs, au rétablissement de la suite-clé, et de là, au remontage de l'algorithme de production des éléments-clé, c'est-à-dire aux 105 bits de clé de la machine assurant le secret.

C'est sur la base d'observations de ce genre, dictées par la cryptologie bien plus que par des considérations mathématiques, que sont apportées les modifications dites « anti-analytiques », qui renforceront la valeur cryptologique de ces machines et conduiront aux machines modifiées C36 M1 et C36 M2 qui vont équiper l'armée française aux bas échelons opérationnels. Les cryptologues utilisent les faiblesses cryptologiques qu'ils découvrent, plutôt qu'une approche purement mathématique, pour mieux employer leurs capacités de conception de systèmes sûrs.

LA SECONDE GUERRE MONDIALE : STAGNATION DU CHIFFRE FRANÇAIS

Quand éclate la Seconde Guerre Mondiale, ces machines sont les bienvenues, mais se révèlent bien trop lentes, compte tenu de l'ampleur du trafic à traiter. Lors de la campagne de France de mai 1940, le Chiffre n'a ni mieux ni moins bien servi que les autres armes ou services. Dès le début, il a été débordé face au volume de trafic à traiter, comparé à l'insuffisance de ses moyens en hommes et en matériels. Quant à la Section du Chiffre, elle parvient à décrypter environ 9 000 messages tactiques allemands en systèmes manuels. De son côté, la Section D du Deuxième Bureau, devenue le PC Bruno, a recueilli l'équipe des cryptologues polonais qui sont parvenus à décrypter l'*Enigma* allemande. Le PC Bruno parvient à décrypter environ 4500 messages *Enigma* de la *Luftwaffe*. L'intérêt porté aux messages décryptés croît au fur et à mesure que la situation se dégrade, mais l'État-Major, débordé et bousculé, ne peut tirer profit de ces informations.

Lors de l'Armistice de 1940, la Section du Chiffre est dissoute à la demande des Allemands qui exigent la fourniture immédiate de tous les moyens de chiffrement français et de leurs clés. Le PC Bruno passe en zone sud où il continuera à travailler jusqu'à l'invasion en 1942.

Le Chiffre renaît, en même temps que l'armée française, en Algérie où est créé en 1943 une Direction Technique des Chiffres à vocation civile et militaire rattachée au Comité Français de Libération Nationale. Cette Direction ne traite que du Chiffre de défense, la cryptologie d'attaque étant

confiée au BCRA[12], ancêtre de l'actuelle DGSE[13]. C'est à compter de cette date que la France se révèle être le seul pays avancé en cryptologie qui maintient une nette séparation entre cryptologie de défense et cryptologie d'attaque, séparation dont il faudra tenir compte quand viendra le moment de concevoir des moyens modernes, séparation qui est toujours la règle aujourd'hui. Cette nouvelle Direction remet le Chiffre sur pied en faisant réaliser de nouveaux moyens manuels – codes et dictionnaires – et en améliorant l'emploi des machines existantes, C36 et B 211 modifiées. Mais l'équipement de l'armée française ne sera réalisé que par l'apport de machines M 209 américaines.

À la fin de la guerre, la Direction Technique des Chiffres rejoint la France en octobre 1944. Elle est rattachée au Secrétariat Général du Gouvernement, où elle est dissoute par mesure d'économie en 1947 alors que tous les anciens belligérants maintiennent des structures cryptologiques puissantes comme la NSA aux États-Unis, le GCHQ en Grande Bretagne et le *Zentral Stelle für das Chieffrierwesen* en RFA. Il ne faut pas s'en étonner : les succès cryptologiques de mai 1940 ont vite été oubliés et nous avons fait, en quelque sorte, une guerre sans cryptologie d'attaque. Les autorités civiles et militaires ignorent le rôle déterminant que la cryptologie a joué chez les Britanniques et chez les Américains, et ceux-ci nous tiendront dans l'ignorance de leurs succès jusqu'en 1973. On ignore donc en France l'intervention des scientifiques comme Turing et Max Newman pour la réalisation à Bletchey Park des « Bombes » pour décrypter l'*Enigma*, et du premier ordinateur *Colossus* jamais conçu pour percer le trafic télégraphique chiffré allemand au plus haut niveau. Quant aux militaires, ils estiment, se référant à la campagne de France de mai 1940, que le Chiffre ne fait que ralentir les transmissions et, en forme de boutade, les officiers déclarent que la meilleure façon d'arrêter une division blindée est de lui opposer une autre division blindée ... ou de la faire chiffrer.

Le manque d'une organisation gouvernementale du Chiffre va se faire sentir assez vite puisqu'une nouvelle structure interministérielle est recréée en 1951 : le Service Technique Central des Chiffres (STCCH) chargé de coordonner au plan technique les services du Chiffre des différents ministères, civils et militaires, et de moderniser le Chiffre français, mais sans crédit alloué pour ce faire. Est créée également une Commission Interministérielle des Chiffres regroupant toutes les administrations civiles et militaires utilisatrices, cette Commission est assistée d'un organe technique d'évaluation, la Sous-Commission « Cryptologie » regroupant les experts du chiffre de l'État.

[12] Bureau Central de Renseignements et d'Action.
[13] Direction Générale de la Sécurité Extérieure.

MODERNISATION DU CHIFFRE FRANÇAIS : VERS L'ELECTRONIQUE ET LES MATHEMATIQUES

Après la Seconde Guerre Mondiale et jusque dans les années 1950, les matériels du temps de guerre, M 209 d'origine US, C 36 et B 211 modifiées restent en service. Une machine électromécanique, la CX 52, dont la France a acquis la licence de fabrication, entre en service. La valeur cryptographique de cette machine est bien supérieure à celle de la C36 modifiée et de la M209, grâce à un avancement irrégulier des roues-clé, et on peut lui adjoindre un clavier ainsi qu'un lecteur perforateur de bande télégraphique, ce qui constitue un net progrès, mais les opérations de chiffrement-déchiffrement restent trop lentes.

On peut également utiliser la KL7, machine de conception américaine, qui est la machine de l'OTAN équipant les pays de l'Alliance Atlantique. C'est une machine à rotors comme l'*Enigma* mais bien plus complexe. Elle aussi est très lente. Malgré ce défaut, elle restera en service jusqu'en 1986.

Naturellement, tous les systèmes manuels et en particulier les codes et dictionnaires surchiffrés sont encore abondamment utilisés et le seront jusque vers la fin des années 1980.

Première étape : les machines TARECs.

Dans le début des années 1950 commencent à apparaître des appareils dits « à bande aléatoire une fois » – « à masque jetable » ou encore *« one-time pad »* selon la terminologie à la mode d'aujourd'hui[14]. Ils sont fabriqués en France par SAGEM, il s'agit des TARECs (Translations Régénératices Et Chiffrantes) qui fonctionnent selon le système Vernam connu depuis 1917. Ce sont des appareils télégraphiques travaillant selon le code Baudot à 32 combinaisons : le texte clair perforé sur une bande de papier est lu et additionné bit à bit modulo 2 avec une bande-clé. La bande-clé doit être constituée des 32 caractères perforés sur une bande dite aléatoire utilisée une fois seulement. Toute la sécurité repose sur l'aléa de la bande-clé et sur le fait que la bande-clé doit être utilisée une seule fois. Bien utilisé, le TAREC réalise l'idéal du chiffrement, le secret parfait décrit par Shannon dans son fameux article « Communication Theory of Secrecy Systems »[15] paru dans le *Bell System Technical Journal* en octobre 1949. Cet article avait fortement intéressé la communauté des cryptologues-chiffreurs français, même si certains vieux cryptologues s'en moquaient, considérant que ce que démontrait Shannon à grand renfort d'une théorie de

[14] Voir le chapitre « Du message chiffré au système cryptographique » p. 127.
[15] Shannon, « Communication Theory of Secrecy Systems », pp. 679-683.

l'information qu'ils maîtrisaient assez mal, était connu d'eux depuis longtemps, par expérience et de façon pragmatique. C'était vrai, mais Shannon apportait l'explication scientifique qui manquait précisément à cette expérience, et il fallait que les jeunes cryptologues de conception s'en imprègnent, d'autant plus que les liens avec la cryptologie d'attaque étaient désormais coupés, comme on l'a dit ci-dessus.

Pour utiliser les TARECs avec des clés utilisées une seule fois, il faut une organisation adaptée, telle que des réseaux de transmissions télégraphiques fonctionnant en étoile, comme c'est le cas aux Affaires Etrangères et au Ministère de l'Intérieur : les Ambassadeurs ne correspondent pas entre eux mais chacun avec le Quai d'Orsay à Paris, les Préfets trafiquent avec le Ministère de l'Intérieur mais n'ont pas à communiquer entre eux. Pour ces applications, le TAREC se révélait idéal. Encore fallait-il fabriquer les bandes-clés aléatoires et garantir leur qualité, charge aux Administrations Centrales de les acheminer sur les lieux d'utilisation. Pour faire face à ce besoin est créé, en 1958, un Atelier Interministériel placé au STCCH : il est chargé d'assurer la fabrication des bandes-clés pour les ministères civils et militaires. Mais il faut garantir la qualité de ces bandes fabriquées avec des matériels fournis par Hagelin dont la source d'aléa a été au préalable bien vérifiée. Pour cela, il convient de définir des tests d'aléa qui permettent non seulement de garantir la qualité de l'aléa produit mais de détecter les défauts éventuels de fabrication, qui ne sont pas rares eu égard à la vitesse de perforation des deux bandes identiques fabriquées simultanément à grande vitesse[16] : deux bandes de 100 000 signes sont faites en moins de 15 mn. La mise au point de ces tests a conduit le STCCH à rechercher la compétence d'universitaires spécialistes de statistique mathématique. Comme il n'y a pas de test statistique meilleur que tous les autres, il a fallu définir une panoplie de tests plus ou moins originaux. C'est à partir de cette expérience que les mathématiques sont entrées dans le domaine de la cryptologie, du moins en France.

Mais le fait de réaliser des TARECs fournissant au plan théorique le secret parfait démontré par Shannon ne suffit pas à garantir la sécurité, car il y a loin des calculs et spéculations théoriques aux réalisations matérielles. On constate en effet que les TARECs sont de simples additionneurs modulo 2, qui mélangent une bande-clé aléatoire renfermant tout le secret à une bande claire ou chiffrée. Ils sont donc dotés de lecteurs-perforateurs de bandes, équipements télégraphiques soumis à des variations brutales de tension et de courant qui en font des émetteurs d'ondes électromagnétiques pouvant être captées à distance. Ces ondes, si elles sont corrélées au clair ou à la clé, peuvent se révéler compromettantes et trahir le secret. L'Atelier Interministériel doit donc se doter, dès le début des années 1960, de la

[16] Voir aussi p. 127.

compétence et des moyens – cage de Faraday et mesureurs de champs – pour évaluer le phénomène qualifié de TEMPEST (*Telecommunications Electronic Material Protected from Emanating Spurious Transmissions*). Le Constructeur SAGEM, de son côté, doit acquérir le savoir-faire pour minimiser ce phénomène dans ses équipements, ce qui conduit à un surcoût du matériel considérable. Le phénomène TEMPEST mettait à jour une évidence : un procédé cryptographique ou un algorithme de chiffrement pouvait être parfait, indécryptable en théorie, mais la réalisation matérielle pouvait recéler des canaux cachés à même de compromettre l'information, tout comme aujourd'hui un algorithme programmé sur ordinateur peut voir sa sécurité s'effondrer à cause de failles insoupçonnées dans le système d'exploitation.

Ces TARECs ne pouvaient satisfaire la totalité des besoins des militaires qui travaillent surtout en réseau. C'est la faiblesse de nos moyens, manifeste lors de l'expédition de Suez en 1956, qui va attirer l'attention des autorités et débloquer la situation.

MYOSOTIS et la formation mathématique des cryptologues

Lors de l'opération de Suez conduite avec les Britanniques contre l'avis des Américains et des Soviétiques[17], l'inadéquation de nos moyens, notamment de la B 211 que les Britanniques nous recommandent de ne pas utiliser, est patente. La CX 52 s'avère trop lente et dépassée… Le choc est considérable chez les militaires qui conduiront les opérations en minimisant au maximum le trafic radio chiffré. La Commission Interministérielle des Chiffres recommande de lancer au plus vite l'étude d'un matériel télégraphique moderne : les crédits sont débloqués par les Armées. À la même époque, à la fin des années 1950, l'OTAN décide aussi la modernisation de ses matériels de chiffrement et fait appel aux nations de l'Alliance, sous la forme d'un concours, pour la fourniture d'une machine à chiffrer télégraphique fonctionnant « en circuit » – *on line*. La France décide de participer à ce concours et chaque armée veut piloter un projet : La Marine étudie une machine appelée ULYSSE mais abandonnera son projet assez vite, l'Armée de l'Air se lance avec SAGEM dans l'étude d'une machine électronique inspirée des rotors et compatible avec la KL7 dans un de ses modes de fonctionnement, l'Armée de Terre sponsorise un matériel électronique original chez CSF – aujourd'hui THALES – : MYOSOTIS.

[17] Ferro, *1956, Suez.*

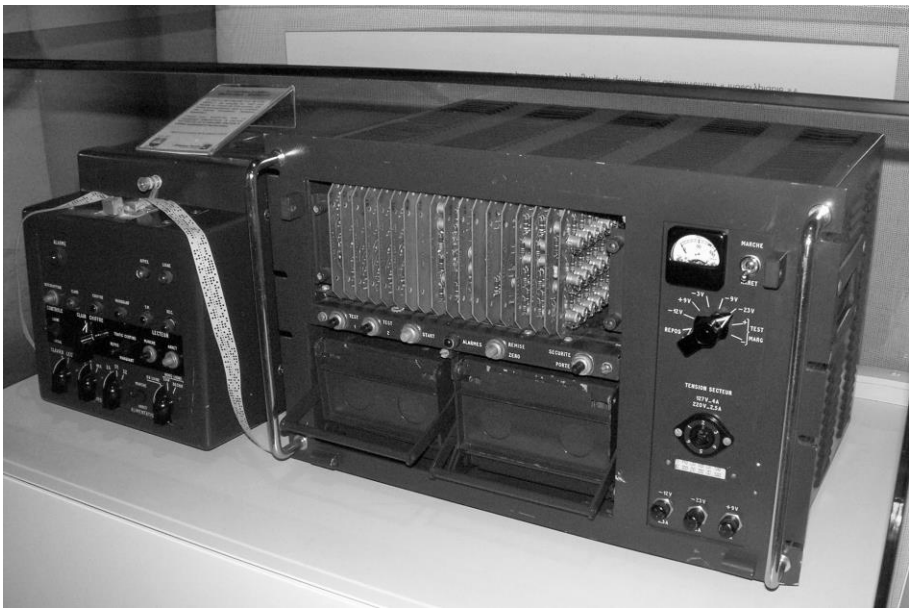


Fig. 2. Machine Myosotis exposée à l'espace Ferrié. Autorisation J. L. Desvignes.

Pour former les jeunes experts en cryptologie dont on manque, est créé en 1960 un Centre d'Etudes Cryptographiques Supérieures (CECS) auprès du Comité d'Action Scientifique de la Défense Nationale qui bénéficie du concours de professeurs de mathématiques de l'Université. Au CECS, qui sera rattaché au STCCH en 1960, les élèves cryptologues reçoivent sur deux ans, outre un enseignement approfondi de cryptologie, un enseignement de qualité dans les diverses branches des mathématiques : théorie des ensembles, théorie des groupes et des corps finis, théorie de l'information et, bien sûr, théorie du secret de Shannon, statistique mathématique et calcul des probabilités, théorie des nombres, codes détecteurs et correcteurs d'erreurs *etc*. En outre les jeunes officiers qui suivent ces cours dans le cadre de l'Enseignement Militaire Supérieur Scientifique et Technique sont invités à suivre, en parallèle, l'enseignement de l'ISUP (Institut de Statistique de l'Université de Paris).

Pour réaliser une machine moderne, les cryptologues savent qu'il faut que cette machine génère des alphabets de chiffrement de façon un peu plus élaborée que dans les machines à rotors comme l'*Enigm*a ou la KL7, et que les alphabets de « Jules César » des machines de type C. Au cours des discussions sur ce thème, quelqu'un, un élève du CECS pense-t-on, a lancé un jour l'idée qu'une machine électronique moderne devrait, pour chaque lettre à chiffrer d'un alphabet à n lettres, choisir au hasard un alphabet parmi les $n!$ alphabets possibles.

L'idée est discutée et paraît séduisante mais est-elle réaliste ? L'ingénieur en chef Marius Gaubert, polytechnicien, membre de la Sous-Commission « Cryptologie », et qui connaît bien la technologie des transistors, étudie la question. Il lui semble que la technologie des transistors permettrait de fabriquer des alphabets si on disposait d'une source de caractères aléatoires fournis à une cadence suffisante. La question se pose alors du nombre de caractères aléatoires qu'il faut fournir pour simuler le tirage d'un alphabet – à 26, 27, 31 et 32 caractères. Les calculs sont effectués par le colonel Ribadeau-Dumas, polytechnicien chef du Bureau du Chiffre de l'Armée de Terre (futur Général de Division et président de l'Association des Réservistes du Chiffre) et, après des calculs numériques assez difficiles à faire car on ne dispose pas d'ordinateur, on arrive au résultat : il suffit de tirer au hasard 127 caractères aléatoires pour avoir 90 % de chance de bâtir un alphabet aléatoire de 32 caractères. Une machine à chiffrer disposant d'un générateur pseudo-aléatoire assez rapide serait donc capable de simuler le tirage au hasard d'un alphabet si elle fournit pour chaque lettre à chiffrer 127 lettres pseudo-aléatoires à l'émission et la réception.

Signalons au passage qu'au cours de ces recherches visant la confection d'alphabets, le professeur Jean Favard (1902-65) de l'Université de Grenoble, qui enseignait à Polytechnique et au CECS dans les années 1960, a proposé le recours à des exponentielles modulaires ou à des logarithmes discrets comme fonctions de chiffrement produisant des alphabets de chiffrement[18]. Il a décrit au passage ce qu'on appellerait aujourd'hui un procédé d'échange public de clés, chose qui ne retint nullement l'attention et passa pour une curiosité. Mais il est vrai qu'on ne disposait pas d'ordinateur et que la taille des nombres en jeu était modeste. L'idée venait trop tôt et tourna court, vraisemblablement à cause de l'impossibilité pratique d'effectuer ces calculs complexes avec les moyens de l'époque. De plus, chaque Administration et chaque Armée disposait d'une organisation parfaitement rodée et efficace pour gérer et distribuer ses clés de chiffrement. Il n'était nul besoin d'envisager d'en changer.

Pour réaliser ces alphabets pseudo-aléatoires dont on vient de parler, restait la question de savoir s'il était possible de réaliser ce générateur pseudo-aléatoire rapide, eu égard à la technologie existante, pour assurer la vitesse requise de chiffrement en ligne – 75 et 50 bauds. Question qui se complique du fait qu'il faut prévoir en outre un dispositif à même de compléter l'alphabet pour les cas rares – mais pas impossibles – où l'alphabet tiré n'est pas complet.

La question intéresse Jean-Pierre Vasseur, l'ingénieur spécialiste des études de transistorisation chez CSF, qui va se passionner pour le

[18] Favard, *Théorie de l'information.*

problème[19]. Il lui semble que l'objectif assigné serait atteint en faisant évoluer un générateur pseudo-aléatoire à 2400 bits/s, ce que va permettre bientôt la technologie disponible. Reste qu'il faut définir un générateur pseudo-aléatoire. Pour réaliser cet automate, ce n'est pas simple : Vasseur et ses collaborateurs vont s'appuyer sur la théorie de Shannon en validant leurs choix par des campagnes approfondies de tests statistiques. Plusieurs principes fondamentaux inspirés par Shannon les conduisent notamment à :

– créer partout où c'est possible de la confusion et de la diffusion entre les informations,
– briser toute corrélation entre les données,
– recourir à des circuits et des logiques non linéaires,
– faire jouer aux éléments secrets variables internes des rôles symétriques et équivalents,
– rechercher au maximum l'équiprobabilité des variables,
– garantir une période minimale suffisante de l'automate.

Mais il faut penser aux conditions d'exploitation. Le but recherché est de ne laisser à l'opérateur aucune initiative lui permettant de commettre des erreurs préjudiciables à la sécurité : toutes les opérations seront automatiques, l'action de l'opérateur se limitant seulement à l'appui sur un bouton pour faire démarrer le chiffrement qui s'effectue automatiquement.

Toutes ces recherches et ce travail effectué en relation avec le STCCH et la Sous-Commission « Cryptologie » ont conduit à la machine MYOSOTIS dont la conception fut validée par nos alliés de l'OTAN. On peut dire que la réalisation de ce projet a introduit de plein pied la conception assistée par les mathématiques de moyens de cryptologie modernes et a fait de M. Vasseur le père de la nouvelle cryptologie gouvernementale française.

De son côté, l'Armée de l'Air avait mis au point sa machine VIOLETTE avec la SAGEM. Il s'agissait d'une machine électronique basée sur des rotors électroniques, mais d'un fonctionnement très complexe dont les performances étaient comparables à celles de MYOSOTIS. Il fallait donc choisir entre MYOSOTIS et VIOLETTE quelle serait la machine qui équiperait l'Armée Française et les Administrations. Le choix n'était pas simple et de sérieuses querelles d'experts éclatèrent au sein de la Sous-Commission « Cryptologie » : comment choisir, au plan cryptologique, la meilleure machine, chacune des deux Armées soutenant son projet à fond ? Dans l'impossibilité de trancher, on fit appel à des sommités scientifiques extérieures et quelques personnalités de l'Université, dont le célèbre professeur Robert Fortet[20] (1912-98), furent invitées à étudier les deux

[19] Ameil, Vasseur et Ruggiu, « Histoire de la machine Myosotis ».
[20] Ses travaux portent notamment sur la théorie des processus aléatoires et la théorie ergodique dans le cadre de la théorie de la mesure. Il était alors directeur du laboratoire de probabilités de Jussieu.

projets et à donner leur avis. Ces mathématiciens de haute volée restaient extrêmement prudents, abasourdis par l'enfer de complexité de chacune des deux machines. Ils découvraient, en collaborant avec les membres de la Sous-Commission « Cryptologie », qu'il était impossible de démontrer la valeur cryptologique de ces automates … sinon en montrant qu'on savait les décrypter, c'est-à-dire en montrant qu'ils n'étaient pas valables. En fait, une machine à chiffrer reste valable tant qu'on n'exhibe pas son décryptement. Or, VIOLETTE et MYOSOTIS avaient été conçues pour ne pas être décryptables, du moins dans l'état des connaissances des experts du moment. Naturellement, cette situation n'exclut pas la possibilité qu'une faille insoupçonnée puisse être ultérieurement découverte selon le progrès des connaissances cryptologiques et milite pour un réexamen périodique des machines. Les deux machines ne pouvaient être départagées au seul plan de la cryptologie, et les mathématiciens consultés restaient muets…. C'est donc sur les conditions d'emploi et d'exploitation que se fonda le choix, VIOLETTE étant beaucoup plus encombrante et volumineuse que MYOSOTIS, c'est cette dernière qui fut retenue en 1965 pour les Armées Françaises et construite sur la base d'un accord entre les deux industriels concernés. Un fossé venait d'être franchi ; avec MYOSOTIS, on chiffrait et déchiffrait plus vite qu'on ne transmettait, le reproche fait au chiffre de ralentir les transmissions venait de tomber !

CONCLUSION

À partir des études de définition de MYOSOTIS, les armées ont entretenu ultérieurement un courant constant d'études et de réalisations – chiffrement de la parole numérisée par *vocoder*[21], chiffrement du fac-similé, cryptophonie numérique tactique, chiffrement des données, chiffrement d'artères de transmissions, chiffrement des voies montantes et descendantes des satellites, chiffrement du réseau intégré de la zone de combat, *etc*. – qui perdure aujourd'hui. Naturellement, ces études et réalisations se sont enrichies des nouveaux concepts mathématiques apparus depuis 1976, notamment des systèmes à clé publique et de la notion plus récente de « sécurité prouvée ». On peut dire qu'aujourd'hui la cryptologie gouvernementale est fondée en grande partie sur les mathématiques telles qu'elles apparaissent dans la cryptologie ouverte et universitaire.

[21] Le vocoder (*voice coder*) est un appareil mis au point aux *Bell Telephone Laboratories* pendant la Seconde Guerre Mondiale, permettant de coder la voix humaine à partir d'un découpage des fréquences en dix blocs, et d'en effectuer ainsi la transmission par câble télégraphique. Ségal, *Le zéro et le un*, p. 116.

Parallèlement au développement des nouvelles technologies, les experts du chiffre gouvernementaux ont étendu leur champ d'action et, depuis 1986, se sont transformés en spécialistes de la sécurité des systèmes d'information prenant en compte, au-delà de la cryptologie et de la sécurité des communications, la sécurité des systèmes d'information, qui comporte trois volets : la cryptologie, la protection contre les rayonnements compromettants (TEMPEST), et la sécurité informatique. Le STCCH dont on a parlé ci-dessus est devenu le Service Central des Chiffres et de la Sécurité des Télécommunications (SCCST) en 1976. Il est remplacé par la Direction Centrale de la Sécurité des Systèmes d'information (DCSSI) du Secrétariat Général de la Défense Nationale, devenue l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Les études de cryptologie de la Défense sont désormais pilotées par le Centre Electronique de l'Armement (CELAR) de Rennes.

BIBLIOGRAPHIE

Ameil, X., Vasseur, J.-P., et Ruggiu, G., « Histoire de la machine Myosotis », *Actes du septième colloque sur l'histoire de l'informatique et des transmissions, Rennes-Cesson*, 2004, pp. 95-125.

Bazeries, E., *Les chiffres secrets dévoilés, étude historique sur les chiffres appuyée de documents inédits tirés des différents dépôts d'archives*, Paris, E. Fasquelle, 1901.

Cattieuw, A. et Hébrard, P., « L'origine des codes secrets », *Pour la Science*, numéro spécial « La cryptographie, l'art du secret », juillet-octobre 2002, n° 36, pp. 8-17.

— « De la mécanique à l'ordinateur », *Pour la Science*, numéro spécial « La cryptographie, l'art du secret », juillet-octobre 2002, n° 36, pp. 18-25.

Delastelle, F., *Traité élémentaire de cryptographie*, Paris, Gauthier-Villars, 1902.

De Lastours, S., *La France gagne la guerre des codes secrets*, Paris, Taillandier, 1998.

De Viaris, G., « Cryptographie », *Le Génie Civil*, 1888, tome XXIII, pp. 24-32, pp. 38-39, pp. 55-56, pp. 72-75, pp. 84-88, pp. 104-107.

Favard, J., *Théorie de l'information. Langage. Codage. Cryptage,* Paris, Service de la Présidence du Conseil, 1960.

Ferro, M., *1956, Suez*, Paris, Editions Complexe, 1982.

Givierge, M., *Cours de cryptographie*, Nancy-Paris-Strasbourg, Berger-Levrault, 1925.

Hermann, A., *Méthode pour chiffrer et déchiffrer les dépêches secrètes*, Paris, Hermann, 1872.

Kahn, D., *The Codebreakers, The Comprehensive History of Secret Communication from Ancient Times to the Internet*, New York, Scribner, 1996.

Kerckhoffs, A., « La cryptographie militaire », *Journal des sciences militaires*, Paris, Imprimerie et Librairie Militaires, L. Baudouin & Co.

Ségal, J., *Le Zéro et le Un, Histoire de la notion scientifique d'information au 20e siècle*, Paris, Ed. Syllepse, Coll. « Matériologiques », 2004.

Shannon, C. E., *Collected Papers of C. E. Shannon*, (eds.) Sloane, N. J. A. et Wyner, A. D., New York, IEEE Press, 1993.

— « Communication Theory of Secrecy Systems », *The Bell System Technical Journal*, 1946-49, vol. 28, pp. 656-711, *in Shannon's Collected Papers*, pp. 656-711.

Valério, P.-L.-E., *De la cryptographie, essai sur les méthodes de déchiffrement*, Paris, L. Baudoin, 1893-1896, 2 vols.

LES NOUVELLES ORIENTATIONS DE LA CRYPTOGRAPHIE[*] [1]

Whitfield DIFFIE et Martin E. HELLMAN[2]
Traduction Marie-José DURAND-RICHARD et Philippe GUILLOT

RESUME

Cet article présente deux types de développements contemporains en cryptographie. L'extension des applications de télétraitement a engendré un besoin de nouveaux types de systèmes cryptographiques qui minimisent le besoin de sécuriser les canaux pour la distribution des clés et fournissent l'équivalent d'une signature écrite. Cet article explore des pistes pour résoudre ces problèmes qui sont présentement ouverts. Il examine aussi comment la théorie de la communication et la théorie du calcul commencent à fournir des outils permettant de résoudre des problèmes cryptographiques longtemps résistants.

INTRODUCTION

Nous sommes aujourd'hui à l'aube d'une révolution en cryptographie. La diminution des coûts du matériel numérique a permis de se libérer des

---

[*] NdT. : la version originale de cet article a été publiée en 1976 dans IEEE *Transactions on Information Theory*, vol. 22, n° 6, pp. 644-654.

[1] Manuscrit reçu le 3 juin 1976. Ce travail a été partiellement soutenu par la bourse NSF ENG 10173 de la *National Science Foundation.* Il a été en partie présenté au *IEEE Information Theory Workshop*, Lenox MA, 23-25 Juin 1975, et au *IEEE International Symposium on Information Theory*, Ronneby, Suède, 21-24 Juin 1976.

[2] NdT. : au moment de la publication de cet article, W. Diffie travaillait au département d'ingénierie électrique de l'université de Stanford, CA, et au Laboratoire d'intelligence artificielle de Stanford, CA 94305. M. E. Hellman travaillait au département d'ingénierie électrique de l'université de Stanford CA 94305. Tous deux étaient membres de l'IEEE.

limitations inhérentes au calcul mécanique et a réduit le coût des systèmes cryptographiques jusqu'à pouvoir les mettre à la disposition des applications commerciales : distributeurs de billets, terminaux d'ordinateurs. En retour, ces applications créent le besoin de nouveaux types de systèmes cryptographiques, qui permettent de minimiser la nécessité de canaux sécurisés de distribution des clés, et de fournir l'équivalent d'une signature écrite. En même temps, des développements théoriques en théorie de l'information et en informatique permettent d'envisager l'obtention de cryptosystèmes à sécurité prouvée, transformant cet art ancien en science.

Le développement des réseaux de communication contrôlés par ordinateur permet d'envisager des contacts faciles et peu coûteux entre des personnes ou des ordinateurs situés d'un bout à l'autre de la planète, remplaçant de nombreux courriers et voyages par des télécommunications. Dans de nombreux cas, il est indispensable de sécuriser ces échanges à la fois contre des oreilles indiscrètes et contre l'injection malveillante de faux messages. La résolution de ce problème de sécurité est aujourd'hui très en retard par rapport à d'autres problèmes de technologie des communications. La cryptographie contemporaine est incapable de satisfaire ces exigences en ce sens que sa mise en œuvre impose de sérieux inconvénients aux utilisateurs du système, jusqu'à ruiner bon nombre des bénéfices du télétraitement.

Le problème cryptographique le mieux connu est celui de la confidentialité : empêcher le prélèvement non autorisé d'information lors de communications sur un canal non sécurisé. Toutefois, utiliser la cryptographie pour assurer cette confidentialité impose en général aux deux interlocuteurs de partager une clé qui ne soit connue de personne d'autre. Ils le font en envoyant une clé à l'avance par une voie sécurisée quelconque comme par exemple un messager privé ou un courrier recommandé. Cependant, une communication privée entre personnes qui n'ont eu aucune relation préalable est chose courante dans le domaine des affaires, et il n'est pas réaliste d'envisager que les premiers contacts commerciaux soient retardés jusqu'à ce que des clés soient transmises par quelque moyen physique. Le coût et le retard imposé par le problème de la distribution des clés constituent une barrière majeure au transfert des communications d'affaires vers les grands réseaux de télécommunications.

Le paragraphe « Cryptographie à clé publique » propose deux approches nouvelles pour transmettre l'information relative aux clés sur des canaux publics (c'est-à-dire non sécurisés) sans compromettre la sécurité du système. Dans un *cryptosystème à clé publique*, le chiffrement et le déchiffrement sont gouvernés par deux clés distinctes, E et D, telles que le calcul de D à partir de E soit calculatoirement irréalisable (nécessitant par exemple 10^{100} instructions). La clé de chiffrement E peut donc être publiquement divulguée sans compromettre la clé de déchiffrement D.

Chaque utilisateur du réseau peut donc placer sa clé de chiffrement dans un répertoire public. Ceci permet à tout utilisateur du système d'envoyer à tout autre utilisateur un message, chiffré de telle sorte que seul le destinataire voulu puisse le déchiffrer. Comme tel, un cryptosystème à clé publique est un chiffre à accès multiple. Une conversation privée peut ainsi avoir lieu entre deux individus même s'ils n'ont jamais communiqué auparavant. Chacun envoie des messages à l'autre, chiffré avec la clé de chiffrement publique du destinataire, et déchiffre les messages qu'il reçoit avec sa propre clé de déchiffrement.

Nous proposons quelques pistes pour développer des crytposystèmes à clé publique, mais ce problème reste largement ouvert.

Les *systèmes de distribution de clé publique* offrent une approche nouvelle pour éliminer le besoin d'un canal sûr lors de la distribution des clés. Dans un tel système, deux utilisateurs qui souhaitent échanger une clé communiquent mutuellement jusqu'à ce qu'ils s'accordent sur une clé commune. Si l'oreille indiscrète d'une tierce partie capte cet échange, il doit lui être calculatoirement irréalisable de calculer la clé à partir des informations captées. Une solution possible au problème de la distribution publique des clés est donnée dans le paragraphe « Cryptographie à clé publique », et Merkle[3] apporte une solution partielle sous une forme différente.

Un second problème, susceptible d'une solution cryptographique, est celui de l'authentification. Il intervient lorsqu'on souhaite remplacer les communications d'affaires actuelles par des systèmes de télétraitement. Dans les affaires courantes, la validité des contrats est garantie par des signatures. Un contrat signé sert de preuve légale d'un accord, que son détenteur peut présenter à un tribunal si nécessaire. Mais l'utilisation de ces signatures suppose que ces contrats écrits soient transmis et conservés. Pour remplacer ce document papier par une solution purement digitale, chaque utilisateur doit pouvoir produire un message dont l'authenticité est vérifiable par n'importe qui, mais qui ne peut avoir été produit par personne d'autre, pas même le destinataire. Puisqu'un message ne peut provenir que d'une seule personne, mais peut être reçu par beaucoup d'autres, ces échanges peuvent être considérés comme un chiffrement à grande diffusion. Les techniques actuelles d'authentification électronique ne conviennent pas à ce besoin.

Le paragraphe « Authentification à sens unique » examine le problème relatif à l'obtention d'une véritable signature numérique qui dépende du message. Pour des raisons qui seront explicitées plus loin, nous l'appellerons le problème de l'authentification à sens unique. Nous donnerons quelques solutions partielles et nous montrerons comment un cryptosystème à clé

[3] Merkle, « Secure Communication over an Insecure Channel ».

publique peut être transformé en un système d'authentification à sens unique.

Le paragraphe « Interdépendance des problèmes et portes dérobées » traitera des relations entre différents problèmes cryptographiques, et introduira le problème encore plus difficile des portes dérobées.

Au moment même où les communications et l'informatique ont donné naissance à de nouveaux problèmes cryptographiques, leurs retombées, la théorie de l'information ainsi que la théorie du calcul ont commencé à fournir des outils pour résoudre des problèmes importants de cryptographie classique.

La recherche de codes incassables est un des plus vieux thèmes de recherche en cryptographie, mais jusqu'à ce siècle, tous les systèmes proposés ont finalement été cassés. Pourtant, dans les années 1920, on a produit le « masque jetable », puis on a montré qu'il était incassable[4]. Un quart de siècle plus tard, la théorie de l'information a donné des fondements solides aux bases théoriques sous-jacentes et aux systèmes associés[5]. Le masque jetable nécessite des clés extrêmement longues et a donc un coût prohibitif pour la plupart des applications.

À l'opposé, la sécurité de la plupart des systèmes cryptographiques s'accompagne d'une difficulté calculatoire pour le cryptanalyste qui doit découvrir le texte clair sans connaître la clé. Ce problème relève du domaine de la complexité calculatoire et de l'analyse des algorithmes, deux domaines qui étudient la difficulté à résoudre les problèmes calculatoires. En utilisant les résultats de ces théories, on pourra étendre les preuves de sécurité à des classes de systèmes plus utiles dans un futur proche. Le paragraphe « Complexité calculatoire » explore cette possibilité.

Avant de procéder à de nouveaux développements, le prochain paragraphe introduit le vocabulaire et définit les contextes de menaces.

CRYPTOGRAPHIE CONVENTIONNELLE

La cryptographie est l'étude des systèmes « mathématiques » impliquant deux types de problèmes de sécurité : la confidentialité et l'authentification. Un système de confidentialité empêche le prélèvement d'information par des tiers non autorisés dans des messages transmis sur un canal public. L'émetteur d'un message est ainsi assuré que celui-ci ne sera lu que par le destinataire voulu. Un système d'authentification empêche l'injection non autorisée de messages sur un canal public, et assure le destinataire d'un message de la légitimité de son envoyeur.

---

[4] Kahn, *The Codebreakers*, pp. 398-400.

[5] Shannon, « Communication Theory of Secrecy Systems ».

Un canal est considéré comme public si sa sécurité n'est pas adaptée aux besoins de ses usagers. Un canal comme une ligne téléphonique peut donc être considéré comme privé par certains et public par d'autres. Tout canal peut être menacé soit par des écoutes, soit par des injections, soit par les deux, selon la façon dont il est utilisé. Dans les communications téléphoniques, la menace d'injection est dominante, puisque le correspondant ne peut déterminer quel téléphone l'appelle.

Les écoutes qui nécessitent l'usage d'un branchement sur la ligne sont techniquement plus difficiles et légalement hasardeuses. Mais en radio, la situation est inverse : les écoutes sont passives et ne comportent aucun danger légal, tandis que l'injection expose le transmetteur illégitime à être découvert et poursuivi.

Ayant séparé nos problèmes entre confidentialité et authentification, nous allons encore subdiviser le problème de l'authentification entre l'authentification du message, qui vient d'être défini ci-dessus, et l'authentification de l'utilisateur, pour laquelle la seule tâche du système est de vérifier qu'un individu est bien celui qu'il prétend être. Par exemple, l'identité d'un individu qui présente une carte de crédit doit être vérifiée, alors qu'il n'a aucun message à transmettre. Malgré cette absence apparente de message, les deux problèmes sont en grande partie équivalents. Lors de l'authentification de l'utilisateur, il y a un message implicite : « je suis l'utilisateur X » tandis que l'authentification du message consiste simplement à vérifier l'identité de son émetteur. Les différences entre les contextes de menace et d'autres aspects de ces sous-problèmes font qu'il est commode de les distinguer.

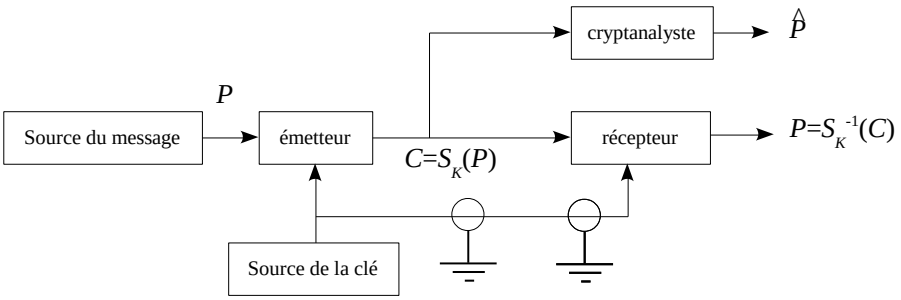


Fig. 1. Flux d'informations dans un système cryptographique conventionnel.

La figure 1 illustre le flux d'information dans un système cryptographique conventionnel utilisé pour la confidentialité des communications. Il y a trois parties : l'envoyeur, le destinataire, et l'intercepteur. L'envoyeur produit un texte clair, ou message non chiffré *P*, à communiquer sur un canal non sécurisé au destinataire légitime. Afin

d'empêcher l'intercepteur de connaître P, l'envoyeur applique à P une transformation inversible S_K pour produire un cryptogramme $C=S_K(P)$. La clé K n'est transmise qu'au destinataire légitime *via* un canal sécurisé, représenté sur la figure par un câble blindé. Comme le destinataire légitime connaît K, il peut déchiffrer C en appliquant $S_K{}^{-1}$ pour obtenir, $S_K{}^{-1}(C) = S_K{}^{-1}(S_K(P)) = P$, le message clair d'origine. Le canal sécurisé ne peut pas être utilisé pour transmettre P lui-même pour des raisons de capacité ou de retard. Par exemple, le canal sécurisé pourrait consister en une estafette hebdomadaire, et le canal non sécurisé en une ligne téléphonique.

Un *système cryptographique*, est une famille $\{S_K\}_{K\in\{K\}}$, à un seul paramètre, de transformations inversibles :

$$S_K : \{P\} \rightarrow \{C\}$$

d'un espace $\{P\}$ de messages clairs dans un espace $\{C\}$ de messages chiffrés. Le paramètre K est appelé la clé. Il est sélectionné dans un ensemble fini $\{K\}$ appelé e*space des clés*. Si les espaces des messages $\{P\}$ et $\{C\}$ sont égaux, nous les noterons tous deux $\{M\}$. Quand on évoque des transformations cryptographiques individuelles S_K, on omet parfois de mentionner le système et on se réfère seulement à la transformation K.

La conception d'un cryptosystème $\{S_K\}$ a pour but de rendre les opérations de chiffrement et de déchiffrement peu coûteuses, mais aussi d'assurer que la réussite de toute opération de cryptanalyse soit trop complexe pour être économique. Il y a deux approches à ce problème. Un système qui est sûr du point de vue du coût calculatoire de la cryptanalyse à l'aide d'un ordinateur, mais qui succomberait à une attaque avec des moyens de calcul illimités, est appelé système *calculatoirement sûr*, tandis qu'un système qui résiste à toute cryptanalyse indépendamment des moyens informatiques mis en œuvre est appelé système *inconditionnellement sûr*. Les systèmes inconditionnellement sûrs sont traités par Shannon[6] dans son article de 1949 et par Hellman[7] dans son article de 1975. Ils relèvent de la partie de la théorie de l'information appelée la théorie de Shannon, qui traite de l'étude des performances optimales pouvant être obtenues avec des moyens de calcul illimités.

La sécurité inconditionnelle résulte de l'existence de plusieurs solutions significatives pour un cryptogramme donné. Par exemple, le cryptogramme XMD obtenu par substitution simple à partir d'un texte en anglais peut représenter les clairs suivants : « *now* », « *and* », « *the* », *etc*. Un cryptogramme calculatoirement sûr, au contraire, contient quant à lui suffisamment d'information pour déterminer le clair et la clé de chiffrement de façon unique. Sa sécurité repose seulement sur le coût de leur calcul.

---

[6] Shannon, « Communication theory of secret systems ».
[7] Hellman, « An Extension of the Shannon Theory Approach to Cryptography ».

Le seul système inconditionnellement sûr d'usage courant est le *masque jetable* (*one-time pad*) dans lequel le clair est combiné à une clé de même longueur, choisie aléatoirement[8]. Bien qu'on puisse démontrer qu'un tel système est sûr, la grande taille requise pour la clé rend ce système impraticable pour la plupart des applications. Sauf mention explicite, cet article ne traite que de systèmes calculatoirement sûrs, puisqu'ils sont plus généralement utilisables. Lorsque nous parlons du besoin de développer des cryptosystèmes prouvés sûrs, nous excluons ceux qui, comme le masque jetable, ne sont pas facilement maniables. Nous aurons plutôt à l'esprit des systèmes qui n'utilisent que quelques centaines de bits de clé, et qu'on peut implémenter soit avec une faible quantité de matériel numérique, soit avec quelques centaines de lignes de logiciel.

Nous dirons qu'une tâche est *calculatoirement irréalisable* si son coût en temps de calcul et en espace mémoire est fini mais trop grand pour être envisagé.

De même que les codes correcteurs d'erreurs sont classés en codes convolutifs et codes en blocs, les systèmes cryptographiques peuvent être divisés en deux grandes classes : le *chiffrement à flots* et le *chiffrement par blocs*. Le chiffrement à flots opère sur des petits morceaux du texte clair (symboles binaires ou caractères), produisant habituellement une suite pseudo-aléatoire de bits qui est additionnée modulo 2 aux bits du texte clair. Le chiffrement par blocs agit de manière purement combinatoire sur de grands blocs de texte, de telle manière qu'un petit changement sur un bloc d'entrée produise un changement majeur sur la sortie qui en résulte[9]. Cet article traite surtout du chiffrement par blocs, parce que cette propriété de *propagation d'erreur* intervient de manière intéressante dans de nombreuses applications d'authentification.

Dans un système d'authentification, la cryptographie est utilisée pour garantir au destinataire l'authenticité du message. Non seulement on doit empêcher un fouineur d'injecter dans le canal des messages totalement nouveaux qui puissent sembler authentiques, mais il doit également lui être impossible de créer des messages apparemment authentiques en combinant, ou seulement en répétant de vieux messages qu'il aurait copiés dans le passé. En général, un système cryptographique destiné à garantir la confidentialité ne garantit rien contre cette malveillance.

Pour garantir l'authenticité d'un message, on ajoute une information, qui est fonction, non seulement du message et d'une clé secrète, mais aussi de la date et de l'heure, par exemple en attachant la date et l'heure à chaque message et en chiffrant le tout. Ceci garantit que seul quelqu'un qui possède la clé peut produire des messages qui, lorsqu'ils seront déchiffrés,

[8] NdT. : voir le chapitre « Du message chiffré au système cryptographique » p. 127.
[9] NdT. : *ibid*., pp. 144-147.

contiendront la bonne date et la bonne heure. Des précautions doivent cependant être prises pour utiliser un système dans lequel de petits changements dans le cryptogramme produisent de grands changements dans le texte clair une fois déchiffré. Cette propagation intentionnelle d'erreur assure que si l'injection délibérée de bruit dans le canal change un message comme « effacer le fichier 7 » en un message différent tel que « effacer le fichier 8 », elle corrompe également les informations d'authentification. Le message sera ainsi rejeté comme non authentique.

La première étape pour évaluer l'adéquation d'un système cryptographique est de répertorier les menaces auxquelles il peut être soumis. Les menaces ci-dessous peuvent survenir dans les systèmes cryptographiques utilisés, soit pour la confidentialité, soit pour l'authentification.

Une *attaque à chiffré seul* est une attaque où le cryptanalyste ne possède que le message chiffré.

Une *attaque à clair connu* est une attaque où le cryptanalyste possède une quantité substantielle de couples clair-chiffré qui se correspondent.

Une *attaque à clair choisi* est une attaque où le cryptanalyste peut soumettre au chiffrement un nombre illimité de textes clairs de son choix et examiner les cryptogrammes obtenus.

Dans tous les cas, nous admettrons que l'adversaire connaît le système général $\{S_K\}$ utilisé, puisque cette information peut être obtenue en analysant le dispositif cryptographique. Alors que de nombreux utilisateurs de la cryptographie tentent de garder leur équipement secret, de nombreuses applications commerciales, au contraire, requièrent non seulement que le système général soit public, mais qu'il soit standard.

Une attaque à chiffré seul intervient très souvent en pratique. Le cryptanalyste utilise seulement la connaissance des propriétés statistiques de la langue utilisée (par exemple, en anglais la lettre *e* apparaît 13 % du temps) et la connaissance de certains mots « probables » (par exemple, une lettre peut commencer par « Cher Monsieur »). C'est la menace la plus faible à laquelle un système peut être soumis et tout système succombant à cette attaque est considéré comme totalement non sûr.

Un système qui est sûr contre une attaque à clair connu libère ses utilisateurs du besoin de garder secrets leurs anciens messages ou de les reformuler avant de les déclassifier. C'est une charge déraisonnable que de faire peser sur les utilisateurs du système, en particulier dans les situations commerciales où des annonces de produits ou des communiqués de presse peuvent être transmis sous forme chiffrée avant d'être publiquement divulgués. Une situation semblable dans les correspondances diplomatiques a conduit à casser de nombreux systèmes supposés sûrs. Même si une attaque à clair connu n'est pas toujours possible, elle est assez fréquente pour qu'un système qui ne peut y résister ne soit pas considéré comme sûr.

L'attaque à clair choisi est difficile à réaliser en pratique, mais une approximation peut en être obtenue. Par exemple, soumettre une proposition commerciale à un compétiteur peut conduire à la chiffrer pour la transmettre à sa direction. Un système de chiffrement qui résiste à l'attaque à clair choisi libère ses utilisateurs du souci de savoir si ce sont des concurrents qui ont semé des messages dans leur système.

Afin de certifier la sécurité des systèmes, il convient de tenir compte de l'attaque la plus puissante possible comme celles qui, non seulement correspondent à des modèles plus réalistes dans l'environnement de travail du système cryptographique, mais rendent plus facile l'évaluation de la force du système. Beaucoup de systèmes qui sont difficiles à analyser dans une attaque à chiffré seul peuvent être immédiatement éliminés par une attaque à clair connu ou à clair choisi.

Il est clair d'après ces définitions que la cryptanalyse est un problème d'identification. Les attaques à clair connu et à clair choisi correspondent respectivement aux problèmes d'identification passive et active. Au contraire de beaucoup de sujets où on considère un système d'identification, comme le diagnostic automatique de panne, le but de la cryptographie est de construire des systèmes dans lesquels l'identification est difficile, plutôt que facile.

L'attaque à clair choisi est souvent appelée attaque IFF, terminologie qui tient son origine du développement des systèmes cryptographiques IFF (*Identification Friend or Foe)* après la Seconde Guerre Mondiale. Un système IFF permet aux radars militaires de discerner automatiquement entre un avion ami et un avion ennemi. Le radar envoie un signal variant dans le temps comme défi à l'avion. Celui-ci le chiffre avec la clé appropriée, et le renvoie au radar. En comparant la réponse avec la version correctement chiffrée du défi, le radar peut reconnaître un avion ami. Lorsque l'avion se trouve en territoire ennemi, les cryptanalystes ennemis peuvent envoyer des signaux et attendre les réponses chiffrées pour tenter de déterminer la clé d'authentification utilisée, et ainsi monter une attaque à clair choisi contre le système. En pratique, cette menace est contrée en restreignant la forme des défis qui n'ont pas à être imprévisibles, mais seulement non répétés.

Il y a d'autres menaces sur les systèmes d'authentification qui ne peuvent pas être traitées par la cryptographie conventionnelle, et nécessitent de recourir à de nouvelles idées et de nouvelles techniques qui seront introduites dans cet article. La *menace de compromission des données d'authentification du récepteur* est motivée par la situation des réseaux à utilisateurs multiples, où le destinataire est souvent le système lui-même. Les tables de mots de passe du destinataire et autres données d'identification sont alors plus vulnérables au vol que celles de l'émetteur (un utilisateur individuel). Comme nous le verrons plus loin, certaines techniques protégeant contre ces menaces peuvent également protéger contre la *menace*

de contestation. En effet, un message peut être envoyé et ensuite répudié par l'émetteur ou le destinataire. Ou bien, une des deux parties peut affirmer qu'un message a été envoyé sans que cela ne soit en fait le cas. Signatures numériques infalsifiables et reçus numériques sont donc nécessaires. Par exemple, un agent de change malhonnête peut essayer de couvrir, pour ses gains personnels, des achats ou des ventes non autorisés en fabriquant de faux ordres de clients, ou un client peut réfuter un ordre qu'il a pourtant produit après s'être rendu compte que cela lui cause une perte. Nous introduirons les concepts qui permettent au destinataire de vérifier l'authenticité d'un message, tout en l'empêchant de produire des messages d'apparence authentique, et ce faisant assurent la protection contre la menace de falsification des données d'authentification du receveur et contre la menace de contestation.

CRYPTOGRAPHIE A CLE PUBLIQUE

Comme le montre la figure 1, la cryptographie a été une mesure d'extension de la sécurité. Dès qu'il existe un canal sûr le long duquel des clés peuvent être transmises, la sécurité peut être étendue à d'autres canaux ayant une bande passante supérieure ou un temps de transfert plus réduit, par le chiffrement des messages sur ces canaux. Ceci a eu pour effet de limiter l'usage de la cryptographie à des communications entre acteurs qui se sont préalablement préparés en vue d'une sécurité cryptographique.

Pour développer de grands réseaux de télécommunication sécurisés, ceci doit changer. Un grand nombre n d'usagers conduit à un nombre encore plus grand, $(n^2 - n)/2$, de paires potentielles d'usagers qui souhaitent établir une communication privée, à l'abri des autres. Il n'est pas réaliste de supposer que chaque couple d'utilisateurs sans aucune relation préalable puisse attendre la transmission d'une clé par quelque moyen physique sécurisé, ou que toutes ces clés pour tous les $(n^2 - n)/2$ paires d'usagers puissent être préparées à l'avance. Dans un autre article[10], les auteurs ont considéré une approche conservatoire, qui ne nécessite pas de développement cryptographique nouveau, mais qui implique une sécurité plus réduite, peu commode et la restriction du réseau à une configuration en étoile dépendant du protocole de connexion initial.

Nous suggérons qu'il est possible de développer un système du type de celui présenté sur la figure 2, dans lequel deux parties qui communiquent seulement sur un canal public, et qui n'utilisent que des techniques publiques, peuvent créer une connexion sécurisée. Nous examinerons deux approches de ce problème appelées respectivement cryptosystèmes à clé

[10] Diffie et Hellman, « Multiuser Cryptographic Techniques ».

publique et systèmes de distribution publique des clés. Les premiers sont plus puissants, se prêtant eux-mêmes à une solution au problème de l'authentification traité dans le paragraphe suivant, tandis que les seconds sont plus proches d'une réalisation effective.

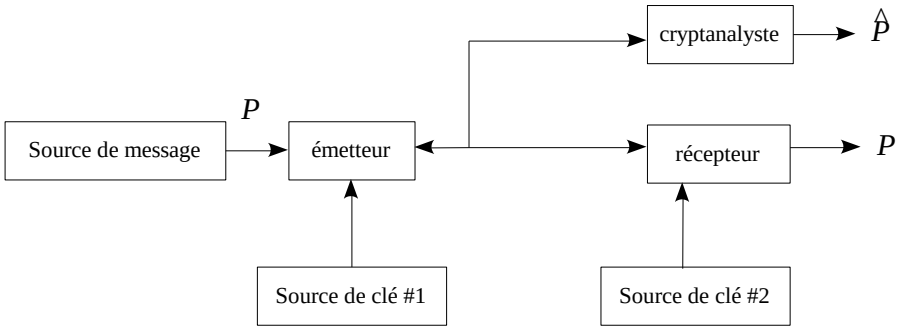


Fig. 2. Flot d'information sur un système à clé publique.

Un *cryptosystème à clé publique* est la donnée d'une paire de familles $\{E_K\}_{K \in \{K\}}$ et $\{D_K\}_{K \in \{K\}}$ d'algorithmes représentant des transformations inversibles :

$$E_K : \{M\} \to \{M\}$$

$$D_K : \{M\} \to \{M\}$$

dans l'espace fini de messages $\{M\}$, tels que :

1) Pour tout $K \in \{K\}$, E_K est l'inverse de D_K.

2) Pour tout $K \in \{K\}$, et $M \in \{M\}$, les algorithmes E_K et D_K sont facilement calculables.

3) Pour presque tout $K \in \{K\}$, il est calculatoirement impossible de retrouver, à partir de E_K, un algorithme facile à calculer équivalent à D_K.

4) Pour tout $K \in \{K\}$, il est possible de trouver des paires de fonctions inverses E_K et D_K à partir de K.

En raison de la troisième propriété, la fonction de chiffrement E_K d'un utilisateur peut être rendue publique sans compromettre la sécurité de sa clé de déchiffrement secrète D_K. Le système cryptographique est ainsi découpé en deux parties **:** une famille de transformations de chiffrement et une famille de transformations de déchiffrement de telle sorte que, étant donné un élément d'une famille, il soit irréalisable de trouver l'élément correspondant de l'autre famille.

La quatrième propriété garantit qu'il est concrètement possible de calculer des paires correspondantes de transformations inverses quand on ne

se donne aucune contrainte sur les transformations de chiffrement ou de déchiffrement. En pratique, l'équipement cryptographique doit contenir un générateur de nombres véritablement aléatoires (par ex. une diode bruitée) pour générer K, couplé à un algorithme qui calcule les paires E_K et D_K à partir de ses sorties.

Ce type de système simplifie grandement le problème de la distribution des clés. Chaque utilisateur produit une paire de transformations inverses E et D sur son terminal. La transformation de déchiffrement D doit être tenue secrète, et n'a jamais besoin d'être communiquée sur quelque canal que ce soit. La clé de chiffrement E peut être rendue publique en la plaçant dans un répertoire public, avec le nom et l'adresse de l'utilisateur. N'importe qui peut ainsi chiffrer des messages et les envoyer vers l'utilisateur, mais personne d'autre ne peut déchiffrer ce message. Les cryptosystèmes à clé publique peuvent ainsi être considérés comme *des chiffrements à accès multiples.*

Il est crucial que le fichier public des clés de chiffrement soit protégé contre toute modification non autorisée. Cette tâche est rendue plus facile du fait de la nature publique du fichier. La protection contre la lecture n'est pas nécessaire, mais comme ce fichier n'est pas modifié fréquemment, on peut avantageusement employer des mécanismes élaborés de protection de l'écriture.

Un exemple suggestif, mais malheureusement inutilisable, de système à clé publique consiste à chiffrer le clair, représenté par un vecteur binaire m de dimension n en le multipliant par une matrice inversible E de dimension $n \times n$. Le cryptogramme est alors égal à Em. En posant $D = E^{-1}$, on a $m = Dc$. Ainsi, le chiffrement et le déchiffrement nécessitent environ n^2 opérations. Mais calculer D à partir de E nécessite l'inversion d'une matrice, ce qui est un problème plus difficile. Et il est plus simple, du moins conceptuellement, d'obtenir une paire arbitraire de matrices inverses l'une de l'autre que d'inverser une matrice donnée. Il suffit de partir de la matrice identité I et de faire les opérations élémentaires en ligne et en colonne pour obtenir une matrice inversible arbitraire E, puis, partant de I, d'effectuer les réciproques des mêmes opérations élémentaires dans l'ordre inverse $D = E^{-1}$. La suite des opérations élémentaires peut être facilement déterminée à partir d'une chaîne de bits aléatoires.

Malheureusement, l'inversion des matrices prend seulement environ n^3 opérations. Le rapport du temps « cryptanalytique » (c'est-à-dire le temps de calcul de D à partir de E) au temps de chiffrement ou de déchiffrement est ainsi au plus n, et il faudrait des tailles énormes de blocs pour obtenir des rapports de 10^6 ou plus. De plus, il ne semble pas que la connaissance des opérations élémentaires utilisées pour obtenir E à partir de I réduise beaucoup le temps de calcul de D. Et puisqu'il n'y a pas d'erreur d'arrondi en arithmétique binaire, la stabilité numérique importe peu dans l'inversion des matrices. Malgré son inutilité pratique, cet exemple sur des matrices est

tout à fait utile pour clarifier les relations requises dans un cryptosystème à clé publique.

Une approche plus pratique pour trouver une paire d'algorithmes inverses *E* et *D* faciles à calculer, telle que *D* soit difficile à inférer de *E*, utilise la difficulté d'analyser les programmes dans les langages de bas niveau. Quiconque a essayé de déterminer quelle opération est effectuée par un programme en langage machine écrit par quelqu'un d'autre sait que *E* lui-même (c'est-à-dire ce que fait *E*) peut être difficile à inférer à partir de l'algorithme pour *E*. Si le programme devait être écrit à dessein pour être confus, en ajoutant des variables et des instructions inutiles, alors, déterminer l'algorithme inverse pourrait être rendu très difficile. Bien sûr, *E* doit être assez compliqué pour empêcher son identification à partir d'une paire d'entrée-sortie.

Pour l'essentiel, ce qui est requis est un compilateur à sens unique, qui prend un programme facilement compréhensible, écrit avec un langage de haut niveau, et le traduit en un programme incompréhensible dans un quelconque langage machine. Le compilateur est à sens unique parce que la compilation doit être réalisable, mais il doit être irréalisable de renverser le processus. Puisque l'efficacité en taille de code et en temps de calcul n'est pas cruciale pour cette application, de tels compilateurs peuvent être imaginés dès lors que la structure du langage machine peut être optimisée pour aider à la confusion.

Indépendamment, Merkle[11] a étudié le problème de la distribution des clés sur un canal non sécurisé. Son approche est différente de celle des cryptosystèmes à clé publique suggérés ci-dessus, et sera nommée un *système de distribution publique de clés*. Le but, pour deux utilisateurs *A* et *B*, est d'échanger une clé en toute sécurité sur un canal non sécurisé. Cette clé est alors utilisée à la fois par les deux utilisateurs d'un cryptosystème normal, aussi bien pour chiffrer que pour déchiffrer. Merkle donne une solution dont le coût cryptanalytique croît en n^2, n étant le coût pour les utilisateurs légitimes. Malheureusement, le coût pour les utilisateurs légitimes du système provient autant du temps des transmissions que du temps de calcul, parce que le protocole de Merkle requiert que n clés potentielles soient transmises avant qu'une clé puisse être déterminée. Merkle remarque que ce fort surcoût de transmission empêche le système d'être très utile en pratique. Si on place une limite d'un mégabit pour le surcoût de l'initialisation du protocole, sa technique peut aboutir à des rapports de coût d'environ 10 000 à 1, qui sont trop faibles pour la plupart des applications. Si des liaisons peu chères, à bande passante élevée, deviennent accessibles, des rapports d'un million à 1 ou plus peuvent être obtenus et le système deviendrait d'une valeur pratique substantielle.

[11] Merkle, « Secure Communication over an Insecure Channel ».

Nous suggérons maintenant un nouveau système de distribution publique de clés, qui a plusieurs avantages. Tout d'abord, il ne requiert d'échanger qu'une seule « clé ». Deuxièmement, l'effort cryptanalytique tend à croître exponentiellement en fonction de l'effort des utilisateurs légitimes. Et troisièmement, son utilisation peut être liée à un fichier public d'informations de l'utilisateur, qui serve à authentifier l'utilisateur *A* par l'utilisateur *B*, et *vice-versa*. En considérant ce fichier public essentiellement comme une mémoire à lecture seule, une seule intervention personnelle permet à un utilisateur de rendre authentique son identité de nombreuses fois auprès de nombreux usagers. La technique de Merkle impose à *A* et *B* de vérifier les identités de chacun par d'autres moyens.

Cette nouvelle technique repose sur l'apparente difficulté de calculer les logarithmes sur le corps fini $GF(q)$ contenant un nombre q d'éléments. Soit :

$$Y = \alpha^X \bmod q, \quad \text{pour } 1 \leq X \leq q-1 \tag{4}$$

Ici, α est un élément primitif donné de $GF(q)$. Alors X est défini comme le logarithme de Y dans la base α mod q :

$$X = \log_\alpha Y \bmod q, \quad \text{pour } 1 \leq Y \leq q-1 \tag{5}$$

Calculer Y à partir de X est facile, et nécessite au plus $2 \times \log_2 q$ multiplications. Par exemple[12], pour $X = 18$,

$$Y = \alpha^{18} = (((\alpha^2)^2)^2)^2 \times \alpha^2 \tag{6}$$

Calculer X à partir de Y, en revanche, peut être beaucoup plus difficile, et, pour certaines valeurs soigneusement choisies de q, nécessiter un nombre d'opérations de l'ordre de $q^{1/2}$, en utilisant le meilleur algorithme connu[13].

La sécurité de notre technique dépend crucialement de la difficulté de calculer les logarithmes modulo q, et si on découvrait un algorithme dont la complexité croisse comme $\log_2 q$, alors on pourrait casser notre système. Alors que la simplicité de l'énoncé du problème peut donner de tels algorithmes simples, elle devrait plutôt suggérer une preuve de la difficulté du problème. Pour l'instant, nous supposons que le meilleur algorithme connu pour calculer les logarithmes modulo q est en fait proche de l'optimal, et donc que $q^{1/2}$ est une bonne mesure de la complexité du problème, pour une valeur bien choisie de q.

---

[12] Knuth, « The art of Computer Programming », vol. 2, pp. 398-422.

[13] Knuth, « The art of Computer Programming », vol. 3, pp. 9 et 575-576. Polhig et Hellman, « An Improved Algorithm for Computing Logarithms ».

Un tel utilisateur produit un nombre aléatoire indépendant X_i choisi uniformément dans l'ensemble des entiers {1, 2, ..., q}, qu'il garde secret, mais place :

(7) $$Y_i = \alpha^{X_i} \bmod q$$

dans un fichier public avec son nom et son adresse. Lorsque les utilisateurs i et j veulent communiquer en privé, ils utilisent :

(8) $$K_{ij} = \alpha^{X_i X_j} \bmod q$$

comme clé. L'utilisateur i obtient K_{ij} en se procurant Y_j dans le répertoire public, et pose

(9) $$K_{ij} = Y_j^{X_i} \bmod q$$

(10) $$= (\alpha^{X_j})^{X_i} \bmod q$$

(11) $$= \alpha^{X_j X_i} = \alpha^{X_i X_j} \bmod q$$

L'utilisateur j obtient K_{ij} de la même manière :

(12) $$K_{ij} = Y_i^{X_j} \bmod q$$

Un autre utilisateur doit calculer K_{ij} à partir de Y_i et Y_j, par exemple en calculant :

(13) $$K_{ij} = Y_i^{\log_\alpha Y_j} \bmod q$$

Nous voyons ainsi que si les logarithmes modulo q sont faciles à calculer, le système peut être cassé. Bien que nous n'ayons pas de preuve générale de la réciproque (c'est-à-dire que le système soit sûr si les logarithmes modulo q sont difficiles à calculer), nous ne voyons aucune manière de calculer K_{ij} à partir de Y_i et Y_j sans obtenir d'abord soit X_i soit X_j.

Si q est un nombre premier légèrement inférieur à 2^b, alors, toutes les quantités sont représentables comme des nombres de b chiffres binaires. L'exponentiation prend alors au plus $2b$ multiplications modulo q, tandis que par hypothèse, prendre les logarithmes requiert $q^{1/2} = 2^{1/2}$ opérations. L'effort cryptographique croît donc exponentiellement par rapport aux efforts légitimes. Si b = 200, alors, il faut au plus 400 multiplications pour calculer Y_i à partir de X_i, ou K_{ij} à partir de Y_i et de X_j, alors que prendre les logarithmes modulo q nécessite 2^{100} soit approximativement 10^{30} opérations.

AUTHENTIFICATION A SENS UNIQUE

Le problème de l'authentification est sans doute une barrière encore plus sérieuse que le problème de la distribution des clés afin que les télécommunications soient universellement adoptées dans les transactions d'affaires. L'authentification est au cœur de tous les systèmes impliquant des contrats et des facturations. Sans elle, les affaires ne peuvent pas fonctionner. Les systèmes usuels d'authentification électroniques ne peuvent pas satisfaire ce besoin d'une signature purement digitale, infalsifiable, et qui dépend du message. Ils fournissent une protection contre toute falsification par une tierce partie, mais ne protègent pas des contestations entre celui qui émet et celui qui reçoit.

Afin de développer un système susceptible de remplacer le contrat écrit usuel par quelque forme purement électronique de communication, il nous faut découvrir un phénomène digital qui ait les mêmes propriétés que la signature écrite. Il doit être facile à quiconque de reconnaître une signature comme authentique, mais elle doit être impossible à produire par toute autre personne que le signataire légitime. Nous appellerons une telle technique une *authentification à sens unique*. Puisqu'un signal numérique peut être copié avec précision, une véritable signature numérique doit être reconnaissable sans être connue.

Considérons le problème de la connexion à un système informatique multi-utilisateurs. Lorsqu'il initialise son compte, l'utilisateur choisit un mot de passe qui est entré dans le fichier des mots de passe du système. À chaque fois qu'il se connecte, il est encore demandé à l'utilisateur de saisir son mot de passe. En tenant le mot de passe secret pour tous les autres usagers, on se préserve d'entrées illicites. Mais il devient alors vital de préserver la sécurité du répertoire des mots de passe, puisque l'information qu'il contient permettrait une imposture totale sur toute connexion. Le problème devient encore plus complexe si des administrateurs du système ont des raisons légitimes d'accéder au répertoire. Permettre ces accès légitimes tout en interdisant les autres frise l'impossible.

Ceci conduit à l'exigence apparemment impossible de trouver une nouvelle procédure de connexion, capable de juger de l'authenticité des mots de passe sans les connaître effectivement. Bien que cette exigence puisse apparaître comme une impossibilité logique, elle est facile à satisfaire. Quand un utilisateur entre son mot de passe PW pour la première fois, l'ordinateur calcule automatiquement et en toute transparence une fonction $f(PW)$ qu'il stocke, plutôt que PW, dans le répertoire des mots de passe. À chaque connexion successive, l'ordinateur calcule $f(X)$, dès que X est présenté comme mot de passe, et compare $f(X)$ au $f(PW)$ enregistré en mémoire. L'utilisateur est accepté comme authentique si et seulement si ces deux valeurs sont égales. Puisque la fonction f doit être calculée une fois par

connexion, son temps de calcul doit être court. Un million d'instructions (ce qui coûte environ 0,10 $ à la valeur du bicentenaire US) semble une limite raisonnable pour ce calcul. Mais si on peut affirmer que le calcul de f^{-1} nécessite 10^{30} instructions ou plus, alors quiconque subvertirait le système pour obtenir le répertoire des mots de passe ne pourrait en pratique pas obtenir *PW* à partir de *f*(*PW*), et ne pourrait donc ainsi effectuer aucune connexion non autorisée. Remarquons que *f*(*PW*) ne serait pas accepté comme mot de passe par le programme de connexions, puisqu'il calculerait automatiquement *f*(*f*(*PW*)) qui ne correspond pas à l'entrée *f*(*PW*) du répertoire des mots de passe.

Nous supposons que la fonction *f* est connue publiquement, de telle sorte que ce n'est pas d'ignorer *f* qui rend difficile le calcul de f^{-1}. De telles fonctions sont appelées fonctions à sens unique, elles ont été utilisées pour la première fois dans les procédures de connexion par R. M. Needham[14]. Elles sont également étudiées dans deux articles récents[15], qui suggèrent des approches intéressantes pour concevoir des fonctions à sens unique.

Plus précisément une fonction *f* est *une fonction à sens unique*, si pour tout argument *x* du domaine de *f*, il est facile de calculer la valeur correspondante *f*(*x*), alors que, pour presque tous les *y* dans l'éventail des valeurs de *f*, il est calculatoirement impossible de résoudre l'équation pour obtenir un argument *x* qui convienne.

Il est important de remarquer que nous définissons une fonction qui n'est pas inversible du point de vue calculatoire, mais dont la non-inversibilité est tout à fait différente de ce qui est habituellement entendu en mathématiques. Une fonction *f* est normalement qualifiée de « non-inversible » lorsque l'inverse d'un élément *y* n'est pas unique (c'est-à-dire lorsqu'il existe des points distincts x_1 et x_2 tels que $f(x_1) = y = f(x_2)$). Nous insistons sur le fait que ce n'est pas ce type de difficulté à inverser qui est requis. C'est plutôt que la difficulté doit être insurmontable pour calculer un *x* quelconque ayant la propriété $y = f(x)$, à partir d'une valeur donnée de *y* et de la connaissance de *f*. Bien sûr, si *f* n'est pas inversible au sens usuel du terme, la tâche de trouver une image inverse peut devenir plus facile. Dans le cas extrême où pour tout *x* dans le domaine, $f(x) = y_0$, alors l'éventail des valeurs de *f* est $\{y_0\}$, et on peut prendre n'importe quel *x* pour $f^{-1}(y_0)$. Il est donc indispensable que *f* ne soit pas trop dégénérée. Un faible degré de dégénérescence est tolérable, et, comme on va le voir plus loin, cette situation existe sans doute dans une classe des plus prometteuses de fonctions à sens unique.

Les polynômes offrent un exemple élémentaire de fonctions à sens unique. Il est plus difficile de trouver une racine x_0 de l'équation

[14] Wilkes, « Time Sharing Computer Systems », p. 91.
[15] *ibid.*, et Purdy, « A High Security Log-in Procedure ».

polynômiale $p(x) = y$ que d'évaluer le polynôme $p(x)$ en $x = x_0$. Purdy[16] a suggéré d'utiliser des polynômes de très haut degré ayant peu de termes sur des corps finis, qui semblent donner des rapports très élevés entre le temps de calcul d'une racine et le temps de calcul d'une valeur. Le fondement théorique des fonctions à sens unique est discuté plus longuement dans le paragraphe « Complexité calculatoire ». Et comme on l'a montré dans le paragraphe « Interdépendance des problèmes et porte dérobée », les fonctions à sens unique sont faciles à inventer en pratique.

Le protocole de connexion utilisant des fonctions à sens unique ne résout que certains des problèmes qui surgissent dans un système multi-utilisateurs. Il protège contre la compromission des données d'authentification du système lorsqu'il n'est pas en fonction, mais il requiert encore que l'utilisateur envoie le vrai mot de passe au système. La protection contre l'interception du mot de passe doit être réalisée par un supplément de chiffrement, et on doit également assurer la protection contre toute menace de répudiation.

Un cryptosystème à clé publique peut être utilisé pour produire un véritable système d'authentification à sens unique de la manière suivante. Si un utilisateur *A* souhaite envoyer un message *M* à un utilisateur *B*, il le « déchiffre » grâce à sa clé secrète de déchiffrement et envoie $D_A(M)$. Lorsque l'utilisateur *B* le reçoit, il peut le lire, et être sûr de son authenticité en le « chiffrant » avec la clé publique de chiffrement E_A de l'utilisateur *A*. L'utilisateur *B* sauvegarde aussi $D_A(M)$ comme preuve que le message vient bien de *A*. N'importe qui peut contrôler cette affirmation en appliquant à $D_A(M)$ l'opération publiquement connue E_A pour retrouver *M*. Comme seul *A* a pu produire un message ayant cette propriété, la solution du problème de l'authentification à sens unique découle directement du développement des cryptosystèmes à clé publique.

Leslie Lamport, de la firme *Massachusetts Computer Associates*, a suggéré aux auteurs une solution partielle de l'authentification à sens unique. Sa technique utilise une fonction à sens unique *f* appliquant l'espace des vecteurs binaires de dimension *k* dans lui-même, pour une valeur de *k* de l'ordre de 100. Si l'envoyeur désire transmettre un message de *N* bits, il produit $2N$ vecteurs binaires de dimension *k*, choisis aléatoirement : $x_1, X_1, x_2, X_2, \ldots x_N, X_N$, qu'il garde secrets. Le récepteur reçoit les images correspondantes par *f*, à savoir $y_1, Y_1, y_2, Y_2, \ldots y_N, Y_N$. *E*, lorsque le message $m = (m_1, m_2, \ldots m_N)$ doit être envoyé, l'expéditeur envoie x_1 ou X_1 selon que $m_1 = 0$ ou 1. Il envoie x_2 ou X_2 selon que $m_2 = 0$ ou 1, *etc*. Le récepteur fait opérer *f* sur le 1er bloc reçu et examine s'il donne comme image y_1 ou Y_1 comme image. Il apprend ainsi s'il s'agissant de x_1 ou X_1 et si $m_1 = 0$ ou 1.

[16] Purdy, « A High Security Log-in Procedure ».

Le récepteur pourra déterminer m_2, m_3,…, m_N de la même manière. Mais celui-ci est incapable de changer le moindre bit de *m*.

Cette solution n'est que partielle du fait que le taux requis d'expansion des données est voisin de 100. Il existe cependant une modification qui élimine ce problème d'expansion lorsque *N* est de l'ordre du mégabit ou plus. Soit *g* une application à sens unique d'un espace binaire de dimension *N* dans un espace binaire de dimension *n*, où *n* est voisin de 50. Prenons un message *m* de *N* bits et faisons opérer *g* sur lui pour obtenir un vecteur *m'* de *n* bits. Utilisons alors le schéma précédent pour envoyer *m'*. Si $N = 10^6$, $n = 50$, et $k = 100$, alors cela ajoute $kn = 5000$ bits d'authentification au message. Cela n'entraine ainsi que 5 % d'expansion des données pendant la transmission (ou 15 % si on inclut l'échange initial y_1, Y_1, y_2, Y_2, … y_N, Y_N). Même lorsqu'il y a un grand nombre d'autres messages (2^{N-n} en moyenne) ayant la même séquence d'authentification, que *g* soit à sens unique rend calculatoirement impossible de trouver ces autres messages et donc de falsifier la séquence d'authentification. En fait, *g* doit être bien plus forte qu'une fonction à sens unique ordinaire, car un adversaire a accès non seulement à *m*, mais aussi aux différentes images inverses de *m'*. Il doit être difficile, même lorsque *m* est donné, de trouver une autre image inverse de *m'*. Trouver de telles fonctions semble présenter quelques difficultés (voir le paragraphe « Interdépendance des problèmes et portes dérobées »).

Il existe une autre solution partielle au problème de l'authentification à sens unique des utilisateurs. L'utilisateur produit un mot de passe *X* qu'il garde secret. Il donne au système $f^T(X)$, où *f* est une fonction à sens unique. À l'instant *t*, la donnée d'authentification appropriée est $f^{T-t}(X)$, qui peut être vérifiée par le système en appliquant $f^t(X)$. Du fait que *f* est une fonction à sens unique, les anciennes réponses ne sont d'aucune utilité pour en forger une nouvelle. Le problème avec cette solution, c'est qu'elle peut requérir un nombre confortable de calculs pour garantir une connexion légitime (bien qu'il soit d'un ordre de grandeur bien moindre que pour la falsification). Si par exemple *t* augmente d'une unité par seconde et si le système doit travailler un mois, alors pour chaque mot de passe, $T = 2{,}6$ millions. L'utilisateur et le système doivent alors tous deux itérer *f* 1,3 million de fois en moyenne pour chaque connexion. Si ce problème n'est pas insurmontable, il limite évidemment l'utilisation de cette technique. Ce problème peut être surmonté si on peut trouver une méthode simple pour calculer f^{2^n} pour $n = 1, 2,...$, comme pour $X^8 = ((X^2)^2)^2$. Car dans ce cas, les décompositions binaires de *T* et *t* permettraient de calculer rapidement f^{T-t} et f^t. Il se peut cependant que ce calcul rapide de f^n empêche la fonction *f* d'être à sens unique.

INTERDEPENDANCE DES PROBLEMES ET PORTES DEROBEES

Dans ce paragraphe, nous montrerons que certains des problèmes cryptographiques présentés jusqu'ici peuvent être réduits à d'autres, définissant ainsi une sorte d'ordre dans les difficultés. Nous introduirons aussi le problème plus difficile des « portes dérobées ».

Dans le paragraphe « Cryptographie conventionnelle », nous avons montré qu'un système cryptographique conçu pour la confidentialité peut aussi être utilisé pour fournir une authentification contre les falsifications par une tierce partie. Un tel système peut aussi bien être utilisé pour créer d'autres objets cryptographiques.

Un cryptosystème sûr contre une attaque à clair connu peut être utilisé pour produire une fonction à sens unique.

Comme indiqué fig. 3, prenons un cyptosystème $S_K : \{P\} \rightarrow \{C\}_{K \in \{K\}}$, qui est sûr contre une attaque à clair connu, et $P = P_0$ fixé, et considérons l'application :

(14) $$f : \{K\} \rightarrow \{C\}$$

définie par :

(15) $$f(X) = S_X(P_0)$$

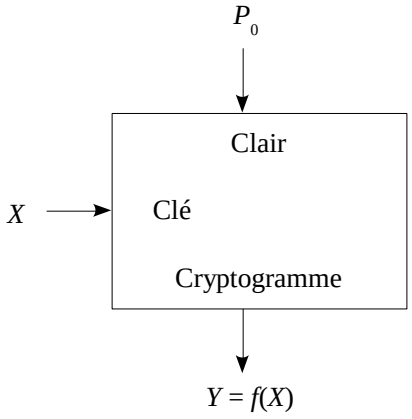


Fig. 3. Cryptosystème sûr utilisé comme fonction à sens unique.

Cette fonction est à sens unique, parce que trouver X, pour $f(X)$ donné, équivaut au problème de cryptanalyse qui consiste à retrouver la clé à partir

d'une seule paire clair-cryptogramme connue. La connaissance publique de f équivaut ici à la connaissance publique de $\{S_K\}$ et de P_0.

Alors que la réciproque de ce résultat n'est pas nécessairement vraie, il est possible qu'une fonction trouvée à l'origine en cherchant des fonctions à sens unique, donne un bon cryptosystème. Ceci est effectivement le cas pour la fonction exponentielle discrète discutée dans le paragraphe « Cryptographie à clé publique »[17].

Les fonctions à sens unique sont fondamentales à la fois pour les chiffrements par blocs et pour les générateurs de clé. Un générateur de clé est un générateur pseudo-aléatoire de bits dont la sortie, le flot de clé, est additionné modulo 2 au message représenté sous forme binaire, imitant ainsi le système de masque jetable. La clé est utilisée comme un « germe » qui détermine la séquence pseudo-aléatoire. Une attaque à clair connu se réduit ainsi au problème de déterminer la clé à partir du flot de clé. Afin que le système soit sûr, le calcul de la clé à partir du flot de clé doit être calculatoirement irréalisable. Ceci dit, pour que le système soit utilisable, le calcul du flot de clé à partir de la clé doit être simple. Un bon générateur de clé est pour ainsi dire par définition, une fonction à sens unique.

L'utilisation de l'un quelconque de ces types de cryptosystèmes en tant que fonction à sens unique souffre d'un problème mineur. Comme nous l'avons vu précédemment, si la fonction f n'est pas inversible de manière unique, il n'est ni nécessaire ni possible de trouver la valeur de X effectivement utilisée. Ou plutôt, tout X ayant la même image conviendrait. Et, alors que dans un cryptosystème, chaque application S_K doit être bijective, il n'y a pas une telle restriction pour la fonction f qui, à la clé, associe le cryptogramme, comme on l'a défini ci-dessus. Bien sûr, garantir qu'un cryptosystème ait cette propriété paraît tout à fait difficile. Dans un bon cryptosystème, il est attendu que l'application f possède les caractéristiques d'une application choisie aléatoirement (c'est-à-dire que $f(X_i)$ soit choisie uniformément parmi tous les Y_i possibles, et que les choix successifs soient indépendants). Dans ce cas, si X est choisi uniformément et s'il y a un nombre égal de clés et de messages (X et Y), alors la probabilité pour que le Y résultant ait $k + 1$ inverses vaut approximativement $e^{-1}/k!$, pour $k = 0, 1, 2, 3, \ldots$. Il s'agit d'une distribution de Poisson de moyenne $\lambda = 1$, décalée d'une unité. Le nombre moyen d'inverses ne vaut que 2. Alors qu'il est possible que f soit encore plus dégénérée, un bon cryptosystème ne doit pas l'être trop, puisqu'alors la clé ne serait pas bien utilisée. Dans le pire des cas, si $f(X) \equiv Y_0$ pour certains Y_0, nous aurions $S_K(P_0) \equiv C_0$, et le chiffrement de P_0 ne dépendrait pas du tout de la clé !

[17] Polhig et Hellman, « An Improved Algorithm for Computing Logarithms in GF(p), and its Cryptographic Significance ».

Alors que les fonctions qui nous intéressent d'habitude sont celles dont les ensembles de départ et d'arrivée sont de taille comparable, il y a des exceptions. Dans le paragraphe précédent, nous avons exigé que les applications à sens unique transforment de longues chaînes en des chaînes bien plus courtes. En utilisant un chiffrement par blocs dont la longueur de la clé est plus grande que la taille des blocs du chiffrement, de telles fonctions peuvent être obtenues en utilisant la technique ci-dessus.

Evans et *al.*[18] ont une approche différente du problème, consistant à construire une fonction à sens unique à partir d'un chiffrement par blocs. Au lieu de sélectionner un P_0 fixé comme entrée, ils utilisent la fonction :

(16) $$f(X) = S_X(X)$$

C'est une approche séduisante car les équations de cette forme sont en général difficiles à résoudre, même lorsque la famille *S* est relativement simple. Quoi qu'il en soit, cette complexité supplémentaire détruit l'équivalence entre la résistance du système *S* face à une attaque à clair connu et la propriété de *f* d'être une fonction à sens unique.

Une autre relation a déjà été établie au paragraphe « Authentification à sens unique » :

Un cryptosystème à clé publique peut être utilisé pour réaliser un système d'authentification à sens unique.

La réciproque ne semble pas être satisfaite, ce qui fait de la construction d'un cryptosystème à clé publique un problème strictement plus difficile qu'une authentification à sens unique. Ici encore, un cryptosystème à clé publique peut être utilisé comme un système de distribution publique de clés, mais pas l'inverse.

Puisque dans un cryptosystème à clé publique, le système général qui utilise *E* et *D* doit être public, spécifier *E* spécifie un algorithme complet qui transforme les entrées de messages en sorties de cryptogrammes. Comme tel, un système à clé publique est véritablement un ensemble de *fonctions à sens unique à porte dérobée*. Ce sont des fonctions qui ne sont pas tout à fait à sens unique, en ce sens qu'il existe des inverses de ces fonctions simples à calculer. Mais, étant donné un algorithme pour la fonction dans le sens direct, il est calculatoirement irréalisable de trouver une fonction inverse simple à calculer. C'est seulement par la connaissance d'une certaine information sur la « porte dérobée » (c'est-à-dire la chaîne de bits aléatoires qui produit le couple *E*–*D*) qu'on peut facilement calculer l'inverse.

[18] Evans Kantrowitz et Weiss, « A User Authentication System not requiring Secrecy in a Computer ».

Les *portes dérobées* viennent d'être abordées dans le paragraphe précédent sous la forme de *fonctions à sens unique à porte dérobée*, mais il en existe d'autres variantes. Un *chiffrement à porte dérobée* est un chiffre qui peut résister fortement à la cryptanalyse par quiconque n'est pas en possession de *l'information sur la porte dérobée* utilisée lors de la conception du chiffre. Ceci permet à un concepteur de casser le système après l'avoir vendu à un client, et cependant, de maintenir sa réputation en tant que concepteur de systèmes sûrs. Il est important de remarquer que ce n'est pas une plus grande habileté ni une expertise en cryptographie qui permet au concepteur de faire ce que d'autres ne peuvent pas. S'il perdait l'information sur la porte dérobée, il ne serait pas meilleur qu'un autre. La situation est précisément analogue à celle d'une serrure à combinaisons. Quiconque connaît la combinaison peut faire en quelques secondes ce que même un habile serrurier n'accomplirait qu'en plusieurs heures. Et cependant, s'il oublie la combinaison, il n'aura plus aucun avantage.

Un cryptosystème à porte dérobée peut être utilisé pour produire un système de distribution publique de clés.

Pour que deux utilisateurs *A* et *B* établissent une clé privée commune, il suffit de choisir une clé aléatoire, et d'envoyer une paire arbitraire clair-chiffré à *B*. L'utilisateur *B* qui a réalisé le chiffrement public à porte dérobée, mais qui en garde secrète l'information, utilise la paire clair-chiffré pour retrouver la clé. Les utilisateurs *A* et *B* partagent maintenant une clé en commun.

Il y a actuellement peu de preuve de l'existence de chiffrement à porte dérobée. Cependant, il existe une autre possibilité qui ne doit pas être oubliée lorsqu'on accepte un cryptosystème d'un possible adversaire[19].

Par définition, on demande à un problème avec porte dérobée qu'il soit calculatoirement réalisable de concevoir cette porte dérobée. Cette exigence laisse place cependant à un troisième type d'entité pour laquelle nous utiliserons le préfixe « quasi ». Par exemple, une *fonction quasi à sens unique* n'est pas à sens unique dans la mesure où il existe un inverse facile à calculer. Pourtant, il est calculatoirement irréalisable, même pour le concepteur, de trouver cet inverse facile à calculer. Ainsi une fonction quasi à sens unique peut être utilisée à la place d'une fonction à sens unique pratiquement sans perte de sécurité.

Perdre l'information sur la porte dérobée d'une fonction à sens unique à porte dérobée en fait une fonction quasi à sens unique, mais il peut aussi y avoir des fonctions à sens unique qui ne peuvent être obtenues de cette manière.

---

[19] Diffie et Hellman, « Cryptanalysis of the NBS Data Encryption Standard ».

Que les fonctions quasi à sens unique soient exclues de la classe des fonctions à sens unique n'est vraiment qu'une question de définition. On pourrait tout aussi bien parler de fonction à sens unique au sens large ou au sens strict.

De la même manière, un chiffrement quasi sûr est un chiffrement qui doit complétement résister à la cryptanalyse, y compris par son concepteur, et pour lequel il existe pourtant un algorithme de cryptanalyse efficace (qui est bien sûr calculatoirement impossible à trouver). À nouveau, d'un point de vue pratique, il n'y a au fond aucune différence entre un chiffrement sûr et un chiffrement quasi sûr.

Nous avons déjà vu que les cryptosystèmes à clé publique impliquent l'existence de fonctions à sens unique à porte dérobée. Cependant la réciproque n'est pas vraie. Pour qu'une fonction à sens unique à porte dérobée soit utilisable comme cryptosystème à clé publique, elle doit être inversible (c'est-à-dire avoir un inverse unique).

COMPLEXITE CALCULATOIRE

La cryptographie diffère de tous les autres champs d'activité, par la facilité avec laquelle ses exigences peuvent sembler être satisfaites. Des transformations simples convertiront un texte lisible en un méli-mélo sans signification apparente. Le critique, qui veut affirmer que la signification pourrait toujours être reconstituée par la cryptanalyse, se trouve face à une démonstration ardue s'il veut prouver que son point de vue est correct. L'expérience a montré cependant que peu de systèmes peuvent résister à l'attaque concertée de cryptanalystes adroits, et de nombreux systèmes, supposés sûrs, ont finalement été cassés.

En conséquence, juger de la valeur d'un nouveau système a toujours été une question centrale pour les cryptographes. Au cours des seizième et dix-septième siècles, des arguments mathématiques ont souvent été invoqués pour arguer de la force des procédés cryptographiques qui s'appuyaient en général sur des méthodes de dénombrement montrant le nombre astronomique de clés possibles. Bien que ce problème soit bien trop difficile pour le laisser reposer sur des méthodes si simples, même le célèbre algébriste Cardan est tombé dans ce piège[20]. Puisque des systèmes dont la force avait été ainsi défendue ont régulièrement été cassés, l'idée de donner une preuve mathématique pour la sécurité des systèmes s'est trouvée disqualifiée et remplacée par la certification *via* des assauts cryptanalytiques.

[20] Kahn, *The Codebreakers*, p. 145.

Au cours de ce siècle cependant, le pendule a commencé à balancer dans l'autre direction. Dans un article étroitement lié à la naissance de la théorie de l'information, Shannon a montré que le système du masque jetable (*one-time pad*) qui avait été utilisé depuis la fin des années vingt, offrait une « sécurité parfaite » (un *summum* de sécurité inconditionnelle). Les systèmes prouvés sûrs étudiés par Shannon reposent sur l'utilisation d'une clé dont la longueur croît linéairement avec la longueur du message, ou sur une source parfaite de codage, et sont donc trop lourds pour la plupart des usages. Remarquons que ni les systèmes à clé publique, ni les systèmes d'authentification à sens unique ne peuvent être inconditionnellement sûrs, car l'information publique détermine toujours l'information secrète de manière unique au sein d'un ensemble fini. Avec une capacité de calcul illimitée, le problème pourrait donc être résolu par une recherche exhaustive.

La dernière décennie a donné naissance à deux disciplines étroitement liées consacrées à l'étude des coûts de calcul : la théorie de la complexité et l'analyse des algorithmes. La première a classé les problèmes algorithmiques connus par ordre de difficultés, tandis que la seconde s'est attachée à trouver de meilleurs algorithmes et à étudier les ressources qu'ils consomment. Après une brève discussion sur la théorie de la complexité, nous allons examiner son application à la cryptographie, en particulier à l'analyse des fonctions à sens unique.

On dit qu'une fonction appartient à la classe ***P*** (pour *Polynomial*) si elle peut être calculée par une machine de Turing déterministe en un temps qui peut être majoré par une certaine fonction polynomiale de la longueur de son entrée. On peut la penser comme la classe des fonctions qui peuvent être facilement calculées, mais il est plus précis de dire qu'une fonction qui n'appartient pas à cette classe doit être difficile à calculer, au moins pour certaines entrées. Il y a des problèmes qui sont connus[21] pour ne pas appartenir à la classe ***P***.

Il existe beaucoup de problèmes qui se présentent en ingénierie et qui ne peuvent être résolus en temps polynomial par aucun procédé connu, sauf à les exécuter sur un ordinateur doté d'un degré illimité de parallélisme. Ces problèmes peuvent ou non appartenir à la classe ***P***, mais ils appartiennent à la classe ***NP*** (pour *Nondeterministic Polynomial*) des problèmes qui peuvent être résolus en temps polynomial sur un ordinateur « non déterministe » (c'est-à-dire avec un degré illimité de parallélisme). Il est clair que la classe ***NP*** contient la classe ***P***, et une des grandes questions ouvertes de la théorie de la complexité est de savoir si la classe ***NP*** est strictement plus grande que la classe ***P***.

[21] Aho, Hopcroft et Ullman, *The Design and Analysis of Computer Algorithms*, pp. 405-425.

Parmi les problèmes qui sont connus pour être résolubles en temps ***NP***, mais non connus pour être résolubles en temps ***P***, il y a des versions du problème du voyageur de commerce, le problème de satisfiabilité en calcul propositionnel, le problème du sac à dos, le problème du coloriage des graphes et de nombreux problèmes d'ordonnancement ou d'optimisation[22]. Nous observons que ce n'est pas le manque d'intérêt ni d'effort qui a empêché de trouver des solutions en temps ***P*** pour ces problèmes. Il est fortement admis qu'au moins un de ces problèmes n'est pas dans la classe ***P***, et donc que la classe ***NP*** est strictement plus grande.

Karp a identifié une sous-classe des problèmes ***NP***, appelés ***NP*** complets, avec la propriété que si l'un d'entre eux appartient à la classe ***P***, alors tous les problèmes ***NP*** sont dans ***P***. Karp a dressé une liste de 21 problèmes qui sont ***NP*** complets, dont les problèmes mentionnés ci-dessus[23].

Bien que les problèmes ***NP*** complets soient prometteurs à des fins cryptographiques, la façon dont on comprend ordinairement leur difficulté n'inclut que l'analyse du pire des cas. Pour l'utilisation en cryptographie, c'est le coût de calcul typique qui doit être pris en compte. Si toutefois on remplace le temps de calcul dans le pire des cas par le temps de calcul moyen ou typique comme mesure de complexité, alors les preuves actuelles d'équivalence des problèmes ***NP*** complets ne sont plus valides. Cela suggère d'intéressants sujets de recherche. L'ensemble et les concepts typiques familiers aux théoriciens de l'information ont un rôle évident à jouer.

Nous pouvons maintenant déterminer la position du problème général de la cryptanalyse parmi les problèmes calculatoires.

*La cryptanalyse d'un système dont les opérations de chiffrement et de déchiffrement s'effectuent en temps **P** ne peut pas être plus difficile que **NP**.*

Pour le voir, il suffit d'observer que tout problème de cryptanalyse peut être résolu en trouvant une clé, un antécédent, *etc*., choisis dans un ensemble fini. Choisissons la clé de façon non déterministe et vérifions en temps ***P*** s'il s'agit de la bonne. S'il y a *M* clés entre lesquelles choisir, on doit utiliser un parallélisme à *M* couches. Par exemple dans une attaque à clair connu, le clair est chiffré simultanément avec chaque clé et comparée avec le cryptogramme. Puisque, par hypothèse, le chiffrement ne prend qu'un temps ***P***, alors la cryptanalyse ne prend qu'un temps ***NP***.

Nous observons également que le problème général de la cryptanalyse est ***NP*** complet. Cela résulte de la souplesse de notre définition des problèmes cryptographiques. Nous discuterons plus loin d'une fonction à sens unique ayant un inverse ***NP*** complet.

---

[22] *ibid.*, p. 363-414. Karp « Reducibility among Combinatorial Problems ».
[23] Karp « Reducibility among Combinatorial Problems ».

La cryptographie peut se décliner directement à partir de la théorie de la complexité ***NP***, en examinant la manière dont les problèmes ***NP*** complets peuvent être adaptés à un usage cryptographique. En particulier, il existe un problème ***NP*** complet, appelé problème du sac à dos, qui se prête bien à la construction de fonctions à sens unique.

Soit à partir de $y = f(x) = a \cdot x$, où a est un vecteur connu de n entiers $(a_1, a_2, ..., a_n)$ et x un vecteur binaire de dimension n. Le calcul de y est simple, il fait appel à une somme d'au plus n entiers. Le problème de l'inversion de f est connu sous le nom de problème du sac à dos, il nécessite de trouver un sous-ensemble des $\{a_i\}$ dont la somme est y.

La recherche exhaustive des 2^n sous-ensembles croît exponentiellement et est calculatoirement irréalisable lorsque n est environ d'ordre supérieur à 100. Il faut cependant être attentif au choix des paramètres du problème pour s'assurer qu'aucun court-circuit n'est possible. Par exemple, si $n = 100$ et que chaque a_i a une taille de 32 *bits*, alors y a au plus une taille de 39 bits et f est fortement dégénérée, ne nécessitant que 2^{38} essais en moyenne pour trouver une solution. De manière encore plus triviale, si $a_i = 2^{i-1}$, alors inverser f revient à trouver la décomposition binaire de y.

Cet exemple montre à la fois le côté prometteur et l'insuffisance considérable de la théorie de la complexité contemporaine. La théorie nous affirme seulement que le problème du sac à dos est probablement difficile dans le pire des cas. Elle ne donne aucune indication sur sa difficulté pour un vecteur particulier. Il apparaît cependant que choisir les a_i uniformément dans $\{0, 1, 2, \ldots, 2^{n-1}\}$ conduit à un problème difficile avec probabilité 1 lorsque $n \to \infty$.

Potentiellement, une autre fonction à sens unique intéressante dans l'analyse d'algorithmes est l'exponentiation modulo q, qui a été suggérée aux auteurs par le professeur John Gill de l'université de Standford. Le caractère à sens unique de cette fonction a déjà été discuté dans le paragraphe « Cryptographie à clé publique ».

PERSPECTIVE HISTORIQUE

Bien qu'à première vue, les systèmes à clé publique et les systèmes d'authentification à sens unique suggérés dans cet article paraissent ne pas être dans la lignée des développements cryptographiques antérieurs, il est possible de les envisager comme une suite naturelle de tendances de la cryptographie qui remontent à plusieurs siècles.

Le secret est au cœur de la cryptographie. Pourtant, au début de la cryptographie, il y avait un flou à propos de ce qui devait être gardé secret. Les cryptosystèmes tels que le chiffre de César (où chaque lettre est

remplacée par celle située trois places plus loin, *A* devenant ainsi *D*, *B* devenant *E*, *etc*.) dépendaient, pour leur sécurité, du fait que tout le processus de chiffrement soit gardé secret. Après l'invention du télégraphe[24], la distinction entre un système général et une clé spécifique a permis que le système général puisse être compromis, par exemple par le vol d'un appareil cryptographique, sans que les futurs messages chiffrés avec de nouvelles clés ne le soient. Ce principe a été codifié par Kerckhoffs[25], qui a écrit en 1881 que compromettre un système cryptographique ne devrait entraîner aucun inconvénient pour les correspondants[26]. Autour des années 1960, des cryptosystèmes furent mis en service, estimés assez solides pour résister à une attaque cryptanalytique à clair connu, éliminant ainsi l'inconvénient de garder secrets les anciens messages. Chacun de ces développements a fait décroître la portion du système qui devait être préservée de la connaissance publique, en éliminant les expédients laborieux tels que la paraphrase des dépêches diplomatiques avant qu'elles ne soient présentées. Les systèmes à clé publique sont dans le prolongement naturel de cette tendance vers la diminution de la sphère secrète.

Avant ce siècle, les systèmes cryptographiques se limitaient à des calculs qui pouvaient être effectués à la main, ou avec des instruments aussi simples qu'une règle à calcul. La période qui a immédiatement suivi la Première Guerre Mondiale a vu le début d'une tendance révolutionnaire qui atteint aujourd'hui son aboutissement. Des machines spécialisées ont été élaborées pour le chiffrement. Toutefois, jusqu'au développement des machines digitales universelles, la cryptographie se limitait aux opérations qui pouvaient s'effectuer sur des systèmes électromécaniques simples. Le développement des calculateurs numériques l'a libérée des limitations du calcul réalisé avec des engrenages et a permis la recherche de meilleures méthodes de chiffrement, fondées sur des critères purement cryptographiques.

L'échec des nombreuses tentatives pour démontrer la résistance des systèmes cryptographiques par des preuves mathématiques a conduit au paradigme de certification par attaque cryptanalytique établi par Kerckhoffs au siècle dernier[27]. Bien que certaines règles aient été développées, qui aident le concepteur à éviter des faiblesses évidentes, le test ultime est l'assaut par des cryptanalystes habiles sous les conditions les plus favorables (par exemple l'attaque à clair choisi). Le développement des ordinateurs a conduit pour la première fois à une théorie mathématique des algorithmes qui permet de commencer à aborder le difficile problème de

[24] Kahn, *The Codebreakers*, p. 191.
[25] *ibid.*, p. 235.
[26] NdT. : le texte de Kerckhoffs est de 1883. Voir pp. 118-123.
[27] *ibid.*, p. 234.

l'estimation de la difficulté calculatoire pour casser un système cryptographique. La preuve mathématique ainsi posée permet de refermer la boucle et se trouve restaurée comme meilleure méthode de certification.

La dernière caractéristique que nous remarquons dans l'histoire de la cryptographie est la séparation entre les cryptographes amateurs et professionnels. L'habileté à produire des cryptanalyses a toujours été fortement ancrée du côté des professionnels, mais l'innovation, en particulier dans la conception de nouveaux types de systèmes cryptographiques, est venue d'abord des amateurs. Thomas Jefferson, un cryptographe amateur, a inventé un système qui était encore en usage pendant la Seconde Guerre Mondiale[28], tandis que le plus remarquable des systèmes cryptographiques du vingtième siècle, la machine à rotors, a été inventée simultanément et séparément par quatre personnes, toutes amateurs[29]. Nous espérons que ceci inspirera d'autres travaux sur ce fascinant sujet où la participation a été découragée dans le passé récent par un monopole gouvernemental presque total.

BIBLIOGRAPHIE

Aho, A. V., Hopcroft, J. E. et Ullman, J. D., *The Design and Analysis of Computer Algorithms*, Reading, MA, Addison-Wesley, 1974.

Diffie, W. et Hellman, M. E., « Cryptanalysis of the NBS Data Encryption Standard », soumis à *Computers*, Mai 1976. [NdT. : paru en juin 1977, vol. 10, n° 6, pp. 74-84.]

— « Multiuser Cryptographic Techniques », présenté à *National Computer Conference*, New York, 7-10 Juin 1976.

Evans Jr, A., Kantrowitz, W. et Weiss, E., « A User Authentication System not Requiring Secrecy in a Computer », *Communication of the Association for Computing Machinery (ACM)*, Août 1974, vol. 17, pp 437-442.

Hellman, M. E., « An Extension of the Shannon Theory Approach to Cryptography », soumis à *IEEE Transactions on Information Theory*, Sept 1975. [NdT: paru en mau 1977, vol. 23, n° 3, pp. 289-295.]

Kahn, D., *The Codebreakers, the Story of Secret Writing*, New York, Macmillan, 1967.

Karp, R. M., « Reducibility among Combinatorial Problems », *in* (eds.) R. F. Miller et J.W. Thatcher, *Complexity of Computer Computations*, New York Plenum, 1972, pp 85-104.

[28] *ibid.*, pp. 192-195.
[29] *ibid.*, pp. 415, 420, 422-424.

Knuth, D., *The art of Computer Programming*, vol. 2 : *Seminumerical Algorithms*, Reading (Mass.), Addison-Wesley, 1969.

— *The art of Computer Programming*, vol. 3 : *Sorting and serarching*, Reading (Mass.), Addison-Wesley, 1973.

Merkle, R., « Secure Communication over an Insecure Channel », soumis à *Communication of the ACM*. [NdT. : paru en avril 1978, vol. 21, n° 4, pp. 294-199, sous le titre « Secure Communications over Insecure Channels ».

Polhig S. et Hellman, M. E., « An Improved Algorithm for Computing Logarithms in GF(*p*), and its Cryptographic Significance », soumis à *IEEE Transactions on Information Theory*. [NdT. : paru en janvier 1978, vol. 24, n° 1, pp. 106-110.]

Purdy, G. B., « A High Security Log-in Procedure », *Communication of the ACM*, Août 1974, vol. 17, pp. 442-445.

Shannon, C. E., « Communication Theory of Secrecy Systems », *Bell Systems Technical Journal*, octobre 1949, vol. 28, pp. 656-715.

Wilkes, M. V., *Time Sharing Computer Systems*, New York, Elsevier, 1972.

POURQUOI ET COMMENT LA CRYPTOLOGIE VIENT DE SURGIR DANS LE DOMAINE PUBLIC ? ROLE DE LA CARTE A PUCE

Louis GUILLOU[1]

Longtemps réservée aux domaines diplomatique et militaire, la cryptologie envahit désormais notre quotidien. Au cours de ma carrière de chercheur, je me suis souvent trouvé au bon endroit au bon moment pour observer et parfois participer aux développements de la carte à puce et de la cryptologie, deux technologies très liées l'une à l'autre. J'explique pourquoi c'est durant ces quarante dernières années (et pas avant) que la cryptologie apparaît dans le domaine public. J'aborde aussi la saga de la carte à puce en insistant sur les interférences avec la cryptologie.

LA CRYPTOLOGIE DURANT LA SECONDE GUERRE MONDIALE

Durant la Seconde Guerre Mondiale, quelques êtres exceptionnels croisent la cryptologie ; cette rencontre est particulièrement féconde pour deux d'entre eux : Shannon aux États-Unis et Turing au Royaume-Uni.

Claude E. Shannon et la théorie de l'information

De 1942 à 1945 aux États-Unis, Claude E. Shannon (1916-2001)[2] analyse les systèmes secrets et généralise ses réflexions aux systèmes de communication, créant ainsi la théorie de l'information. Après la guerre, le *Bell System Technical Journal* publie ses deux articles majeurs : « A Mathematical Theory of Communication » en 1948 et « Communication

[1] Expert émérite, Division Recherche et Développement de France Telecom (FTR&D).
[2] Voir le chapitre « Du message chiffré au système cryptographique » pp. 129-142 et le chapitre « La cryptologie gouvernementale française » p. 164.

Theory of Secrecy Systems » en 1949. Mais pour ces articles, la chronologie de publication est à mon avis l'inverse de la chronologie de gestation[3].

Dans une opération de chiffrement, Shannon formalise l'usage d'une clé tirée au hasard pour masquer la signification d'un message au cours de sa transmission. Un ennemi interceptant un chiffré – ou cryptogramme – peut tenter de rétablir la clé – et le clair – grâce à la redondance naturelle du langage utilisé par l'émetteur.

Dans une opération de codage, Shannon formalise l'usage d'une redondance artificielle pour détecter, voire éliminer, le bruit introduit au hasard dans un message au cours de sa transmission.

Dans les deux cas, l'expéditeur cherche à protéger la signification du message qu'il transmet bien que les menaces soient différentes. Hasard et redondance s'affrontent. Tout système secret comporte une opération de chiffrement pratiquée par la source afin de transformer le clair en chiffré et une opération de déchiffrement pratiquée par le destinataire pour rétablir le clair. Chaque opération se décrit par un chiffre – ou algorithme – contrôlé par une clé. L'analyse des systèmes secrets conduit Shannon à définir trois espaces : l'espace des clairs, l'espace des clés et l'espace des chiffrés.

Attention aux faux amis dans le vocabulaire de la cryptologie

En français

« Chiffrer » : transformer un clair en chiffré en utilisant une clé de chiffrement.

« Déchiffrer » : restituer le clair à partir du chiffré et de la clé secrète de déchiffrement.

« Décrypter » : retrouver le clair sans connaître *a priori* la clé secrète de déchiffrement, c'est-à-dire casser le code.

En anglais

« *To encipher, to encrypt* »: chiffrer.

« *To decipher, to decrypt* »: déchiffrer.

Pour « décrypter », il faut utiliser une périphrase : « *to break the code* ».

Le verbe français « déchiffrer » est équivalent aux verbes anglais « *to decrypt, to decipher* », eux-mêmes équivalents entre eux ; « chiffrer » est équivalent à « *to encrypt, to encipher* », eux-mêmes équivalents entre eux. Par contre, les verbes français « déchiffrer » et « décrypter » ont des sens très différents : « déchiffrer » consiste à rétablir le clair en utilisant la clé secrète de déchiffrement, alors que « décrypter » consiste à rétablir le clair sans connaître *a priori* la dite clé, c'est-à-dire « casser le code ». Il s'en suit que les Anglo-saxons doivent traduire le verbe français « décrypter » par la

[3] Voir le chapitre « Du message chiffré au système cryptographique » pp. 129-142.

périphrase : « *to break the code* ». Le verbe français « décrypter » n'ayant pas d'inverse, « crypter » est un barbarisme à proscrire absolument.

La sécurité « inconditionnelle » au sens de Shannon

Précisons la menace : l'ennemi peut intercepter des chiffrés et tenter de les interpréter. On considère qu'il sait quel chiffre et quel langage utilise la source. S'il connaît aussi la clé de déchiffrement, il n'a aucun problème pour rétablir les clairs. Mais que se passe-t-il s'il ne la connaît pas ?

Shannon dit qu'un chiffre donné est « inconditionnellement sûr » lorsque pour chaque chiffré et chaque clair, il existe au moins une clé pour les relier. N'ayant aucune idée particulière sur la clé en usage, car toutes les clés sont également probables, l'ennemi ne peut décider quel est le clair transmis. L'information *a posteriori*, c'est-à-dire après interception du chiffré, est la même que l'information *a priori*, c'est-à-dire avant l'interception. Alors la clé masque totalement le clair ; les statistiques et les règles de constitution du langage ne sont d'aucun secours pour décrypter.

La clé aléatoire utilisée une seule fois est un bon exemple de chiffre inconditionnellement sûr : aussi longue que le clair, la clé est une séquence de bits pris au hasard. Par ou-exclusif, chaque bit de clé est combiné à un bit du clair pour fournir le bit correspondant du chiffré. La même opération permet au destinataire de rétablir le clair. Mais bien rares sont les cas où l'on se permet des clés aussi volumineuses que les messages à transmettre[4].

Shannon et le facteur de travail : la complexité de décryptement

En pratique dans la plupart des chiffres, la même clé est utilisée pour protéger un grand nombre de messages durant un certain temps appelé la « crypto-période ». Pour chaque chiffré intercepté, on peut donc en principe essayer toutes les clés, l'une après l'autre, et déclarer qu'une clé est probable lorsque le résultat est intelligible, c'est-à-dire qu'il satisfait aux règles du langage de la source. Ainsi au fur et à mesure qu'augmente le volume de chiffrés gouvernés par la même clé, l'ensemble des clés probables s'amenuise jusqu'à atteindre le « point d'unicité » lorsque la redondance naturelle du langage est égale à l'entropie de la source des clés. Au-delà du point d'unicité, il n'y a plus qu'une seule solution en clé et donc en clair.

[4] *ibid.*, pp. 127-129.

Pour la plupart des chiffres, la sécurité repose sur ce que Shannon appelle le « facteur de travail », aujourd'hui appelé la « complexité de calcul » ou plutôt en français, la « complexité de décryptement ».

Bien sûr, le décrypteur recherche des raccourcis pour atteindre la solution avec un minimum d'efforts. L'art de la cryptanalyse consiste à définir des stratégies réduisant le nombre d'essais de clés. L'art de la cryptographie consiste à spécifier des chiffres tels que la seule solution pour trouver des clés probables soit de les essayer toutes, l'une après l'autre. La cryptologie comprend les deux arts : cryptographie et cryptanalyse.

Évidemment, un chiffre est sûr dès lors que les ressources nécessaires pour l'attaquer dépassent la valeur de l'information que l'on espère en retirer. Plutôt reliée à la valeur de l'information qu'à l'efficacité du meilleur décryptement connu, une telle définition n'est cependant pas opérationnelle.

Le concept d'efficacité d'un algorithme de décryptement doit être précisé plus objectivement : un algorithme est efficace tant qu'il requiert des ressources raisonnables en temps, mémoire et énergie, alors qu'il devient inefficace et inutilisable dès lors que les ressources nécessaires ne sont plus disponibles ; le temps devient astronomique, la mémoire galactique et l'énergie sidérale. Cette croissance des ressources requises est liée à la taille d'un paramètre de sécurité. Un algorithme a un comportement non polynomial quand il exige des ressources qui croissent plus vite que n'importe quel polynôme d'une variable qui est un paramètre de sécurité – par exemple, la taille d'un nombre entier composé public dont les facteurs premiers doivent être gardés secrets[5].

La théorie de la complexité déclare qu'un problème est complexe dès qu'il existe quelques cas où l'on ne parvient pas à la solution. Mais la cryptologie s'intéresse aux problèmes complexes pour lesquels la probabilité de trouver une solution est presque toujours négligeable. La cryptologie ouvre ainsi une voie nouvelle et originale à la théorie de la complexité.

Toutefois, remarquons qu'un problème est réputé complexe par manque d'entendement, voire par ignorance, c'est-à-dire tant que l'on ne connaît que des méthodes inefficaces pour le résoudre. Ce que l'on connaît en fait, c'est l'évolution de l'efficacité des seules méthodes connues, c'est-à-dire une sorte de borne supérieure de la complexité du problème posé alors que la cryptologie recherche une borne inférieure. Et il faut bien voir que l'efficacité évolue au gré de la puissance et de l'architecture des ordinateurs disponibles et au gré d'avancées en mathématiques pouvant survenir à tout moment. La complexité des problèmes utilisés en cryptologie, tout comme l'entropie de l'univers, décroît avec le recul de notre ignorance.

[5] Voir le chapitre « Les nouvelles orientations de la cryptographie » pp. 196-199.

Il semble donc illusoire de chercher à montrer qu'un chiffre à clé limitée est sûr au sens de la complexité de calcul ; seul le fait de le décrypter montre qu'il est désormais mauvais. Rappelons l'aphorisme bien connu attribué au philosophe Alain : « Tomber à l'eau en tentant de franchir le ruisseau à pieds joints ne prouve rien. Seul le fait d'atterrir sans se mouiller sur l'autre rive prouve que le ruisseau peut être franchi à pieds joints ».

Il y a une grande différence entre la philosophie de certains westerns où un bon Indien est un Indien mort et la philosophie de la cryptologie où un bon chiffre est un chiffre vivant, c'est-à-dire qui n'est pas encore mort. Il faut bien comprendre que tous les chiffres sont mortels. En d'autres termes, l'absence d'une méthode efficace de décryptement ne garantit rien : une découverte inattendue peut survenir à tout moment. Un chiffre meurt dès qu'un décryptement efficace est disponible. Les chiffres en usage, qui sont aujourd'hui considérés comme solides, sont en fait des chiffres dont les défauts n'ont peut-être pas encore été découverts, ou pire, révélés.

Bletchley Park et la réalisation des premiers calculateurs

Au Royaume-Uni, à Bletchley Park de 1940 à 1945, autour d'Alan M. Turing (1912-54), une équipe développe des machines *Colossus* pour décrypter les machines à chiffrer allemandes *Enigma* qui équipent chaque sous-marin, chaque navire de guerre, chaque unité de commandement[6].

La machine *Enigma* comprend une batterie électrique et une série de trois ou cinq rotors munis de contacts reliés d'une face à l'autre par un câblage interne propre au rotor. Au bout de la série de rotors, il y a un réflecteur avec des contacts sur une seule face et son propre câblage interne. Le clavier – un ensemble de touches – est complété par un ensemble de lampes, chacune associée à une lettre. Chaque frappe au clavier – une lettre claire ou chiffrée – induit un mouvement de rotors, et tant que la touche est enfoncée, un circuit électrique passant par les rotors et le réflecteur allume une lampe – la lettre correspondante chiffrée ou claire[7].

La machine *Colossus* comprend des lampes électroniques avec grilles et filaments, essentiellement des triodes faisant office de portes logiques

[6] NdE. : Contrairement à la conviction de l'auteur, les historiens, y compris les plus favorables à Turing, comme A. Hodges, conviennent que la machine *Colossus* a été élaborée par une équipe de chercheurs et d'ingénieurs autour de Max H. A. Newmann (1897-1984) et Thomas H. (Tommy) Flowers (1905-98) pour décrypter les machines de Lorenz (voir le chapitre « Du message chiffré au système cryptographique » p. 129). Au sein de Bletchley Park, Turing a pour sa part développé les « Bombes » qui ont permis de décrypter la machine *Enigma*. Il a ensuite travaillé au codage de la voix humaine. Turing est aujourd'hui universellement reconnu pour sa conception de la machine éponyme qui théorise la calculabilité (1936), et qui sera ultérieurement investie dans les ordinateurs.

[7] Voir le chapitre « L'ancrage de la cryptologie dans les jeux d'écriture » pp. 56-59.

laissant passer ou pas un signal électrique ; ce sont les tout premiers balbutiements d'une nouvelle technologie : l'électronique. Mais la durée de vie de chaque lampe est très limitée et imprévisible. Sur une machine *Colossus*, pour qu'un calcul de clés ait de bonnes probabilités d'aboutir, il faut pouvoir à tout moment changer des lampes sans arrêter la machine, c'est-à-dire organiser la machine en tiroirs qui détectent les pannes et se mettent hors tension en le signalant au monde extérieur ; on peut alors retirer le tiroir pour y changer la lampe défectueuse sans interrompre le calcul sur le reste de la machine ; une fois le tiroir réparé et remis en place, on le remet sous tension pour qu'il reprenne part aux calculs. Par la force des choses, la machine *Colossus* est ainsi tolérante aux pannes.

La machine *Enigma* fait penser à la machine à calculer de Blaise Pascal (1623-62) – encore appelée « Pascaline » – alors que la machine *Colossus* est le tout premier calculateur électronique. Mais contrairement à la machine *Enigma*, la machine *Colossus* a une taille physique et une consommation électrique l'excluant de tout terrain d'opérations. Durant la guerre, le décryptement est nettement favorisé au détriment du chiffrement.

Le pas technologique d'avance se prolonge tant que la maturité de la nouvelle technologie, l'informatique, n'atteint pas un niveau suffisant.

De suite après la guerre, sur ordre des plus hautes autorités britanniques du moment, toutes les machines *Colossus* sont détruites ainsi que les plans ; tout ce qui s'y rapporte est classifié, afin d'effacer la mémoire des acteurs et des témoins[8] ; cette lutte semble se poursuivre encore aujourd'hui.

Chaque année depuis 1966, l'ACM (*Association for Computing Machinery*) décerne le prix Turing (*Turing Award*, l'équivalent du prix Nobel en informatique) à des personnes ayant apporté une contribution significative à la science de l'informatique. C'est une reconnaissance posthume de la contribution significative de Turing à l'informatique.

L'OUVERTURE DE LA BOITE DE PANDORE

Dans les années 1970, un seul circuit intégré peut enfin réaliser une machine à chiffrer, en portant et en utilisant un chiffre, et même en y intégrant une gestion de clés. Depuis la guerre, l'informatique est restée au service exclusif de la cryptanalyse – l'art de casser des chiffres. Le pas technologique d'avance s'efface avec l'avènement du circuit intégré et plus particulièrement du microprocesseur. L'informatique passe ainsi au service de la cryptographie – l'art de concevoir des chiffres.

[8] Grâce à la mémoire des ingénieurs, notamment Thomas Flowers, et à la ténacité de Tony Sale, la machine *Colossus* a été reconstituée à Bletchley Park où elle est exposée (1994-96).

La cryptologie est restée classifiée, enterrée, soumise au secret, tant que la technologie a favorisé le décryptement. La traversée du désert aura duré une trentaine d'années.

Dans les années 1970, IBM (*International Business Machines*) mène des études dans le cadre d'un projet appelé *Démon* puis *Lucifer*. Les 30 juin et 2 novembre 1971, IBM dépose deux brevets d'invention, ouvrant ainsi la voie aux brevets sur les algorithmes cryptographiques. Le numéro de mai 1973 de la revue *Scientific American* comporte un article de vulgarisation de Horst Feistel (1915-90) : « Cryptography and Computer Privacy[9] ». Ainsi le projet *Lucifer* filtre dans le domaine public. Notons que dans l'article, la clé comporte 128 bits.

Les appels du NBS et la genèse du DES

Dans le journal officiel des États-Unis d'Amérique (*Federal Register*), afin de protéger des données fédérales sensibles non classifiées, le NBS (*National Bureau of Standards*) – devenu depuis NIST (*National Institute for Standards and Technology*) – publie deux appels à proposer un chiffre : le 15 mai 1973 et le 27 août 1974, puis deux appels à commenter une proposition : le 17 mars 1975 et le 1 août 1975.

Enfin, le 15 janvier 1977, le NBS publie le FIPS PUB 46 (*Federal Information Processing Standard, Publication* 46) plus connu sous le nom de DES (*Data Encryption Standard*). Dans le cadre d'une collaboration d'IBM avec le NBS et la NSA (*National Security Agency*), le projet *Lucifer* est à la base des spécifications du DES. Toutefois les principes de sécurité retenus pour guider les spécifications du DES n'ont toujours pas été révélés.

Le DES transforme un bloc (clair ou chiffré) de 64 bits en un autre bloc de 64 bits sous le contrôle d'une clé de 56 bits : tout couple de tels blocs (un clair et son chiffré) donne au moins une solution en clé, en général unique – le point d'unicité étant dépassé. Le DES est un chiffre « symétrique » : la même clé chiffre et déchiffre ; elle doit bien sûr rester secrète.

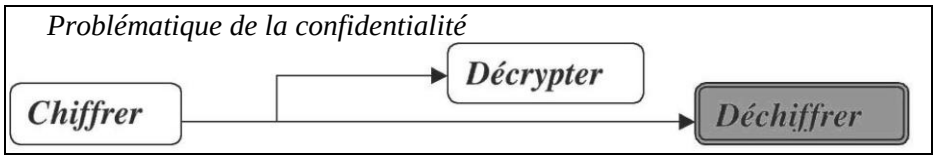
Diffie et Hellman à Stanford

À l'Université de Stanford en écho aux appels du NBS, Whitfield Diffie (né en 1941) et Martin E. Hellman (né en 1945) découvrent le concept de chiffre à clé publique, encore appelé chiffre asymétrique. Ils en parlent en juin 1975 à Lennox (Massachusetts) et en juin 1976 à Ronneby (Suède) à deux congrès de théorie de l'information organisés par l'IEEE (*Institute of*

[9] Voir le chapitre « Du message chiffré au système cryptographique » pp. 143-147.

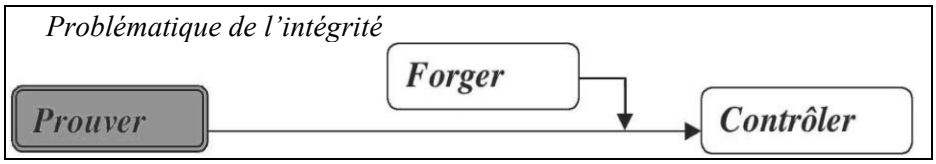
Electrical and Electronic Engineers). Le concept couvre la confidentialité et l'intégrité.

Le message peut atteindre quelqu'un d'autre que le légitime destinataire ; la communication peut être interceptée et écoutée. Pour assurer la confidentialité, il faut garder secrète au moins la clé de déchiffrement alors que la clé de chiffrement peut être publiée.



J'illustre la problématique de confidentialité par la boîte à lettres scellée au mur du bureau de Poste : n'importe qui peut y déposer du courrier ; le Préposé de la Poste dispose d'une clé afin d'ouvrir la boîte pour y relever le courrier déposé par le public. Soulignons l'ordre des opérations : le public dépose du courrier, puis le Préposé relève le courrier grâce à la clé.

Un faux message peut être injecté ; un message intercepté peut être modifié ou retardé ; l'expéditeur légitime peut être simulé. Pour assurer l'intégrité, il faut garder secrète au moins la clé utilisée pour prouver alors que la clé de contrôle peut être publiée.



J'illustre la problématique d'intégrité par la vitrine d'affichage scellée au mur de la Mairie : le Secrétaire de Mairie dispose d'une clé afin d'ouvrir la vitrine pour y afficher des avis municipaux à l'attention du public ; n'importe qui peut y lire les avis. Remarquons l'ordre des opérations : le Secrétaire affiche des avis grâce à la clé, puis le public lit les avis.

En 1976, Diffie et Hellman découvrent encore l'établissement d'une clé secrète entre deux correspondants ayant fixé deux nombres au préalable : un grand nombre premier p et une base a. Chacun choisit au hasard un grand nombre inférieur à p : c'est son exposant privé x (respectivement y) à garder secret. Pour établir une clé partagée, chacun élève la base a à son propre exposant privé modulo p, soit $a^x \bmod p$ (respectivement $a^y \bmod p$), et transmet le résultat à l'autre. Ensuite, pour chacun, la clé partagée est le nombre reçu élevé modulo p à son propre exposant privé. La fonction « exponentielle modulaire » est commutative :

$$(a^x)^y \bmod p = (a^y)^x \bmod p.$$

En juin 1976 à New York, Diffie et Hellman en parlent à la conférence NCC (*National Computer Conference*). En novembre 1976, ils publient leur article de référence : « New Directions in Cryptography »[10] dans la revue *IEEE Transactions on Information Theory*.

En avril 1977, je rends visite pour la première fois à Martin Hellman à l'Université de Stanford. Nous parlons de grands nombres premiers.

Pour calculer dans des corps et des anneaux sur des nombres entiers de plusieurs centaines de bits, je développe alors une bibliothèque en Fortran sur un ordinateur CII-HB 10070, l'ordinateur disponible à l'époque au CCETT (Centre Commun d'Etudes de Télévision et Télécommunications). En 1977, je ne suis sûrement pas le seul à développer ce genre de bibliothèque de calcul sur de grands nombres entiers. En juin 1977, cette bibliothèque me permet de trouver quelques grands nombres premiers, tels que $2^{209} - 33$ (un nombre premier de Sophie Germain[11]) et $2^{210} - 65$.

En mars 1979, paraît un article de synthèse de Diffie et Hellman, « Privacy and authentication : an introduction to cryptography ». On y trouve une bibliographie remarquable portant essentiellement sur les activités d'IBM dans les années 1970. Une fois ouverte, la boîte de Pandore ne se refermera plus[12].

Rivest, Shamir et Adleman au MIT

Outre les opérations de chiffrement et de déchiffrement pour assurer la confidentialité, ou bien de preuve (signature ou authentification) et de contrôle pour assurer l'intégrité, chaque système à clé publique comporte une troisième opération : la création de jeux de clés comprenant chacun une clé privée et une clé publique.

Diffie et Hellman n'ont pas encore trouvé d'exemple pratique lorsque durant les vacances de Noël 1976, Ronald L. Rivest (né en 1947), Adi Shamir (né en 1952) et Leonard Adleman (né en 1945), chercheurs au MIT (*Massachusetts Institute of Technology*), inventent le RSA, premier chiffre à clé publique.

La divulgation du RSA filtre d'abord de manière insolite en août 1977 dans la rubrique des jeux mathématiques de la revue *Scientific American* où l'article « Mathematical Game : A new kind of cipher that would take

[10] Voir le chapitre « Les nouvelles orientations de la cryptographie » p. 173.
[11] Sophie Germain (1776-1831) est une mathématicienne française. Par définition, tout nombre premier p tel que $2p + 1$ soit également premier est un nombre de Sophie Germain.
[12] Comme je n'ai malheureusement jamais rencontré Ralph Merkle, je ne le cite pas ici.

millions of years to break » de Martin Gardner[13] (1914-2010) retient toute mon attention.

Voici la clé publique RSA dans l'article (sans doute la première au monde) :
v = 9007 (ce nombre est premier)
n = RSA-129 (129 chiffres décimaux) = 114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 561 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541

En codant chaque lettre du message clair par deux chiffres décimaux : 01 pour *A*, 02 pour *B*, … 26 pour *Z* et 00 pour un espace, sans majuscule ni minuscule, le message « *IT IS ALL GREEK TO ME* » est transformé en un nombre. Grâce à ma bibliothèque en Fortran, je vérifie tous les exemples numériques dans la semaine suivant la parution de l'article.

L'article invite encore à demander au MIT une copie du mémoire technique MIT/LCS TM82. J'écris en septembre puis en novembre. Faute de réponse, j'écris une troisième fois au MIT en décembre 1977 en y insérant des vœux cryptographiques afin de retenir l'attention de Rivest.

Pour créer mon propre jeu de clés RSA, je fixe un exposant public v ; puis je prends au hasard deux grands facteurs premiers : p_1 et p_2, à garder secrets. Le module public est le produit des facteurs premiers ($n = p_1 p_2$). La clé publique comprend l'exposant public et le module [v, n]. L'exposant public doit être premier avec chaque facteur premier moins un.

$$\text{pgcd}(v, p_i - 1) = 1$$

Cette contrainte entre l'exposant et chaque facteur assure que chaque fonction « élever à la puissance v-ième modulo p_i » permute l'ensemble des entiers de 0 à $p_i - 1$: la fonction est inversible.

La fonction inverse est une autre fonction puissance dont l'exposant s_i est l'inverse de v modulo $p_i - 1$:

$$v\, s_i \mod (p_i - 1) = 1$$

La fonction composée « élever à la puissance v-ième modulo n » est donc également inversible : elle permute l'ensemble des entiers de 0 à $n - 1$.

La fonction inverse est une autre fonction puissance dont l'exposant s, à garder secret, est l'inverse de v modulo ppcm$(p_1 - 1, p_2 - 1)$:

$$v\, s \mod \text{ppcm}(p_1 - 1, p_2 - 1) = 1$$

[13] Gardner anime la rubrique « Mathematical Games » du *Scientific American* de 1956 à 1981.

La clé privée RSA comprend l'exposant privé et le module : [*s*, *n*]. Dans ma bibliothèque, afin de réduire la charge de calcul, j'utilise chaque facteur premier avec l'exposant privé associé : [p_1, s_1, p_2, s_2].

Voici la clé publique RSA du CCETT (sans doute la seconde au monde) :
v = 10103 (ce nombre est premier tout comme 9007)
n = CCETT-129 (129 chiffres décimaux) = 114 331 674 692 170 021 543 566 548 973 781 017 441 790 837 262 788 891 346 006 256 380 182 010 783 582 559 365 751 613 488 728 226 552 502 131 311 260 220 786 172 216 269

Dans l'article de Gardner, on signe un cryptogramme et on chiffre une signature. C'est pourquoi j'ai construit le nombre CCETT-129 avec les mêmes quatre chiffres en poids forts que RSA-129. La « proximité » des modules limite les effets de bord pour signer un cryptogramme et chiffrer une signature.

Voici mes vœux en clair :

HAPPY NEW YEAR BONNE ANNEE BLOAVEZ MAD LOUIS GUILLOU

En breton, les mots « bloavez mad » signifient la même chose que « bonne année » en français et « happy new year » en anglais. Leur usage réduit sensiblement la probabilité de rétablir le texte clair pour des gens qui ne connaissent pas le breton (il n'y a pas beaucoup de bretonnants au MIT).

Le codage indiqué dans l'article de Gardner donne le nombre :

80 116 162 500 140 523 002 505 011 800 021 514 140 500 011 414 050 500 021 215 012 205 260 013 010 400 000 012 152 109 190 007 210 912 121 521

Je signe d'abord le nombre avec ma clé privée ce qui donne la signature :

72 460 412 348 038 838 058 341 812 565 585 282 410 250 353 887 348 666 078 030 592 927 589 114 525 792 783 873 924 354 989 153 999 792 980 739 816 337 960 103 744 428 702

Puis je chiffre avec la clé publique du MIT ce qui donne le nombre :

866 848 798 341 150 392 408 504 327 835 826 084 136 073 367 118 725 975 767 180 150 248 262 737 158 155 636 407 559 273 328 750 205 408 752 542 724 736 983 422 506 663

En décembre 1977, le MIT dépose une demande de brevet délivré le 20 septembre 1983. À mon avis, cette demande aurait été classifiée si l'article de Martin Gardner n'avait divulgué l'invention, ou bien elle aurait été rejetée si *Lucifer* n'avait ouvert la voie aux brevets sur les algorithmes.

Toutefois, ce même article empêche d'étendre le brevet en dehors des États-Unis parce que l'invention est divulguée dans le reste du monde. C'est

une spécificité de la loi américaine par rapport aux lois du reste du monde : l'inventeur américain qui divulgue ses résultats dispose d'une année pour déposer une demande de brevet aux États-Unis.

En février 1978, l'article de référence de Rivest, Shamir et Adleman « A Method for Obtaining Digital Signatures and Public-Key Cryptosystems » paraît dans la revue *Communications of the ACM*.

En avril 1978 pour la seconde fois, je rends visite à Martin Hellman à Stanford. Je lui fais remarquer que l'article paru dans les publications de l'ACM livre beaucoup moins d'informations que le mémoire MIT/LCS TM82. Il me répond : « Bien obligé, la publication est contrôlée ! ». Il ne s'agit donc pas tant d'une version simplifiée que d'une version expurgée ! Persuadé que je détiens une copie du mémoire, Hellman me questionne à son tour. Je lui réponds : « Non, je n'en ai pas, mais je voulais savoir si toi, tu en détenais une ». Du coup, il n'est pas très content. Je prêche en somme le vrai pour savoir le vrai et il se sent un peu manipulé. C'est d'ailleurs un subterfuge que j'utilise plusieurs fois par la suite pour faire émerger ce qu'on ne dit pas.

Ensuite, toujours en avril 1978, pour la première fois, je rends visite à Ronald Rivest au MIT. Je lui demande pourquoi il ne distribue pas le MIT/LCS TM82 ; il m'apprend que le MIT ayant reçu environ 4000 demandes, la NSA s'en est émue et a fait retirer tous les exemplaires des étagères du MIT. Ceci démontre bien que la boîte de Pandore est définitivement ouverte. Je ne suis pas le seul à avoir développé une bibliothèque de calcul arithmétique.

Dans l'article de Gardner, il y a la promesse de Rivest d'un chèque de cent dollars au premier qui décryptera un cryptogramme donné en défi. Rivest m'avoue n'avoir pas osé tester mes vœux, car il aurait dû utiliser l'exposant privé du MIT, un secret permettant de décomposer le nombre RSA-129 en facteurs premiers. Or les ordinateurs disponibles à l'époque au MIT sont incapables de garantir un secret face à la curiosité des étudiants – sur ce point, les ordinateurs ne se sont pas beaucoup améliorés en trente ans.

Factorisation de RSA-129

Par contre, les performances évoluent vite. Selon l'article de Gardner en 1977, il faudrait des millions d'années pour décomposer RSA-129 en facteurs premiers. Pourtant le 27 avril 1994, le mathématicien hollandais Arjen K. Lenstra (né en 1956), employé des *Bell Labs* aux États-Unis, publie :

RSA-129 = 3 490 529 510 847 650 949 147 849 619 903 898 133 417 764 638 493 387 843 990 820 577
× 327 691 329 932 667 095 499 619 881 908 344 614 131 776 429 679 929 425 397 982 88 533

Durant une phase initiale de filtrage d'environ 5000 Mips-année[14], 600 volontaires de plus vingt pays sur tous les continents (sauf l'Antarctique) récoltent beaucoup de relations, difficiles à trouver mais faciles à vérifier.

Il en résulte une matrice presque vide de 569 466 rangées et 534 338 colonnes. La matrice est réduite en une matrice dense de 188 614 rangées et 188 160 colonnes par élimination gaussienne structurée. Chaque élimination gaussienne ordinaire sur la matrice dense de 35 489 610 240 bits (4,13 Go) demande 45 heures sur un ordinateur massivement parallèle 16K MasPar MP-1. Les trois premières éliminations sont infructueuses : elles donnent une décomposition triviale ; la quatrième décompose RSA-129.

Bien entendu, Lenstra n'encaisse jamais le chèque de cent dollars de Rivest : chacun des 600 volontaires ayant collaboré au projet reçoit une photocopie certifiée du chèque original que j'ai vu exposé sous verre au mur du bureau de Lenstra aux *Bell Labs*. Le clair du cryptogramme publié par Gardner est : « *THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE* ».

Révélations du CESG

Après le décès de James H. Ellis[15] (1924-97), lors d'une conférence à Cirencester le 18 décembre 1997, Clifford C. Cocks fait un exposé qui révèle l'activité du CESG (*Communication Electronics Security Group*), groupe d'études au service britannique du chiffre, en matière de chiffre à clé publique. Le CESG met alors cinq notes en ligne sur Internet :

– James H. Ellis, « The Possibility of Secure Non-Secret Encryption », janvier 1970 ; cette note explique le concept du chiffrement sans secret ;

– Clifford C. Cocks, « A Note on Non-Secret Encryption », 20 novembre 1973 ; cette note explique la fonction « élever à la puissance *n*-ième modulo *n* » ;

– Malcolm J. Williamson, « Non-Secret Encryption Using a Finite Field », 21 janvier 1974 ; cette note explique comment assurer la confidentialité avec deux cadenas : l'expéditeur ferme une boîte avec son cadenas et l'adresse au destinataire ; puis, le destinataire y ajoute son propre cadenas et retourne la boîte à l'expéditeur ; l'expéditeur retire son cadenas et retourne la boîte au destinataire ; le destinataire retire son propre cadenas et ouvre la boîte ;

[14] Million d'instructions par seconde pendant une année.
[15] http://en.wikipedia.org/wiki/James_H._Ellis.

L'intérêt de la fonction : puissance *n*-ième modulo *n*
Si n est le produit de deux grands facteurs premiers p_1 et p_2, que p_1 ne divise pas $p_2 - 1$ et que p_2 ne divise pas $p_1 - 1$, alors la fonction « puissance n-ième modulo n » permute l'anneau des entiers mod n ; cette permutation est inversée par la fonction « puissance x-ième modulo n » où x est le plus petit nombre entier tel que $\lambda(n) = \text{ppcm}(p_1 - 1, p_2 - 1)$ divise $xn - 1$.
Cette fonction est donc une réalisation particulière du RSA avant la lettre.

– Malcolm J. Williamson, « Thoughts on Cheaper Non-Secret Encryption », 10 août 1976 ; cette note explique la mise à la clé par la fonction « exponentielle modulaire » ;

L'intérêt de la fonction : exponentielle modulaire
Soit p un grand nombre premier. Chacun des deux communicants choisit un grand nombre entier inférieur à p et premier avec $p - 1$ et le garde secret. Chaque nombre privé, a et b, a un inverse modulo $p - 1$, soit x et y.
La boite est un grand nombre k inférieur à p échangé en trois passes.

$$k^a \bmod p$$
$$(k^a \bmod p)^b \bmod p$$
$$((k^a \bmod p)^b \bmod p)^x \bmod p = k^b \bmod p$$

Le destinataire retrouve la boîte $(k^b \bmod p)^y \bmod p = k$.
Cette fonction est donc une réalisation particulière du DH[16] avant la lettre.

– James H. Ellis, « The History of Non-Secret Encryption », 1987 ; cette note de synthèse sert de chapeau aux quatre notes précédentes.

Ainsi, le CESG découvre les chiffres à clé publique un peu plus tôt que Diffie, Hellman, Rivest, Shamir et Adleman. Trois remarques s'imposent :
1. Les Anglais inventent le « RSA » avant le « DH ».
2. Axés sur la « confidentialité », les Anglais passent à côté de « l'intégrité », c'est-à-dire la signature et l'authentification.
3. Pour les Anglais, il est hors de question de breveter : en effet, une agence gouvernementale se doit de classifier tout travail en cryptographie.

Diffie, Hellman, Rivest, Shamir et Adleman vont bien plus loin que Ellis, Cocks et Williamson : le mérite d'introduire la cryptologie dans le domaine public leur revient ; le CESG ne l'aurait jamais fait sans eux.

Une visite chez IBM

En janvier 1980, je rends ma seule et unique visite à Walter Tuchman[17] chez IBM à Poughkeepsie, sur les rives de l'Hudson, au nord de New York.

[16] NdE. : Echange de clé Diffie-Hellman, voir le chapitre « Les nouvelles orientations de la cryptographie » pp. 186-187.

Il me reçoit dans une pièce sans fenêtre, sans tableau, avec juste une table et deux chaises ; dans un coin, un observateur muet qui ne se présente même pas prend fébrilement des notes : curieuse ambiance.

Walter envisage de réaliser un circuit intégré spécifique implémentant le DES et gérant des clés n'apparaissant jamais en clair à l'interface.

Je lui fais remarquer qu'un tel circuit intégré spécifique poursuit les mêmes objectifs qu'une carte à puce, si ce n'est que la carte porte un circuit intégré à tout faire, à savoir, un microprocesseur. Il est persuadé que le DES est hors de portée des microprocesseurs : le DES a été conçu pour un circuit intégré spécifique. Pour IBM et la NSA, implanter le DES sur un microprocesseur est sans doute à l'époque une hérésie. Ce soir-là, Walter ne m'invite même pas à diner : il me dit qu'il fête l'anniversaire de sa fille.

Preuves de sécurité et protocoles de preuve interactive

Aux États-Unis, les recherches de preuves de sécurité en matière de chiffres à clé publique commencent dans les années 1980-83 au laboratoire de Manuel Blum à Berkeley. C'est là que Shafi Goldwasser (né en 1958) et Silvio Micali (né en 1954) – deux thésards – imaginent des schémas probabilistes avec une sécurité équivalente à celle du problème arithmétique sous-jacent, en l'occurrence la décomposition en facteurs premiers de grands nombres entiers composés.

Pour un schéma de confidentialité, l'espace des clairs étant réduit à deux éléments (un seul bit), l'ennemi reçoit autant de cryptogrammes qu'il souhaite. Il connaît la clé publique : essentiellement, un module public composé. S'il s'éloigne sensiblement d'une chance sur deux pour rétablir les clairs (un bit par clair), alors il dispose d'un algorithme qui lui permet de décomposer le module.

Pour un schéma de signature, l'ennemi reçoit autant de signatures qu'il souhaite. Il connaît la clé publique : essentiellement, deux modules publics composés. S'il produit une signature de plus, alors il connaît une information qui lui permet de décomposer l'un des deux modules.

Goldwasser et Micali sont nommés professeurs au MIT avant leur trente ans, un exploit qui mérite d'être souligné. Rivest les fait venir tous les deux au colloque *Eurocrypt*, organisé à la Sorbonne[18] à Paris du 4 au 6 mars 1984. C'est ma première rencontre avec Shafi Goldwasser et Silvio Micali et le début d'une longue amitié qui se poursuit encore aujourd'hui.

---

[17] Walter Tuchman a dirigé avec Carl Meyer le développement du DES chez IBM.

[18] Voir le chapitre « L'influence de la cryptologie moderne sur les mathématiques et l'université » p. 278.

Parmi les présentations à *Eurocrypt '84*, je retiens celle de Fisher, Micali et Charles Rackoff (né en 1948) : « A Secure Protocol for the Oblivious Transfer ». Etant donné un nombre public et un module composé, il s'agit de prouver la connaissance d'une racine carrée modulaire du nombre public sans révéler la valeur de cette racine, c'est-à-dire en la maintenant secrète. Cette présentation ne figure pas dans les actes du colloque *Eurocrypt '84*, les auteurs n'ayant pas fourni de manuscrit en temps utile ; en 1996, douze ans plus tard, la revue *Journal of Cryptology* publie cette présentation, démontrant ainsi son importance dans le déroulement des évènements.

En mai 1985 à Providence (Rhode Island), Goldwasser, Micali et Rackoff font une communication au 17e *Symposium on Theory of Computing* : « Knowledge Complexity of Interactive Proofs ». L'article est publié la même année. Quatre ans plus tard, ils publient un article de référence « The Knowledge Complexity of Interactive Proof Systems » dans la revue *SIAM Journal of Computing*. En 1985, à la demande de Shafi, je prends part aux vérifications des épreuves de l'article.

Les preuves interactives permettent de prouver que l'on connaît une solution d'un problème sans la révéler et de vérifier la solution sans en prendre connaissance. Pour s'authentifier[19] ou par extension, pour signer, on peut donc utiliser indéfiniment le même secret sans que le secret ne s'use.

Ces travaux et leurs conséquences justifient l'attribution en 2013 du prix Turing (*Turing Award*, l'équivalent du prix Nobel en informatique) à Silvio Micali et Shafi Goldwasser. Rappelons que le prix Turing a été attribué à Manuel Blum (né en 1938) en 1995 et à Rivest, Shamir et Adleman en 2002.

Une vulgarisation réussie

En 1980, je rends visite à Jean-Jacques Quisquater[20] et Marc Davio à Bruxelles chez Philips/MBLE (Manufacture Belge des Lampes Electriques). Je leur explique mes développements en matière d'accès conditionnel par carte à puce en radiodiffusion. C'est le début d'une profonde amitié et d'une fructueuse collaboration en matière de carte à puce et de cryptologie.

Le concept de preuve interactive est assez difficile à expliquer, mais c'est pourtant crucial, puisqu'il faut parvenir à convaincre les acteurs économiques ou politiques sans accaparer plus de cinq ou dix minutes de leur temps précieux. Si on ne parvient pas à le leur faire comprendre dans le

[19] La question de l'authentification est largement abordée dans le chapitre « Les nouvelles orientations de la cryptographie », surtout pp. 188-191.

[20] Jean-Jacques Quisquater travaille pour l'entreprise Philips de 1970 à 1991. Il y développe la sécurisation des informations, avant d'y créer un département entier de cryptographie. En 1991, il rejoint l'Université Catholique de Louvain (UCL), où il dirige le laboratoire de cryptologie jusqu'en octobre 2010. Il est aujourd'hui professeur émérite à l'UCL.

temps imparti, c'est trop tard ! Les autorités hiérarchiques n'accordent que quelques minutes d'attention et s'ils n'ont pas compris en aussi peu de temps, ils en déduisent que le sujet est définitivement incompréhensible.

Alors en 1989, avec Jean-Jacques Quisquater, on a l'idée que si les enfants comprennent, les chefs comprendront sans doute aussi !

À Crypto '89, lors de la dernière présentation de la session impromptue (*rump session*), les familles Quisquater et Guillou ont introduit une étrange caverne. L'article figure à la fin des actes du colloque, avec pour auteurs : Soazig, Gwénolé, Anna, Gaïd, Marie-Annick et moi-même, Michael, Muriel, Myriam et Jean-Jacques Quisquater, en collaboration avec Thomas A. Berson pour la version en langue anglaise.

L'étrange caverne comporte essentiellement une entrée, un point de rencontre et une porte à digicode : de l'entrée, on ne voit ni le point de rencontre, ni la porte ; du point de rencontre, on ne voit pas la porte. Le digicode permet d'actionner la porte. Pour qui ne le connaît pas, chaque couloir d'accès est un cul-de-sac. Notre protocole de preuve interactive fait intervenir Claire et Véronique.

– Claire veut prouver qu'elle connaît le digicode sans le dévoiler.
– Véronique veut contrôler sans prendre connaissance du digicode.

Ces deux contraintes excluent le protocole trivial où Claire utilise le digicode en présence de Véronique.

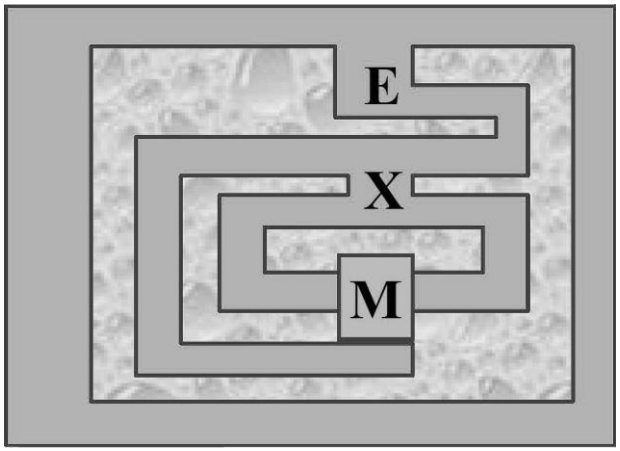


Fig. 1. La caverne à preuve interactive. Illustration L. Guillou.

Voici un protocole où le secret ne s'use pas quand on s'en sert :

1. Claire et Véronique se tiennent à l'entrée.
2. Claire s'engage seule, au hasard et en secret, par un des couloirs jusqu'à la porte.

3. Véronique se rend au point de rencontre où, au hasard, elle défie Claire d'apparaître par un des couloirs.
4. Claire répond en utilisant le digicode pour actionner la porte si besoin est.
5. Véronique contrôle que Claire arrive bien par le couloir désigné.
6. Claire et Véronique répètent t fois les étapes 1 à 5. Le nombre t est un facteur de sécurité pour accroître l'intime conviction de Véronique.

Ce protocole introduit les actions de base : engagement, défi, réponse et contrôle. Les remarques suivantes s'imposent :
– Qui dispose du secret réussit chaque itération du protocole en l'utilisant.
– À chaque itération du protocole, qui n'en dispose pas a exactement une chance de passer le contrôle en anticipant le défi : tous les défis possibles doivent donc être également probables.
– On ne distingue pas entre des données échangées lors de t itérations successives réussies et des données échangées en simulant à partir d'une liste préétablie de t défis. Si le contrôleur acquiert bien une conviction en prenant part au protocole, c'est-à-dire en choisissant les défis au hasard une fois que celui qui prouve s'est engagé, les données qu'il recueille ne peuvent pas convaincre un tiers : l'authentification ne laisse aucune trace probante et la preuve interactive n'est pas transmissible.
– Puisque le relevé d'une simulation ne révèle certainement pas le secret et qu'un observateur ne le distingue pas du relevé d'une authentification réussie, ce protocole n'use pas le secret alors même que l'on s'en sert.

Si l'étrange caverne plait à nos enfants, il est probable que nos chefs l'apprécient aussi. Quoiqu'il en soit, comme les actes des colloques *Crypto*, *Eurocrypt* et *Asiacrypt* sont disponibles sur des CD publiés par l'éditeur Springer Verlag, il est aisé d'évaluer l'impact d'une publication en comptant le nombre de fois où elle est citée dans les bibliographies de publications ultérieures. Pour notre article sur l'étrange caverne à Crypto '89, ce décompte dénote une vulgarisation particulièrement réussie.

Exemples de protocoles de preuve interactive

Une fois les concepts de base acquis grâce à la caverne, on peut aborder des réalisations arithmétiques. Je fais ici la synthèse de quatre systèmes : FMR par Fisher, Micali et Rackoff en 1984, FS par Fiat et Shamir en 1986, GQ1 par Guillou et Quisquater de 1987 à 1989 et GQ2 par les mêmes de 1999 à 2004.

Tout comme le RSA, ces quatre systèmes s'appuient sur le problème de la factorisation. Dans chaque cas, on prend au hasard au moins deux grands facteurs premiers p_1 et p_2 à maintenir secrets et on les multiplie l'un par l'autre pour former un module public $n = p_1 p_2$.

On fixe alors un exposant public *v*. Régie par la clé publique [*v*, *n*], une équation générique lie une autre paire de nombres, à savoir, un nombre public *G* et un nombre privé *Q*, liés par l'une des équations génériques :

$$GQ^v \bmod n = 1 \quad \text{ou bien} \quad G = Q^v \bmod n$$

Les nombres *v*, *n* et *G* constituent la clé publique. On garde secret le nombre *Q* (ainsi que p_1 et p_2).

La valeur de l'exposant public *v* ainsi que les contraintes imposées entre l'exposant et les facteurs premiers caractérisent chaque système.

Pour FMR et FS, l'exposant *v* vaut deux, $v = 2$; le nombre *Q* est pris au hasard ($1 < Q < n$-1) ; le nombre *G* est le carré modulaire du nombre *Q*, soit $G = Q^2 \bmod n$. Remarquons que FMR et FS n'utilisent pas les facteurs premiers ; le module *n* peut lui-même être choisi au hasard (la factorisation du module *n* peut donc n'être pas connue).

Pour GQ1, l'exposant *v* est un nombre premier impair qui ne divise ni $p_1 - 1$, ni $p_2 - 1$: [*v*, *n*] est donc une clé publique RSA. Le nombre *G* est déduit d'un train de bits, par exemple, une identité *Id*, selon une norme de signature RSA mettant en œuvre une fonction de hachage[21]. Le nombre *Q* s'obtient en appliquant la clé privée RSA au dit nombre *G*.

Pour GQ2, l'exposant *v* est une puissance de deux : $v = 2^k$. Le nombre *k* est un facteur de sécurité. Le nombre *G* est le carré d'un petit nombre premier *g* appelé « nombre de base », soit $G = g^2$. Chaque facteur premier est congru à 3 mod 4 de sorte que la fonction « carré mod *p* » permute l'ensemble des résidus quadratiques modulo *p*. Les facteurs premiers sont tels que le symbole de Legendre de *g* diffère d'un facteur premier à l'autre :

$$\left(\frac{g}{p_1}\right) = -\left(\frac{g}{p_2}\right)$$

Comme les symboles de Jacobi sont alors $\left(\frac{g}{n}\right) = -1$ et $\left(\frac{n-g}{n}\right) = -1$, ni *g* ni $n - g$ ne sont des carrés modulo *n*.

Pour $g = 2$, un facteur premier est congru à 3 mod 8 et l'autre à 7 mod 8 (donc *n* est congru à 5 mod 8) ; pour $g = 3$, l'un est congru à 1 mod 3 et l'autre à 2 mod 3 (donc *n* est congru à 5 mod 12) ; pour $g = 5$, l'un est congru à 1 ou 4 mod 5 et l'autre à 2 ou 3 mod 5 (donc *n* est congru à 17 mod 20) ; et ainsi de suite. La pertinence de la clé publique GQ2 est évidente.

[21] Voir le chapitre « La relation agitée entre mathématiques et cryptographie » p. 301.

Le nombre Q est une racine 2^k-ième de G, soit une racine 2^{k+1}-ième de g, ce qui implique la connaissance d'une racine carrée modulaire quadratique de g^2 (par construction, ni g ni $n - g$ ne sont des carrés mod n), c'est-à-dire un nombre q tel que n divise $q^2 - g^2$ alors que n ne divise ni $q - g$ ni $q + g$; ce qui donne la décomposition $n = \text{pgcd}\,(n, q - g)\,\text{pgcd}\,(n, q + g)$.

Symbole de Legendre et symbole de Jacobi.
Étant donné un nombre premier p, le symbole de Legendre, appelé aussi caractère quadratique de a par rapport à p, vaut 1 si a est un carré modulo p ; il vaut – 1 dans le cas contraire. Il peut se calculer à l'aide de la formule suivante due à Euler :

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \ (\text{mod. } p).$$

Le symbole de Jacobi généralise le symbole de Legendre aux nombres entiers composés. Par définition, si n est le produit de deux nombres premiers p et q, le symbole de Jacobi est le produit des symboles de Legendre :

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) \times \left(\frac{a}{q}\right)$$

Si l'entier a n'est pas un carré modulo p, ni modulo q, alors les symboles de Legendre de a par rapport à p et à q valent tous deux –1. Le symbole de Jacobi vaut 1 (c'est leur produit), mais pour autant a n'est pas un carré modulo n.
Par contre, si le symbole de Jacobi vaut –1, alors a n'est pas un carré modulo n.
Lorsque la factorisation de n est inconnue, le symbole de Jacobi est facilement calculé grâce à la loi de réciprocité quadratique démontrée par Gauss.

Remarquons que $q/g \bmod n$ est une racine carrée non triviale de l'unité, c'est-à-dire un nombre entier x tel que $x^2 \bmod n = 1$, avec $1 < x < n - 1$.

Le protocole suivant réalise successivement les quatre actions de base identifiées avec le protocole de la caverne : s'engager, défier, répondre, contrôler. Le protocole suivant englobe FMR, FS, GQ1 et GQ2.
– S'engager en tirant au hasard un grand nombre entier r : $1 < r < n–1$ (cet aléa doit rester secret) puis en lui appliquant la clé $[v, n]$.

$$T = r^v \bmod n$$

– Défier en tirant au hasard un nombre entier : 0 ou 1 pour FMR/FS, de 0 à v–1 pour GQ1, k bits pour GQ2.
– Répondre au défi selon l'aléa, le nombre privé et le module.

$$D = rQ^d \bmod n$$

– Contrôler selon le nombre public, le défi, la réponse, la clé [v, n] et l'équation générique : $GQ^v = 1 \bmod n$, ou bien $G = Q^v \bmod n$, en constatant l'une des deux égalités suivantes.

$$T = G^d D^v \bmod n \quad \text{ou bien} \quad TG^d = D^v \bmod n$$

Preuves de sécurité de GQ1 et GQ2

FMR et FS n'ont pas de preuve de sécurité ; mais GQ1 et GQ2 en ont.

Par définition, une paire entrelacée GQ est une paire de réponses valides D et E à deux défis d et e pour le même engagement T, soit :

$$(E/D)^v G^{(e-d)} = 1 \bmod n$$

– Pour GQ1, on calcule les deux nombres entiers uniques x et y (les coefficients de Bézout des nombres v et $e - d$) tels que :

$$x\,v - y\,(e - d) = 1, \text{ ce qui donne : } Q = (E / D)^x\, G^y \bmod n$$

Toute paire entrelacée GQ1 révèle ainsi le nombre Q, c'est-à-dire la signature RSA de l'identité proclamée *Id*.

– Toute paire entrelacée GQ2 révèle une racine carrée modulaire non triviale de g^2, c'est-à-dire un nombre entier q tel que n divise $q^2 - g^2$ sans diviser ni $q - g$ ni $q + g$, ce qui donne n = pgcd (n, $q - g$) pgcd (n, $q + g$).

On peut comparer quatre méthodes d'authentification comme suit :

RSA statique	**RSA dynamique**
Voici mon identité *Id* et la signature RSA d'*Id* produite par l'autorité.	Voici mon identité *Id*, ma clé publique RSA [v, n] et un certificat de l'autorité liant *Id* à [v, n].
	Ma clé privée RSA me permet de déchiffrer n'importe quel défi cohérent.
GQ1 dynamique	**GQ2 dynamique**
Voici mon identité *Id*. Je garde secrète la signature RSA d'*Id* produite par l'autorité.	Voici mon identité *Id*, ma clé publique GQ2 [g, k, n] et un certificat de l'autorité liant *Id* à [g, k, n].
Je prouve par interaction que je connais la signature RSA de *Id*.	Je prouve par interaction que je connais la factorisation de n.

Comparaison des performances de RSA et GQ2 pour le même module

L'expérience suivante se déroule sur un ordinateur personnel dialoguant avec une carte à puce disposant de deux facteurs premiers dont le produit forme un module de 1024 bits. On compare l'authentification dynamique en RSA (défi, réponse) et en GQ2 (engagement, défi, réponse).
– La carte utilise les clés privées RSA [p_1, s_1, p_2, s_2] et GQ2 [p_1, Q_1, p_2, Q_2].
– L'ordinateur personnel utilise les clés publiques RSA [$v = 257$, n] et GQ2 [$g = 2$, $k = 8$, n]. Ainsi chaque défi comporte 8 bits.

Non seulement RSA n'a aucune preuve de sécurité, mais il faut encore se prémunir d'attaques par messages choisis. Par exemple, selon la méthode préconisée par Peter Landrock, à chaque authentification, le contrôleur prend au hasard un aléa de $|n|–|h|–1$ bits ($|n|$ est le nombre de bits du module et $|h|$ le nombre de bits du code de hachage utilisé) ; il calcule le code de hachage de l'aléa et obtient le défi en appliquant la clé publique RSA à la concaténation du code de hachage et de l'aléa : défi = $(\mathrm{h}(x) \parallel x)^v \bmod n$. Avant de délivrer x en réponse, la carte doit constater la cohérence du défi en comparant le code de hachage rétabli avec le code de hachage[22] de l'aléa rétabli. Les opérations de hachage sont négligeables devant les opérations arithmétiques.

Pour l'authentification dynamique avec un module de 1024 bits, RSA requiert 30 à 40 fois plus d'opérations dans la carte que GQ2. Ce ratio croît linéairement en fonction du nombre de bits du module. La dispersion du ratio est due au poids de Hamming du défi de huit bits ($k = 8$) en GQ2.

Notons que RSA et GQ2 accommodent aisément plus de deux facteurs premiers, par exemple, trois ou quatre facteurs pour un module de 1500 bits ou plus. Alors, sans déroger aux preuves de sécurité (toute paire entrelacée dévoile une décomposition non triviale du module ; mais s'il y a plus de deux facteurs, il y a plusieurs décompositions non triviales), si ce n'est que la pertinence d'une clé publique GQ2 n'est plus aussi évidente, GQ2 utilise deux nombres de base avec trois facteurs premiers, trois nombres de base avec quatre facteurs premiers, et ainsi de suite.

Plusieurs produits de sécurisation de communications entre ordinateurs utilisent une variante de GQ1 pour réaliser des réseaux privés d'entreprise. Ce que nous avons inventé tous les deux, Jean-Jacques et moi, est donc utilisé aujourd'hui à très grande échelle : c'est gratifiant au plan intellectuel, même si les brevets sont bafoués.

Certaines cartes à puce utilisent RSA statique, d'autres RSA dynamique. Jusqu'à présent à ma connaissance, aucune carte n'utilise GQ1 ni GQ2. Pour être mise en œuvre, une méthode doit être disponible au bon endroit au bon

[22] Voir chapitre « La relation agitée entre mathématiques et cryptographie » p. 301.

moment. Pour l'authentification dynamique des cartes à puce, GQ2 est bien plus approprié que RSA ou même GQ1.

LA SAGA DE LA CARTE A PUCE

En 1968, les Presses de la Cité publient un roman de science-fiction, *La nuit des temps,* où René Barjavel décrit une bague capable de mémoriser, de traiter et de communiquer de l'information. Cette première édition est rare.

> « Chaque fois qu'un Gonda désirait quelque chose de nouveau, des vêtements, un voyage, des objets, il payait avec sa clé. Il pliait le majeur, enfonçait sa clé dans un emplacement prévu à cet effet et son compte, à l'ordinateur central, était aussitôt diminué de la valeur de la marchandise ou du service demandé »[23].

L'utilisation d'un objet portable doté d'un composant électronique comportant une mémoire a fait l'objet de divers dépôts de brevets dans les années 1970 : les Américains Ellingboe (1970), Castrucci (1971) et Halpern (1972), le Japonais Arimura (1970), l'Allemand Dethloff (1977) et bien d'autres. Ellingboe décrit un moyen électronique de paiement dans une carte de crédit à contacts. Halpern décrit un crayon sécurisé pour le paiement. Arimura décrit l'authentification dynamique d'un dispositif d'identification. Ces brevets n'ont donné lieu à aucune réalisation.

On peut à juste titre se demander pourquoi la carte à puce est considérée comme une invention française. La réponse est simple : c'est en France que le développement industriel a commencé.

La généalogie des premiers brevets

Dans toute nouvelle technologie, je distingue trois types de brevets : des brevets pionniers, des brevets de base et des brevets de développement.
– Les brevets pionniers restent stériles : ils ne débouchent sur aucune valorisation. Comme dans la parabole du semeur, certains grains de blé ne germent pas, faute de réunir les conditions nécessaires à la germination.
– Les brevets de base germent : ils provoquent les premières valorisations. Les technologies nécessaires sont enfin réunies ; pour les cartes à puce, ce sont la micro-électronique, l'informatique et la cryptologie.
– Les brevets de développement établissent des champs d'application : ce sont souvent des brevets de base dans leur branche. La notion de brevet de base est une notion récurrente.

---

[23] Barjavel, *La nuit des temps*, p. 151.

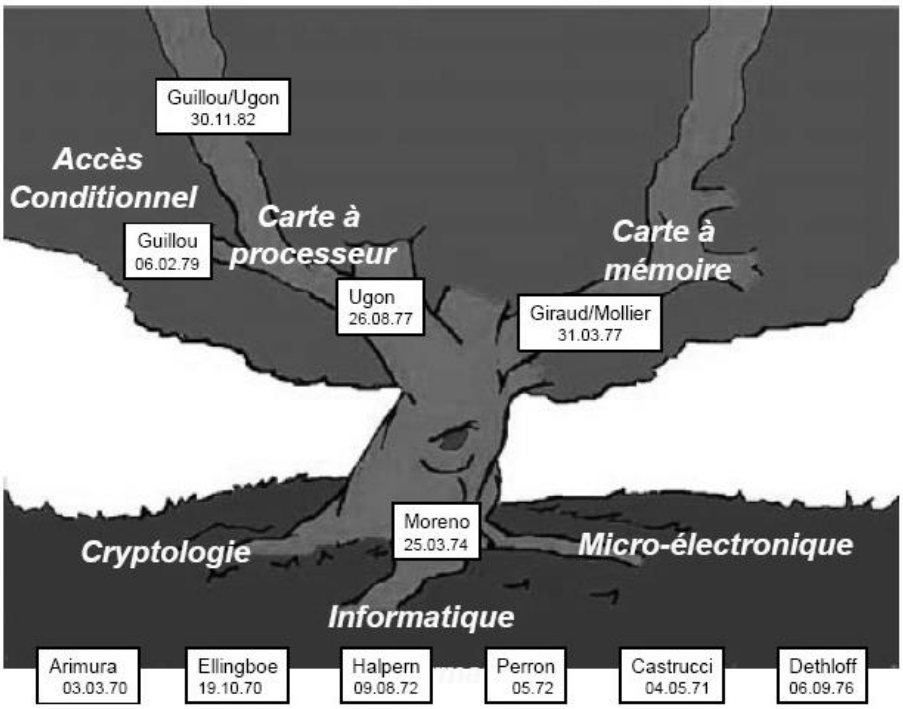


Fig. 2. Généalogie des premiers brevets de cartes à puce. Illustration J. Moulin.

Après quelques demandes de brevet rejetées pour défaut d'inventivité, le Français Roland Moreno (1945-2012) rencontre Jean Moulin qui lui rédige trois brevets publiés en 1974. Ces trois brevets portent sur l'insertion d'un circuit électronique dans une carte en plastique au format des cartes de crédit, sur la gestion d'un code porteur par le circuit électronique et sur les moyens de couplage du circuit électronique avec le monde extérieur.

Je ne fais la connaissance de Jean Moulin que bien des années plus tard, en 1997. C'est lui qui analyse et établit la généalogie des premiers brevets ; en particulier, il introduit l'arbre décrit en figure 2.

De 1977 à 1979, des brevets de développement établissent trois champs d'application : la carte à logique câblée (Giraud et Mollier en 1977), la carte à microprocesseur (Ugon en 1977) et l'accès conditionnel par carte en radiodiffusion (Guillou en 1979).

Les prémices d'une aventure industrielle

Dès 1975 aux Clayes-sous-Bois, la compagnie CII HB (*CII Honeywell Bull*, 1974-82) consacre des moyens de recherche importants en créant une division pour définir l'architecture des composants et trouver des moyens de réaliser des cartes. La division acquiert une licence des brevets de Roland Moreno. Michel Ugon en assure l'animation technique. C'est en 1978 que je le rencontre pour la première fois. C'est aussi le début d'une fructueuse coopération et d'une grande amitié.

Il faut tout d'abord disposer d'une carte expérimentale pour démontrer le concept, en particulier la coexistence d'une piste magnétique et d'une puce électronique sur la même carte, afin de convaincre les utilisateurs potentiels. Il faut aussi développer les divers éléments des systèmes expérimentaux.

Fruit d'une collaboration entre CII HB et Motorola, la première carte, appelée CP8, apparaît le 21 mars 1979, avec deux composants disponibles sur le marché : un microprocesseur masqué[24], à savoir un CPU 3870 conçu par la société Fairchild et une mémoire programmable électriquement (et effaçable par rayonnement ultraviolet), à savoir une mémoire EEPROM 2716 conçue par Intel.

Cependant, la solution naturelle consiste bien sûr à utiliser une seule puce dans la carte, pour au moins trois raisons : coût, fiabilité et sécurité du produit final. En effet, la fabrication des cartes est plus simple ; le risque de panne est réduit ; et enfin, il n'y a pas de connexions d'une puce à une autre, ce qui évite un accès très facile aux bus reliant l'unité centrale et la mémoire non-volatile programmable électriquement.

C'est en 1977 que Michel Ugon invente l'architecture du composant MAM, c'est-à-dire le Microprocesseur Auto-programmable Monolithique ou SPOM (*Self Programmable One-chip Microprocessor*).

Dans tout composant MAM, l'unité centrale doit contrôler elle-même tous les signaux électriques et logiques à destination de la mémoire non-volatile, programmable électriquement, appelée NVM (*Non-Volatile Memory*) : le MAM contrôle tous les accès en écriture à sa propre NVM. Pour ce faire, des dispositifs de bascule s'interposent entre le bus général du microprocesseur et les accès en adresse et en données à la mémoire NVM, de sorte que les signaux électriques et logiques imposés à la NVM restent stables le temps nécessaire au processus d'écriture alors que le programme continue de se dérouler dans l'unité centrale, ce qui entraîne une évolution des états sur le bus général d'adresse et de données du composant MAM. Cette invention a donné lieu à un brevet de base de Michel Ugon.

[24] Un circuit intégré « masqué » est programmé par les opérations successives de masquage et de traitement d'une galette de silicium à la création même du circuit.

En avril 1981, Motorola produit le premier SPOM – le premier masque est celui du contrôle d'accès à ANTIOPE. En 1985, suscitée par la Mission de la Carte à Mémoire dirigée par Alain Turbat au sein de la Direction Générale des Télécommunications, la société Eurotechnique apparaît en seconde source. En réaction, Motorola produit son second SPOM en 1986. La figure 4 représente de gauche à droite ces trois premiers SPOM. Le monde extérieur doit leur fournir une tension de programmation pour qu'ils écrivent sélectivement dans leur mémoire non-volatile.

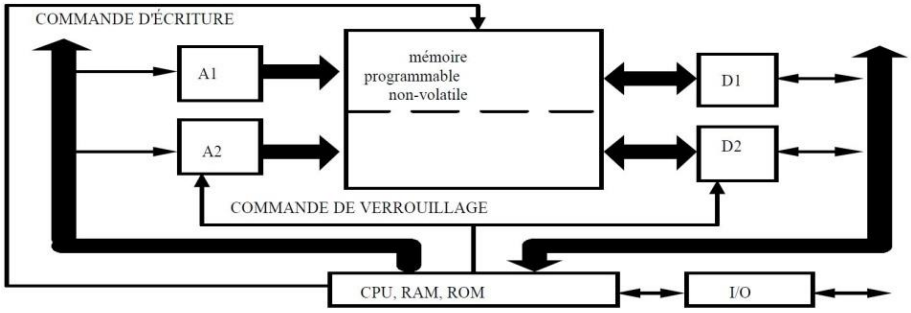


Fig. 3. Schéma MAM / SPOM. Illustration L. Guillou.

Il faut attendre la fin des années 80 pour voir apparaître des circuits dotés d'un dispositif leur permettant de produire en interne les niveaux électriques requis pour écrire dans la mémoire non-volatile (et pour l'effacer).

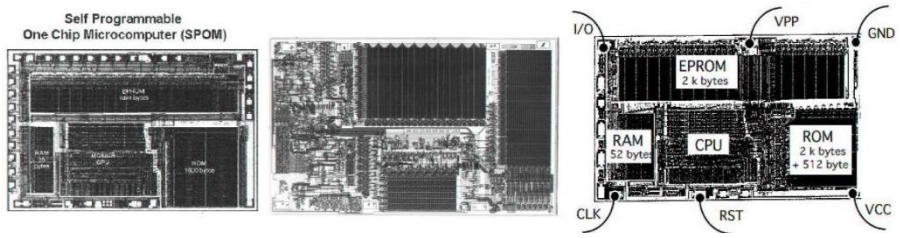


Fig. 4. Les trois premiers composants SPOM. Photographie L. Guillou.

En 1994, vingt ans après les premiers brevets, dix ans après la publication des spécifications bancaires B0, la carte bancaire est une réussite franco-française. On compte alors 22,8 millions de cartes bancaires à puce, pour 2,35 milliards de transactions et un montant de 807 milliards de francs français. Le taux de fraude sur les cartes n'était plus que de 0,035 %

en moyenne. Plus précisément, et c'est intéressant, les cartes françaises utilisées à l'étranger – donc avec la technologie : embossage et piste magnétique – ont un taux de fraude de 0,2 %, et celles utilisées en France – donc avec la technologie puce – un taux de fraude de 0,032 %. Ces deux taux indiquent que la technologie puce divise le taux de fraude par sept environ par rapport à la technologie précédente : embossage et piste magnétique.

Les prémices de la radiodiffusion à péage

Le 20 mars 1978, le décret n° 78379 paraît au *Journal Officiel de la République Française* : il aménage le monopole de radiodiffusion. Pour ma part, je travaille depuis février 1973 au CCETT (Centre Commun d'Etudes de Télédiffusion et de Télécommunication) à Rennes, pour le compte de l'ORTF (Office de Radiodiffusion Télévision Française), puis de TDF (TéléDiffusion de France) à partir de janvier 1975.

L'aménagement du monopole de radiodiffusion ouvre la voie à la radiodiffusion à péage. Ma toute première maquette de dispositif d'accès conditionnel aux services audiovisuels est un kit de développement Intel SDK qui pèse environ sept kilos ; il est accompagné d'un dispositif d'alimentation tout aussi pesant et volumineux. Mais je sais qu'un seul microprocesseur peut réaliser tout ce que fait la volumineuse maquette.

Ma hiérarchie me conforte dans l'idée d'utiliser la carte à puce. En février 1979, je dépose trois demandes de brevets d'invention en contrôle d'accès appliqué au télétexte diffusé ANTIOPE ; aujourd'hui, ce sont les brevets de base en radiodiffusion à péage par carte à puce.

En mars 1979, un laboratoire « Cryptologie et Accès aux Services » est créé au sein des laboratoires TDF du CCETT et j'en suis le responsable avec pour mission de développer un système de contrôle d'accès par carte à puce.

En parallèle, TDF développe un autre système dans un autre laboratoire à Issy-les-Moulineaux avec une technologie « éprouvée » : la carte à piste magnétique ; il vaut toujours mieux avoir deux fers au four.

En 1979, je conçois une maquette à six contacts et deux composants : une mémoire Intel 2716 et un microprocesseur Intel 8748, montés sur les deux faces d'un petit circuit imprimé. En technologie EEPROM, ces deux circuits sont effaçables par rayonnement UV (fonction inutilisée dans la maquette) à travers les fenêtres transparentes sur les deux circuits[25]. Grâce à la maquette, nous développons tous les autres éléments du système d'accès conditionnel sans attendre les cartes définitives.

[25] Voir la figure 5.

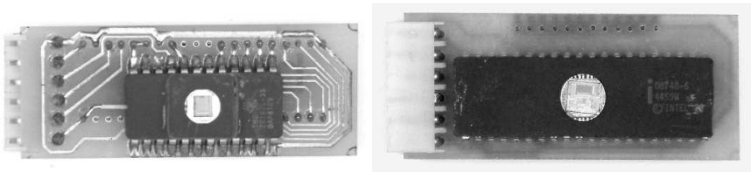


Fig. 5. Recto et verso de la maquette à six contacts du CCETT.
Photographie L. Guillou.

La différence entre la carte à deux puces de CII HB et la maquette du CCETT réside dans le microprocesseur : programmé par les masques successifs à la production d'une série de circuits intégrés pour CII HB, et programmé électriquement à l'unité pour le CCETT. Avec la solution CII HB, on produit quelques milliers de puces à la fois alors qu'on change le programme d'une maquette CCETT à l'autre.

Durant l'été 1980, la Direction de TDF me fait savoir qu'elle envisage une démonstration au plus haut niveau de l'Etat. La maquette à deux puces est insuffisante. Il faut absolument montrer une carte à puce.

Pour y parvenir, je programme un microprocesseur Intel 8748 avec clés et algorithmes et j'entreprends d'extraire le composant de son boîtier DIL (*Dual In Line package*) avant de le coller sur un support de contacts et de le câbler pour en faire une carte. Je m'aperçois que dans le boitier DIL, la puce de silicium est soudée à son support par un eutectique[26] or-silicium ayant une température de fusion de 429° Celsius. Nous brisons quelques puces, mais après quelques péripéties, nous extrayons enfin une puce intacte portant clés et algorithmes. Finalement en novembre 1980, la toute première carte à une seule puce est au point. Dépourvue de toute fonctionnalité d'écriture, cette carte permet de montrer l'essentiel : la fonction de contrôle d'accès.

Malheureusement, Monsieur le Président de la République de l'époque, Valéry Giscard d'Estaing, est, à juste titre, plus préoccupé par sa réélection qui semble devenir de plus en plus problématique. La direction de TDF maintient la pression en m'annonçant une démonstration à Monsieur le Premier Ministre pour Janvier 1981 ; malheureusement le Premier Ministre de l'époque, Raymond Barre, ne vient pas non plus : un autre acte manqué ! Une visite à ce niveau aurait ancré à Rennes toutes les activités ultérieures en matière de cartes à puce !

En avril 1981, Motorola produit le tout premier SPOM avec pour premier masque le contrôle d'accès à ANTIOPE. Ces premiers SPOM sont montés dans des cartes par la division de CII HB aux Clayes-sous-Bois. Devenue

[26] NdE. : un eutectique est un mélange de deux corps – ici or et silicium – qui se comporte comme un corps pur du point de vue de sa fusion : sa température de fusion est constante.

ainsi inutile, la toute première carte à une seule puce sert de cobaye pour démontrer que l'on peut en extraire la puce sans la détruire : la figure 6 montre les débris de cette carte avec une puce toujours en état de marche.

De l'invention au stade expérimental, l'idée de Moreno germe ainsi pour l'accès conditionnel sous l'impulsion de CII HB et du CCETT.

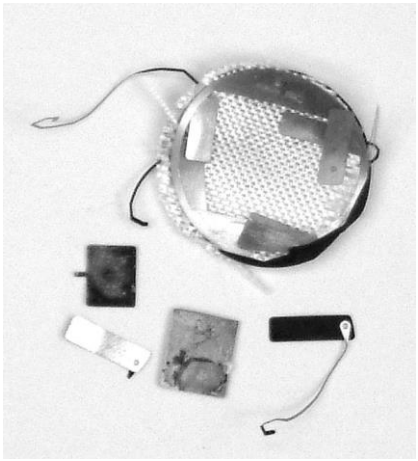


Fig. 6. Les débris de la toute première carte à une seule puce.
Photographie L. Guillou.

Normalisation Européenne de l'accès conditionnel

De 1983 à 1987, les premiers travaux de normalisation en matière d'accès conditionnel sont réalisés dans le cadre de l'UER/EBU (Union Européenne de Radiodiffusion / *European Broadcasting Union*).

A partir de contributions du CCETT, ces normes établissent un vocabulaire et une architecture schématisés en figure 7 et repris ultérieurement de 1992 à 1996 dans le cadre du projet européen EP-DVB (*Digital Video Broadcasting*).

Périodiquement, à intervalles de une à dix secondes, l'émetteur tire au hasard un nouveau mot de contrôle (*Control Word*, CW) et calcule un message de contrôle de titre d'accès (*Entitlement Control Message*, ECM) grâce auquel la carte contrôle les critères d'accès indiqués et recalcule CW à l'aide d'une clé d'exploitation.

Chaque message de gestion de titre d'accès (*Entitlement Management Message*, EMM) permet de gérer des titres d'accès en adressant chaque carte individuellement ou bien par petits groupes de cartes. Chaque titre

d'accès est composé de droits d'accès associés à une ou plusieurs clés d'exploitation.

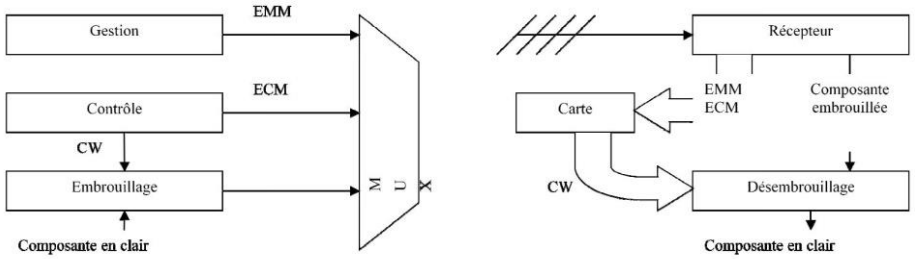


Fig. 7. Schéma de principe de l'accès conditionnel. Illustration L. Guilou.

Consultation du NBS sur l'usage de chiffres à clé publique dans des cartes

En 1982, le NBS lance une consultation sur l'usage de chiffres à clé publique dans des cartes à puce. Le CCETT répond conjointement avec la compagnie CII HB à cette consultation. Notre proposition consiste à utiliser la technologie RSA sur des cartes à puce.

À cette occasion, je formalise dans le détail tous les programmes de ma bibliothèque en Fortran pour créer des jeux de clés RSA et pour effectuer diverses opérations : chiffrer et déchiffrer, ou bien, signer et vérifier.

Ce travail me permet aussi d'obtenir deux brevets sur la mise en œuvre de chiffres à clé publique sur des cartes à puce, dont un brevet en commun avec Michel Ugon.

Les premières expérimentations bancaires

De 1982 à 1984, trois expériences IPSO éprouvent la fiabilité de cartes bancaires à puce utilisées par le grand public sur des terminaux installés chez des commerçants. Chaque expérience inclut 750 terminaux et 125 000 cartes sur chacun des trois sites : Blois avec la compagnie CII HB, Caen avec la société Philips, et Lyon avec la société Flonic-Schlumberger.

Parallèlement aux expériences IPSO, les parties élaborent en commun les spécifications bancaires B0 publiées en janvier 1984 à Paris.

En la personne de Daniel Le Rest, le CCETT a largement pris part à l'élaboration des spécifications B0 en définissant l'interface des cartes : positions des contacts, signaux électriques sur les contacts, protocole

d'échange sur le contact d'entrée/sortie, contenu des commandes et des réponses.

Les spécifications bancaires B0 définissent un procédé d'authentification statique de chaque carte bancaire. C'est la toute première utilisation du RSA.

En août 1983 au CCETT, une machine MAGNOLIA produit trois nombres composés de 321 bits (97 chiffres décimaux), encore appelés « modules » :

– un module de test N_0 dont les facteurs figurent dans la publication B0 :

N_0 = 2 135 987 035 920 910 082 395 023 041 766 080 254 575 657 763 181 686 108 819 565 004 674 139 649 668 169 447 504 285 319 719 057

– un module opérationnel N_1 dont les facteurs, gardés secrets, furent utilisés sur les chaînes d'émission de cartes par un dispositif CAMELIA (semblable à la maquette de la figure 5 noyée dans un bloc de résine de protection) pour signer l'identité de chaque carte bancaire :

N_1 = 2 135 987 035 920 910 082 395 022 704 999 628 797 051 095 341 826 417 406 442 524 165 008 583 957 746 445 088 405 009 430 865 999

– et enfin un module de secours N_2 au cas où il arriverait un problème à N_1 :

N_2 = 2 135 987 035 920 910 082 395 023 167 061 454 287 154 982 970 333 788 538 980 157 785 000 915 339 815 349 436 815 313 646 352 671

J'avais annoncé et écrit que les nombres bancaires N_1 et N_2 résisteraient de cinq à dix ans. Mais ils ont été utilisés quinze ans sans être remplacés par des nombres plus longs.

En novembre 1998, Serge Humpich[27] (né en 1963) dévoile la décomposition de N_1, un secret de l'émission des cartes bancaires :

N_1 = 1 917 481 702 524 504 439 375 786 268 230 862 180 696 934 189 293 × 1 113 954 325 148 827 987 925 490 175 477 024 844 070 922 844 843

En fait, dès 1996, Henri Cohen (né en 1947), professeur à Bordeaux et partie prenante au développement des programmes d'Arjen Lenstra, décompose N_1 ; il en informe alors la direction du GIE CB. Voici comment j'ai deviné cette information jamais divulguée. En 1982, j'appelle Henri Cohen à l'aide en matière de théorie des nombres et d'arithmétique ; mon

[27] Cet événement a fait grand bruit, sous le nom d'« affaire Humpich ». À 35 ans, Serge Humpich, développeur informaticien en finance, à partir d'un simple PC et d'un logiciel japonais de factorisation, est parvenu à factoriser N_1. Et il a tenté en vain de négocier son savoir-faire auprès du GIE CB. Humpich a dévoilé la vulnérabilité du système en retirant publiquement un carnet de tickets de métro au moyen d'une carte de sa fabrication. En 2000, il est condamné à dix mois de prison avec sursis pour « falsification de cartes bancaires et introduction frauduleuse dans un système automatique de traitement ».

appel se solde par une fin de non-recevoir ; Henri est horrifié d'imaginer un usage pratique de l'arithmétique et de la théorie des nombres, la seule science jusqu'alors sans aucun intérêt pratique et économique, déesse courtisée uniquement pour son esthétique et sa beauté ! En 2002, il me demande : « Louis, vous souvenez vous de notre échange téléphonique il y a vingt ans ? » Il ajoute : « J'ai mis quinze ans à me rendre compte que vous aviez raison ».

Ainsi, Humpich a simplement enfoncé la porte ouverte par Cohen. Si la taille du module avait été doublée en 1996, il n'y aurait pas eu de problème. Mais les décideurs du GIE CB n'ont pas tenu compte de ma mise en garde.

En août 2000, François Morain, cryptologue émérite, alors responsable du LIX (Laboratoire d'Informatique de l'Ecole Polytechnique), constate qu'une grappe de 12 PC à 450 Mhz décompose en 12 heures chacun des trois modules N_0, N_1 et N_2 :

N_0 = 592 010 126 613 262 808 346 694 724 347 523 172 057 668 549 003
× 3 608 024 491 304 466 049 410 093 287 681 814 632 309 971 096 019

N_1 = 1 917 481 702 524 504 439 375 786 268 230 862 180 696 934 189 293
× 1 113 954 325 148 827 987 925 490 175 477 024 844 070 922 844 843

N_2 = 657 014 177 716 226 106 458 166 827 072 087 004 714 316 600 391
× 3 251 051 664 281 548 687 178 946 882 180 534 839 889 205 631 081

Rappelons que la spécification B0 publie la factorisation de N_0 en janvier 1984 et Humpich celle de N_1 en novembre 1998. La nouveauté ici est donc la factorisation de N_2 dont la mésaventure mérite d'être rapportée. À Paris lors d'un des nombreux déménagements du Groupement de la Carte à Mémoire puis de son successeur, le Groupement de la Carte Bancaire (GIE CB), une femme de ménage zélée met à la poubelle les facteurs premiers secrets de N_2 dissimulés dans une caisse en carton ! En 1984, ce genre de secret ne fait encore l'objet d'aucune procédure pratique de sauvegarde.

Une procédure pratique de sauvegarde d'un secret

Dans le cadre de l'ETSI en 1995, on crée ETSI-1024, un module de 1024 bits produit de deux grands facteurs premiers, pour l'authentification de matériels d'exploitation de contrôle d'accès en DVB. Ce nombre joue pour le DVB un rôle similaire aux modules des cartes bancaires. Le petit facteur premier d'ETSI-1024 est partagé selon une méthode due à Shamir.

Deux trains de 521 bits sont pris au hasard ; ils constituent deux nombres

a et *b* inférieurs à $2^{521} - 1$ (un nombre premier de Mersenne[28]) ; le nombre *c* est le secret à partager, au plus 512 bits ; *a*, *b* et *c* définissent une courbe du second degré : $y = ax^2 + bx + c \mod 2^{521} - 1$. Les quatre parts sont les valeurs de l'ordonnée à chacune des abscisses 1, 2, 3 et 4. Chaque part est un nombre représenté par un train de 521 bits remis dans une enveloppe scellée à quatre gardiens choisis d'un commun accord pour un an.

Toutes les valeurs du secret sont possibles avec une ou même deux parts. Trois parts, n'importe lesquelles parmi les quatre, restituent le secret, à savoir, l'ordonnée pour l'abscisse 0 par interpolation de Lagrange.

Chaque année, l'ETSI convoque une réunion : chaque gardien y apporte son enveloppe. On vérifie l'intégrité des sceaux ; quatre fois, on rétablit un train de 512 bits codant un nombre qui divise ETSI-1024 si les conditions de conservation sont adéquates ; on détruit les quatre parts ; on tire au hasard deux trains de 521 bits pour établir quatre nouvelles parts remises dans quatre nouvelles enveloppes scellées à quatre gardiens nommés pour un an.

Mon rôle en normalisation à l'ISO

Dès la création des groupes de travail concernés au tout début des années quatre-vingt à l'ISO (*International Organisation for Standardisation*, Organisation Internationale de Normalisation), je prends part à la normalisation dans deux domaines : cartes à puce et techniques de sécurité. Voici les dernières versions de quatre normes dont j'ai assuré l'édition :

– À l'ISO/IEC JTC 1/SC17 : Cartes à circuit intégré, WG4 : Cartes à contacts, deux normes qui assurent la pérennité du développement de cartes à puce :

• ISO/CEI 7816-3:2006, *Cartes d'identification à circuit intégré*, Partie 3 : *Interface électrique et protocoles de transmission*,

• ISO/CEI 7816-4:2005, *Cartes d'identification à circuit intégré*, Partie 4 : *Organisation, sécurité et commandes pour les échanges*.

– À l'ISO/IEC JTC 1/SC27, Techniques de sécurité, WG2, Mécanismes, deux normes qui comprennent les schémas RSA, GQ1 et GQ2 :

• ISO/CEI 9798-5:2004, *Authentification d'entité*, Partie 5 : *Mécanismes*

[28] Marin Mersenne (1588-1648), moine français, a laissé son nom à une famille de nombres premiers. Par définition, tout nombre premier de la forme 2^n-1 est un nombre de Mersenne. Les plus grands nombres premiers connus sont des nombres de Mersenne. La découverte du 48ième nombre de Mersenne, $2^{57\,885\,161}-1$, date de janvier 2013 : http://www.mersenne.org.
En 1951 à l'université de Manchester, Turing teste son ordinateur avec des nombres de Mersenne. Si un long calcul donne le résultat attendu, c'est que la mémoire vive est fiable dans les conditions du test : http://primes.utm.edu/mersenne/LukeMirror/lit/lit_024s.htm. Voir le chapitre « L'ancrage de la cryptologie dans les jeux d'écriture » p. 47 et le chapitre « Cryptographie et théorie des nombres » pp. 256-258.

utilisant des techniques à divulgation nulle,
• ISO/CEI 14888-2:2008, *Signatures numériques avec appendice*, Partie 2 : *Mécanismes basés sur une factorisation entière*.

UNE TENTATIVE AVORTEE DE MISE A MORT DE LA CARTE A PUCE

En 1992, Gustavus J. Simmons[29] (né en 1930) assure l'édition d'un ouvrage collectif sur la cryptologie, *Contemporary Cryptology*, *The Science of Information Integrity*, publié par les presses de l'IEEE. À sa demande expresse, un chapitre de cet ouvrage porte sur la carte à puce ; j'ai rédigé ce chapitre avec Michel Ugon et Jean-Jacques Quisquater.

Dans la préface, Simmons fait l'éloge de la carte à puce, affirmant qu'elle « [mettra] un instrument sophistiqué, dédié à l'intégrité de l'information, dans la poche de pratiquement chaque personne dans le monde, et [sera] probablement l'application la plus répandue jamais réalisée de schémas cryptographiques »[30]. Je pense que cette phrase-là a eu une importance considérable dans la suite des évènements – étant donnés la renommée de l'éditeur et l'impact de l'ouvrage – et qu'elle a induit une attaque physique des puces de carte, suivie d'une vague de piratage de la télévision à péage, avec pour objectif la destruction de l'industrie naissante de la carte à puce.

Piratage en télévision à péage par cartes à puce

L'été 1993 voit s'épanouir une multiplicité de cartes pirates contre des opérateurs européens de télévision à péage par satellite : en juillet contre BSkyB (*British Sky Broadcasting*), opérateur britannique au Royaume-Uni ; en août contre *Interaccess*, opérateur suédois en Scandinavie, puis, en septembre contre *Filmnet*, opérateur hollandais au Bénélux. BSB utilise une technologie développée par *News Datacom*. *Interaccess* et *Filmnet* utilisent une technologie développée au CCETT et commercialisée par *Viaccess*, branche de France Telecom alors dirigée par Jean-Pierre Coustel.

Au CCETT, avec Pierre Février et son équipe, nous nous retrouvons en première ligne pour expertiser environ 200 cartes pirates pendant les deux années suivantes. Les cartes d'août et de septembre portent une seul clé d'exploitation : soit pour *Interaccess*, soit pour *Filmnet*.

---

[29] Simmons dirige alors le département de mathématiques appliquées aux *Sandia National Laboratories* à Albuquerque au Nouveau Mexique.

[30] « *This application (smart card) will put a sophisticated information-integrity device in the wallet or purse of practically every person in the industrialized world, and will therefore probably be the most extensive application ever made of cryptographic schemes* ».

Mais outre des clés d'exploitation – clés qui servent périodiquement à recalculer les mots de contrôle pour mettre en clair des composantes du signal de télévision –, la technologie *Viaccess* utilise aussi des clés de gestion qui servent à gérer les titres d'accès dans les cartes des usagers : chaque titre d'accès est constitué de clés d'exploitation et de droits d'accès associés. Il y a donc deux niveaux hiérarchiques de clés.

La carte elle-même ne sait pas à quoi servent les clés qu'elle porte, c'est uniquement l'adressage des cartes et le contenu des messages (ECM et EMM) qui permettent à la carte d'utiliser la clé appropriée. À un moment donné pour un service donné, la clé d'exploitation en usage est la même dans toutes les cartes, alors que d'une carte à l'autre, ou d'un petit groupe de cartes à l'autre, chaque clé de gestion est fonction du numéro de série de la carte.

Je donne alors un bon coup de pied dans la fourmilière des pirates en changeant la clé d'exploitation d'*Interaccess* en septembre 1993, puis celle de *Filmnet* en octobre. Les usagers normaux ne se rendent compte de rien. Mais les utilisateurs de cartes pirates sont en panne. Les distributeurs de cartes pirates pestent contre les ingénieurs de *Viaccess* qui se permettent de changer de clé sans les prévenir ! Ils assurent leurs clients qu'ils font tout leur possible pour restaurer le service au plus tôt ! En réaction, de nouvelles cartes pirates apparaissent avec toutes les clés à la disposition des pirates.

Dès qu'une clé de gestion apparaît dans une carte pirate analysée au CCETT, Pierre Février utilise un dispositif carte-mère pour restituer le numéro de série de la carte violée dont l'exploitant donne alors l'historique. Je détecte d'abord une carte *Interaccess* délivrée à Stockholm en fin 1992. Ensuite je détecte une carte *Filmnet* activée le 18 janvier 1993 et mise en liste noire le 30 mars 1993. À Bruxelles, un individu donne une fausse adresse et ne paye pas son abonnement : l'intention de nuire est patente.

Je constate que jusqu'en 1996, les clés de gestion dans les cartes pirates proviennent d'une seule carte *Interaccess* et d'une seule carte *Filmnet*, ce qui signifie qu'à ce moment-là, tous les pirates européens sont alimentés par un seul violeur. Ces deux cartes portent la même puce de Motorola. Les cartes BSkyB portent une autre puce de Motorola.

Toutes les puces de Motorola présentent la même spécificité qui impacte la fabrication des circuits intégrés. Lorsqu'une puce est déclarée valide sur une galette de silicium, un fusible est détruit afin de passer définitivement (en principe) la puce du mode test au mode actif. En mode test ou plutôt en mode émulateur, la mémoire de la puce est entièrement accessible.

Cependant à Grenoble, une équipe spécialisée du CNET (Centre National d'Etudes des Télécommunications) extrait tout d'abord la puce d'une carte active puis parvient assez aisément à « ressusciter » le fusible, ce qui ramène la puce en mode test, pour lire toute la mémoire, c'est-à-dire l'ensemble des programmes et des clés figurant dans la carte ainsi violée.

Je soupçonne que le violeur est la NSA motivée par la « prophétie » de Gustavus Simmons et ses grands coups d'encensoir envers la carte à puce. Cependant, tout le monde ne partage pas mon analyse : certains soupçonnent les organismes bancaires *Visa* et *Mastercard*. Quoiqu'il en soit, il faudra attendre longtemps pour analyser les archives correspondantes et éclaircir le mobile du crime.

Actions de normalisation impliquant des cartes à puce

En 1982 au tout début de mes activités en normalisation, Yves Guinet, mon chef à l'époque, me dit : « Tu sais, Louis, si une norme s'établit sans aboutir au mouton à cinq pattes, c'est que le produit n'a aucun avenir commercial ». Considéré comme sans avenir, la norme n'intéresse ni les hiérarchies ni leurs stratèges ; les ingénieurs travaillent tranquillement, sans pression, puisque le résultat doit ne servir à rien.

De 1993 à 1996, l'ETSI (*European Telecommunications Standards Institute*) élabore des normes GSM (*Global System for Mobile*) pour la téléphonie mobile et l'Union Européenne des normes DVB pour la télévision numérique par satellite. Fin 1996, ces deux applications européennes émergentes couvrent vingt millions de téléphones mobiles GSM, chacun avec une carte SIM (*Subscriber Identity Module*), et quinze millions de décodeurs TV à péage, chacun avec une carte à puce ou une clé.

Durant l'élaboration des normes DVB et GSM, aucune pression ne s'exerce sur le résultat des discussions techniques, à part quelques pressions sur la cryptographie embarquée. Fort heureusement à l'époque, les diverses entités aujourd'hui impliquées dans l'industrialisation des matériels GSM et DVB et dans l'exploitation des systèmes correspondants ou bien n'existent pas encore, ou bien ne croient pas à l'imminence du succès. En 1995, on pense qu'il faudra de dix à quinze ans pour développer des circuits intégrés économiquement viables pour les téléphones mobiles et pour les récepteurs de télévision numérique.

En 1996, deux spécifications mondiales prometteuses sont publiées : en juin, la norme EMV '96 élaborée par *Europay*, *Mastercard* et *Visa* pour la carte bancaire à puce, puis en décembre, la norme PC/SC élaborée par *Bull CP8*, *HP*, *Microsoft*, *Schlumberger*, *Siemens*, *Nixdorf*, pour interfacer la carte à puce sur un ordinateur personnel.

Le sauvetage de la carte à puce par la téléphonie mobile

En 1994, la production mondiale de composants SPOM est 30 millions dont la moitié pour les cartes bancaires françaises : le succès est hexagonal. En 1997, la production passe à 375 millions : le succès est européen.

En extrapolant ces chiffres, on prévoit en 1997 un succès mondial avec une production de 1 à 2 milliards pour 2000. Et patatras ! Grave déconvenue, la production n'est que 541 millions en 2000.

Cependant en 2000, contrairement aux prévisions de nos hiérarchies et de nos stratèges, des circuits intégrés économiquement viables sont disponibles en masse pour GSM et DVB.

Ventilons quelques volumes de production en millions de SPOM publiés chaque année par l'association *Eurosmart* :

	2000	2005	2006
Téléphonie mobile	370	1 310	1 650
Secteur bancaire	120	330	400
TV à péage	25	60	85
Gouvernement, santé	20	60	60
Transports	3	25	25

Sans la téléphonie mobile, la carte à puce aurait bel et bien été anéantie, car je ne vois pas comment la jeune industrie aurait pu subsister en 2000 avec une production passant de 375 millions en 1997 à 170 (= 540 – 370) millions en 2000, c'est-à-dire divisée par un peu plus de deux.

Dès 2000, la carte à puce a définitivement échappé au pire. Personne n'avait prévu le boom du téléphone mobile, pas même les assassins de l'ombre qui ont tenté sans succès de tuer la puce dans l'œuf.

Le taux de croissance annuelle est 36 % en 2000 pour un volume de 541 millions de SPOM, 25 % en 2005 pour 1 812 millions. La progression se poursuit : 2 220 millions en 2006. Les dernières prévisions d'Eurosmart sont 6 970 millions en 2012 et 7 595 millions en 2013. Ainsi la prophétie de Gus Simmons se réalise au-delà de toutes les espérances : la cryptologie avec la carte à puce envahit notre vie courante.

Faite en 1997, la prévision de production de puces pour cartes pour l'an 2000 se réalise en 2005 avec cinq ans de retard. Mais en affaiblissant l'Europe et les États-Unis, le délai de cinq ans offre à la Chine l'opportunité d'établir une activité industrielle conséquente en puces et en cartes (je pense qu'*Eurosmart* ne répertorie pas l'activité chinoise). Ce n'était sans doute pas

le but recherché par les apprentis sorciers qui à travers leur attaque, ont vainement tenté d'étouffer la carte à puce dans l'œuf.

BILAN : MON ANALYSE

Les années 1973-1983 voient s'établir la cryptologie non classifiée et le microprocesseur, deux technologies apparemment indépendantes entrainant en France l'apparition d'une activité notable en matière de carte à puce.

Les années 1984-1994 voient s'établir en Europe un processus industriel fiable pour produire des télécartes pour cabines publiques téléphoniques dans les sociétés *Oberthur*, *Solaic*, *Schlumberger*, et enfin *Gemplus* en 1991.

Alors que les années 1994-1996 voient s'élaborer en Europe des normes pratiques et réalistes en téléphonie mobile et en télévision numérique, elles voient se développer aux États-Unis un projet « *Clipper Chip* » visant à introduire une puce de sécurité fixe dans chaque téléphone. On y parle aussi beaucoup d'un autre projet visant à sceller une puce de sécurité dans chaque ordinateur personnel. Ces deux projets ont lamentablement avorté. Ce sont deux antithèses de la carte à puce.

À la fin du vingtième siècle, réalisant leur erreur d'évaluation, le Japon et les États-Unis développent chacun leur propre norme nationale de téléphonie mobile en espérant prendre ainsi la norme GSM à contrepied. Que de complications pour téléphoner alors depuis ces deux pays ! Ces deux normes ont également lamentablement échoué.

Motorola figure au nombre des dommages collatéraux de toutes ces manigances. Bien que venant de beaucoup investir dans son usine d'East Kilbride près de Glasgow en Ecosse, Motorola jette l'éponge : continuer impliquerait de reconcevoir complètement la sécurité de ses puces pour cartes, ainsi que leur processus de fabrication et de test. En matière de production de puces pour cartes, Motorola se retrouve tout à coup rétrogradé du rang de leader mondial à celui de débutant. Je soupçonne que les assassins de l'ombre leur suggèrent alors de ne pas insister et de laisser tomber cette activité vouée selon eux à une disparition précipitée.

Motorola confie alors son activité « carte à puce » à la société Atmel à Colorado Springs qui met l'activité en sommeil ; Atmel est le producteur pressenti (et malchanceux) du fameux « *Clipper Chip* ».

Depuis 1996, *Visa* et *Mastercard* promettent invariablement que, d'ici deux ans, toutes les cartes bancaires du monde seront à puce : est-ce une manière de tenir une promesse que de la répéter invariablement chaque année ? La réalisation d'une telle promesse implique un nouveau modèle commercial (*business model*). Un tel changement relève de décisions politiques au plus haut niveau mondial (G7 ou G20). En ces temps de crise, l'intérêt de la société devrait prévaloir face au gaspillage engendré par

l'intérêt à court terme de deux organisations vieillissantes. Pour la carte à puce au niveau mondial, le secteur bancaire reste faible relativement aux autres ; gardons-nous de continuer à confondre carte à puce et carte bancaire.

Soulignons la persévérance du GIE CB (groupement de la carte bancaire) en France : contre vents et marées, c'est-à-dire malgré *Visa* et *Mastercard*, leur rôle a été et est encore très important. Ce sont bien eux qui ont raison : l'exception française des débuts devient peu à peu la règle mondiale.

La carte SIM joue un rôle crucial dans le succès du téléphone mobile : ce produit « doré » concentre toutes les actions commerciales de l'opérateur, le téléphone mobile restant un produit « brun », c'est-à-dire grand public. Si la carte à puce n'avait pas été disponible, la téléphonie mobile aurait été très handicapée. À la fin du vingtième siècle, se sentant une vocation d'alchimiste moderne d'un nouveau genre, certains fabricants de téléphones mobiles cherchent à transmuter en or leurs produits bruns : dans le processus de normalisation de l'interface de la carte à puce à l'ISO, je dois alors désamorcer une ultime tentative désespérée de déstabilisation.

L'évolution technologique aurait très bien pu être tout autre durant ces vingt dernières années ; l'imprévisibilité de l'évolution va se poursuivre pour les vingt ans à venir. Avec en filigrane, le conflit larvé entre le respect de la vie privée et certaines agences de sécurité épiant tous les systèmes de communication, les affrontements resteront particulièrement visibles, voire violents, dans deux domaines : le téléphone mobile et l'ordinateur personnel sur Internet.

En 1994-1996, aux dires de certains apprentis sorciers, l'Europe se serait amusée à produire des normes ETSI et DVB « sans avenir » selon eux à l'époque. Aujourd'hui, à travers le succès de ces nouvelles technologies, l'Europe s'avère être un vrai empêcheur de tourner en rond ; le complexe « NIH » (*Not Invented Here*) a bon dos. Pour tenir son rang, l'Europe se doit donc de renforcer au plus tôt son efficacité politique. Méfions-nous : ce ne sont pas toujours les mêmes qui perdent.

BIBLIOGRAPHIE

Cocks, C. C., « A Note on Non-Secret Encryption », 1973, http://www.fi.muni.cz/usr/matyas/lecture/paper2.pdf.

Diffie, W. et Hellman, M. E., « New Directions in Cryptography », *IEEE Transactions on Information Theory*, November 1976, vol. IT-22, n° 6, pp. 644-654.

— « Privacy and Authentication: an Introduction to Cryptography », *Proceedings of the IEEE*, mars 1979, vol. 67, n° 3, pp. 397-427.

Ellis, J. H., « The Possibility of Secure Non-Secret Encryption », 1970, http://cryptocellar.web.cern.ch/cryptocellar/cesg/possnse.pdf.

— « The Story of Non-Secret Encryption », 1987, http://cryptocellar.web.cern.ch/cryptocellar/cesg/ellis.pdf.

Feistel, H., « Cryptography and Computer Privacy », *Scientific American*, 1973, vol. 128, n° 5, pp. 15-23.

Fisher, M. J., Micali, S. et Rackoff, C., « A Secure Protocol for the Oblivious Transfer », *Journal of Cryptology*, 1996, vol. 9, n° 3, pp. 191-195.

Gardner, M., « Mathematical Games: A New Kind of Cipher that Would Take Millions of Years to Break », *Scientific American*, 1977, vol. 237-38, pp. 120-124.

Goldwasser, S., Micali, S. et Rackoff, C., « Knowledge Complexity of Interactive Proofs », *Proceedings of the 17th Symposium on Theory of Computing*, Providence, Rhode Island, May 6-8, 1985, *Association for Computing Machinery*, New York, 1985, pp. 291-304.

— « The Knowledge Complexity of Interactive Proof Systems », *SIAM Journal on Computing*, February 1989, vol. 18, n° 1, pp. 186-208.

Guillou, L. C., « Smart Cards and Conditional Access », *Advances in Cryptology: Proceedings of EUROCRYPT '84*, (eds.) T. Beth, N. Cot and I. Ingemarsson, *Lecture Notes in Computer Science*, Springer Verlag, 1985, n° 209, pp. 480-489.

— « Histoire de la carte à puce du point de vue d'un cryptologue », *Actes du septième colloque sur l'histoire de l'informatique et des transmissions*, Rennes-Cesson, 2004, pp. 126-154.

Guillou, S., Guillou, G., Guillou, A., Guillou, G., Guillou, M.-A., Guillou, L., C., Quisquater, M., Quisquater, M., Quisquater, M., Quisquater, J.-J., et Berson, T., A., « How to Explain Zero-Knowledge Protocols to your Children », *Proceedings of Crypto '89*, Santa Barbara, California, August 20-24, 1989. *Advances in Cryptology: CRYPTO '89*, (ed.) Gilles Brassard, *Lecture Notes in Computer Science*, New York, Springer Verlag, 1990, vol. 435, pp. 628-631.

Hellman, M. E., « The Mathematics of Public-Key Cryptography », *Scientific American*, august 1979, vol. 241, n° 2, pp. 146-157.

Rivest, R. L., Shamir A. et Adleman L., « Technical Memo 82 », *M.I.T. Laboratory for Computer Science*, April 1977.

— « A Method of Obtaining Digital Signatures and Public-Key Cryptosystems », *Communications of the ACM*, 21, february 1978, vol. 221, pp. 120-126.

Shannon, C. E., *Collected Papers of C.E. Shannon*, (eds.) Sloane N. J. A., Wyner A. D., New York, IEEE Press, 1993.

— « A Mathematical Theory of Communication », *The Bell System Technical Journal*, july-october 1948, vol. 27, pp. 379-423 et 623-656, *in*

Shannon's Collected Papers, pp. 5-82.
— « Communication Theory of Secrecy Systems », *The Bell System Technical Journal*, 1949, vol. 28, pp. 656-711, *in Shannon's Collected Papers*, pp. 656-711.
Simmons, G. J. (ed.), *Contemporary Cryptology: Cryptology, the Science of Information Integrity*, Piscataway, IEEE Press, 1992.
Williamson, M., J., « Non-Secret Encryption Using a Finite Field », 1974. www.cesg.gov.uk/publications/Documents/secenc.pdf.
— « Thoughts on Cheaper Non-Secret Encryption », 1976. http://cryptocellar.web.cern.ch/cryptocellar/cesg/cheapnse.pdf.

CRYPTOGRAPHIE ET THEORIE DES NOMBRES : QUELQUES REMARQUES SUR LA MEMOIRE D'UNE RENCONTRE

Catherine GOLDSTEIN[1]

Le codage de messages afin qu'ils ne soient pas lus par des indésirables est attesté depuis plusieurs millénaires. Le développement spécifique de mathématiques complexes pour effectuer ces codages, la mise en place de formations universitaires entièrement orientées sur la cryptographie, en revanche, n'ont que quelques décennies. Cette double chronologie rend particulièrement difficile la compréhension des dynamiques en jeu dans l'établissement de la cryptologie[2] mathématique comme discipline propre. Certains phénomènes peuvent être étirés sur le long terme, comme l'usage politique du domaine ou même le recours à des mathématiques discrètes. D'autres sont souvent décrits comme de radicales innovations, par exemple les liens entre mathématiciens, militaires et industriels indissociables de la cryptographie contemporaine. Les nombres premiers sont définis et étudiés dans les *Éléments* d'Euclide (env. 300 avant notre ère), mais, comme bien d'autres, c'est à un mathématicien du 19e siècle, William S. Jevons (1835-82), que Ronald Rivest (né en 1947) – le R. du système RSA – attribue[3] d'avoir lancé le premier défi de factorisation, en 1874 : trouver deux nombres dont le produit soit 8 616 460 799. Ces temporalités sont-elles effectives ou créées par une historiographie plus ou moins spontanée des principaux acteurs du domaine – une historiographie qui, parfois, identifie rétrospectivement des approches modernes dans les processus anciens de

[1] cgolds@math.jussieu.fr, directrice de recherche au CNRS, UMR 7586, Institut de mathématiques de Jussieu-PRG.

[2] Si de nombreux spécialistes distinguent « cryptographie », « cryptologie », « codage », « cryptanalyse », *etc*., le sens de ces distinctions n'est pas toujours fixé. De plus, ces distinctions ne sont en général pas maintenues dans les classements bibliographiques, comme nous le verrons. J'ai pris le parti ici de les ignorer.

[3] Dans son exposé donné le 8 février 2011, à l'occasion du *Killian Award*, « The growth of cryptography », http://people.csail.mit.edu/rivest/pubs/Riv11a.slides.pdf.

codage, ou, au contraire, ignore des configurations lointaines entre sciences et pouvoirs économiques, politiques et militaires parce que la mémoire sociale des mathématiques n'a pas retenu l'importance des domaines pratiques avant le 19e siècle ? « Comment une spécialité qui n'a pas vingt ans d'âge », demande Jacques Stern en 1998, « peut-elle revendiquer une histoire de plus de vingt siècles ? »[4].

QU'EST-CE QU'UNE DISCIPLINE ?

L'impression dominante en assistant actuellement à une conférence sur l'histoire de la cryptographie est bien celle d'une discipline tout juste constituée, ou même en voie de l'être. Or, la notion de discipline, le problème de la disciplinarisation, ont beaucoup intéressé les sociologues et les historiens des sciences. Il faut toutefois noter la variété de leurs définitions de ce qu'est une discipline, de leurs descriptions, et par conséquent des techniques proposées pour les étudier. Certains auteurs mettent l'accent sur l'enseignement : c'est alors avant tout par les manuels, par les programmes de formation spécifiques, que se définit une discipline. Rudolf Stichweh (né en 1951) ouvre ainsi son étude fondamentale sur la genèse du système scientifique moderne :

> « Depuis Aristote, le philosophe a pour tâche de répartir la totalité du savoir humain de manière à dégager un ordre rationnel de la série et de la hiérarchie des domaines du savoir […]. Il est manifeste qu'une telle entreprise est liée à la question de l'enseignement scolaire ; de fait, on appelle « disciplines » les unités qu'engendre la classification : il s'agit d'un savoir présenté sous une forme qui peut s'enseigner. Les principes de classification varient avec la forme que prend l'institutionnalisation sociale de l'éducation »[5].

D'autres auteurs, se focalisant sur l'établissement d'un domaine de recherche, identifient une discipline par un ensemble de caractéristiques communes qu'ils repèrent dans les articles ou mémoires de recherche, des textes de synthèse, des rapports. Martin Guntau et Hubert Laitko voient une discipline scientifique comme un « système d'activités orienté-objet » (*object-oriented system of scientific activities*) et non comme un simple système de connaissances[6]. S'appuyant sur leurs travaux, Ralf Haubrich[7] a proposé une liste de composantes permettant de définir une discipline mathématique particulière qui aurait émergé à partir des *Disquisitiones*

---

[4] Stern, *La science du secret*, p. 8.
[5] Stichweh, *Études sur la genèse du système scientifique moderne*, p. 15.
[6] Guntau et Laitko, *Der Ursprung der modernen Wissenschaften*, p. 26.
[7] Haubrich, « Gaussian Number Theory *vs* Algebraic Number Theory ».

Arithmeticae de Carl Friedrich Gauss (1777-1855), et d'identifier, au moins en moyenne, si des travaux particuliers en relèvent : la définition du sujet (les relations entre nombres entiers), les concepts clés (congruences et formes quadratiques) et les problèmes associés (la classification poussée des formes en classes, ordre, genre, par exemple), l'organisation systémique, reflétée par les classifications des journaux ou les tables des matières des ouvrages de synthèse, comme le « Report on the Theory of Numbers » de H. J. S. Smith (1826-83) pour la *British Association for the Advancement of Science*, ou l'article « Numbers, Theory of » de la IX[e] édition de *l'Encyclopaedia Britannica*. On pourrait selon les cas ajouter d'autres critères, comme les modes de preuve acceptés, ou encore les valeurs mises en avant pour apprécier une solution, comme sa généralité, ou le fait qu'elle soit effective.

Si le mot « activités » (dans « système d'activités orienté-objet ») permet en principe d'attacher ce repérage à des pratiques – celles qui forgent définitions et concepts, celles qui classent, ordonnent et diffusent les résultats –, le fait de concevoir une discipline comme orientée vers un objet (de savoir) retentit donc ici sur la nature des critères retenus, internes aux mathématiques.

Plusieurs sociologues, au contraire, ont focalisé leur définition d'une discipline sur l'existence même de la communauté qui la produit. C'est alors à partir du comportement de cette communauté, de ses modes de recrutement ou d'intégration, de ses rites, de ses liens, de ses actions, que la discipline se construit. Colloques ou séminaires spécifiques, lieux particuliers de rencontres ou de publication, postes-clés, protocoles identiques, mais aussi, au niveau textuel, réseaux de citations partagées, références croisées, histoires communes répétées, deviennent alors les indices d'une coagulation disciplinaire. Pour Thomas S. Kuhn (1922-96),

> « Une communauté scientifique se compose de ceux qui pratiquent une certaine spécialité scientifique. Tous ont une formation et une initiation professionnelle semblables à un degré inégalé dans la plupart des autres domaines. Ce faisant, ils ont assimilé la même littérature technique et en ont retiré dans l'ensemble les mêmes leçons. [...] On peut à bon droit se demander : que partagent ses membres qui explique la relative plénitude de leurs communications professionnelles et la relative unanimité de leurs jugements professionnels ? [...] Je suggère le terme *matrice disciplinaire : disciplinaire* en référence à ce que possèdent en commun les spécialistes d'une discipline particulière ; *matrice* parce que cet ensemble se compose

> d'éléments ordonnés de diverses sortes, dont chacun demande une étude détaillée »[8].

Des modèles sociologiques distincts de la construction sociale des sciences ont donné lieu à de nombreuses variantes, qui se traduisent d'ailleurs par des variations ou des dédoublements de vocabulaire ; les mots « champ de recherche » ou « école » ou « communauté » peuvent par exemple se substituer au mot « discipline » pour décrire des structures de recherche. Le mot « discipline » peut être selon le cas abandonné, relégué en adjectif – la « matrice disciplinaire » de Kuhn –, ou réservé en complément pour le classement institutionnel des enseignements[9].

LA CRYPTOGRAPHIE COMME DISCIPLINE EN FORMATION

La plupart des auteurs de ces théories sociologiques se sont aussi intéressés aux mécanismes de la (trans)formation disciplinaire, et plusieurs des phénomènes qu'ils repèrent sont bien à l'œuvre pour la cryptographie. Les témoignages des spécialistes, les présentations des colloques, les préfaces des livres, évoquent ainsi un amalgame de plusieurs courants de recherche relevant de disciplines plus anciennes, et leur recomposition autour de thèmes et de questions clés.

En même temps, les chercheurs concernés ont commencé à constituer une mémoire collective, tant à partir d'histoires partielles de chacune des composantes que d'épisodes variés de leur rapprochement. Les actes d'un *Workshop on Cryptography*, à Burg Feuerstein au printemps 1982, se placent ainsi sous un double patronage : celui du Goethe de « Plaisir du secret » et celui du lieu même du colloque, construit au début des années

---

[8] Kuhn, *La structure des révolutions scientifiques*, Postface, p. 241 et p. 248 (traduction adaptée par moi-même). « *A scientific community consists … of the practitioners of a scientific specialty. To an extent unparalleled in most other fields, they have undergone similar educations and professional initiations; in the process they have absorbed the same technical literature and drawn many of the same lessons from it.* […] *One may usefully ask : What do its members share that accounts for the relative fullness of their professional communication and the relative unanimity of their professional judgments ?* […] *I suggest 'disciplinary matrix': 'disciplinary' because it refers to the common possession of the practitioners of a particular discipline; 'matrix' because it is composed of ordered elements of various sorts, each requiring further specification* ». Kuhn, *The Structure of Scientific Revolutions*, Postscript, p. 177 et p. 182.

[9] Je renvoie à Gauthier, « La Géométrie des nombres comme discipline », en particulier pp. 20-24, pour une discussion d'exemples de ces notions en histoire des sciences. Remarquons que ces notions ne coïncident pas *a priori*. Voir Goldstein et Schappacher, « A Book in Search of a Discipline » et « Several Disciplines and a Book » pour une illustration possible de la différence entre « champ de recherches » et « discipline », appliquée à la théorie des nombres.

1940 comme « un centre camouflé pour l'ingénierie des communications mettant l'accent sur la recherche cryptographique »[10]. Ce phénomène mémoriel est souvent analysé par les sociologues comme caractéristique de la mise en place d'une nouvelle discipline ou d'un nouveau champ de recherche scientifique.

Des négociations explicites ou non sur les acteurs principaux, des anecdotes personnelles, mais partagées, des discussions sur la date exacte d'un événement – séance décisive de séminaire, premier colloque fondateur, cours dans une université, ou publication d'une modélisation particulièrement fructueuse, d'un théorème identifié comme fondamental – permettent ainsi d'ajuster un récit commun du passé, une histoire. Beaucoup de ces récits adoptent d'ailleurs une description globale similaire, quel que soit le sujet, témoignant donc davantage des conventions sur ce genre d'histoire que d'une étude spécifique des dynamiques à l'œuvre dans le cas concerné. Ils opposent une phase de résultats élémentaires, isolés et dispersés, à l'élaboration récente de théories plus mûres, fondées sur des outils mathématiques avancés et en interaction fructueuse avec plusieurs domaines. Pour le cas de la cryptographie, Elwyn R. Berlekamp (né en1940), dans un recueil destiné à commémorer le 25e anniversaire de l'article fondateur[11] de Claude E. Shannon (1916-2001), écrit ainsi :

> « Dans les premières années de la théorie du codage, la quasi-totalité des interactions avec d'autres disciplines académiques a consisté à découvrir que divers petits problèmes de cette théorie pourraient être résolus en appliquant des techniques élémentaires issues d'autres domaines. Cependant, dans la dernière décennie, la théorie du codage a mûri. Elle a non seulement fourni des applications à un certain nombre de résultats profonds en mathématiques pures, […] mais elle a également été en mesure d'apporter une contribution significative à d'autres domaines »[12].

---

[10] « *a camouflaged center for communications engineering emphasizing cryptographic research* », Beth, *Cryptography*, préface. La citation de Goethe est extraite de la section « Lust am Geheimnis » (Plaisir du secret) de son *Traité des couleurs*, et donnée en page de garde. Plusieurs dispositifs mécaniques de chiffrement, machine *Kryha*, *Enigma*, *etc.*, présentées au centre de Burg Feuerstein, sont aussi illustrés dans la partie historique des actes, voir par exemple pp. 6-7.

[11] Voir le chapitre « Du message chiffré au système cryptographie » p. 129.

[12] « *In the early years of coding theory, nearly all of the interactions with other academic disciplines consisted of discoveries that various minor problems in coding theory could be solved by the application of elementary techniques from other fields. However, in the past decade, coding theory has matured. Not only has coding theory found applications for a number of deep results in pure mathematics, […] but coding theory has also been able to make significant contributions to other areas* », Berlekamp, *Key Papers*, p. 1.

La structure de ce récit concorde avec celle d'autres récits de formation disciplinaire, qui adoptent un schéma analogue[13]. Mais cette concordance de structure cache à peine une grande variété dans les domaines appelés à témoigner, dans les résultats mentionnés et dans la chronologie détaillée, et ce, pour une même discipline. Berlekamp souligne lui-même la variabilité dans le temps de l'importance historique (*historical significance*) qui peut être accordée à un article dans le domaine de la cryptographie, selon les travaux que cet article a suscités à une certaine date[14]. L'ère moderne de la cryptographie commence-t-elle par exemple avec Shannon ou avec Whitefield Diffie (né en 1944) et Martin Hellman (né en 1945), qui définirent en 1976 le concept de clé publique et annoncèrent en même temps « l'aube d'une révolution en cryptographie »[15] ?

Face à ces constructions mémorielles, stéréotypées dans leur forme mais variables dans leur contenu, la position de l'historienne est un peu celle d'un paléontologue habitué à étudier des collections de petits morceaux fossilisés et qui serait projeté au milieu d'un troupeau de brachiosaures vivants : de (trop) nombreuses informations disponibles, de toute nature, sur toutes sortes de supports, à la fois hétérogènes et parcellaires, rendent difficile une appréciation d'ensemble des mécanismes en jeu dans ce domaine en pleine expansion.

Que peut-on voir en changeant la focale et en se plaçant d'emblée à une échelle plus grossière, celles des classifications par sujets adoptées par les mathématiciens eux-mêmes[16] ? Depuis le milieu du 19e siècle au moins – avec l'apparition du journal de recension, *Jahrbuch für die Fortschritte der Mathematik* – ces classifications, changeant au cours du temps, permettent de repérer certaines évolutions disciplinaires[17]. Qu'en est-il de la

---

[13] Voir par exemple la description que David Hilbert (1862-1943) donne en 1896 de la disciplinarisation de la théorie des nombres – en tant que théorie des corps de nombres algébriques – au début du *Zahlbericht*. Ce point est commenté dans Goldstein et Schappacher, « Several disciplines and a Book », pp. 88-90.

[14] Berlekamp, *Key Papers*, p. 3.

[15] Extrait de leur article « New Directions in Cryptography », cité d'après Stern, *La science du secret*, p. 85, qui en fait le point de départ du troisième âge de la cryptographie, celui dans lequel nous sommes. La traduction de cet article figure au chapitre « Les nouvelles orientations de la cryptographie » p. 173.

[16] Une analyse analogue du côté de l'informatique serait instructive. Voir quelques éléments dans Mounier-Kuhn, *L'informatique en France*, pp. 33-36.

[17] Ainsi que des priorités multiples, liées à une nation, un domaine particulier, un parti-pris méthodologique. On pourra se reporter en particulier à Siegmund-Schultze, *Mathematische Berichterstattung in Hitlerdeutschland*, et à Rollet et Nabonnand, « An Answer to the Growth of Mathematical Knowledge ? » pour deux discussions de deux classifications concurrentes au 19e siècle. Voir aussi Goldstein et Schappacher, « Several Disciplines and a Book », pp. 93-96, pour ce que ces classifications reflètent de l'état d'un champ. Rappelons qu'une même norme internationale, la MSC, est maintenant utilisée par les deux principaux journaux

cryptographie dans le standard MSC (*Mathematics Subject Classification*), schéma de classification international adopté pour localiser par sujet tous les articles de mathématiques ?

MSC se présente comme une arborescence de sections indexées par un nombre de deux chiffres et correspondant à de larges divisions des mathématiques (comme l'algèbre linéaire ou les équations aux dérivées partielles), découpées en sous-sections indexées par une lettre, elles-mêmes redécoupées en rubriques indexées par un nombre. « *Cryptography* » apparaît dans le titre de quatre rubriques du dernier classement MSC, celui de 2010 :

– 11T71 : *Algebraic coding theory; cryptography,*
– 14G50 : *Applications to coding theory and cryptography,*
– 81P94 : *Quantum cryptography,*
– 94A60 : *Cryptography.*

La première rubrique relève de la section 11, « Théorie des nombres », plus particulièrement, des « aspects arithmétiques des corps finis » ; la deuxième rubrique de la section 14, « Géométrie algébrique », plus particulièrement de « Géométrie diophantienne » ; la troisième de la section 81, « Théorie quantique » ; la dernière enfin de la section « Communication, Information, Circuits ». Un jeu de renvois[18] pointe aussi sur la rubrique 68P25, « Cryptage de données » (*Data encryption*) de la section Informatique (*Computer Science*) – dont dépend aussi la rubrique 68P30, « Codage et théorie de l'information » – et sur plusieurs rubriques de la sous-section 94B, « Théorie des codes correcteurs » (*Theory of error-correcting codes and error-detecting codes*). Nous sommes d'ailleurs loin d'épuiser ainsi tous les articles pertinents : une recherche sur l'expression « Boolean functions » dans le titre de l'article renvoie, en contexte cryptographique, aux rubriques 94C10, 68T05, 68Q17, *etc*. L'article fondateur de Richard W. Hamming (1915-98), « Error detecting and error correcting codes » était recensé en « probabilités » et, plus remarquable encore, treize des quarante-quatre textes classiques sélectionnés par Berlekamp dans son *Source book* n'ont pas du tout été recensés dans les *Mathematical Reviews*[19].

Ce morcellement et le fait que la cryptographie n'apparaît qu'au niveau des rubriques, pas des sections elles-mêmes, donnent bien l'image d'une disciplinarisation non achevée ; ils indiquent aussi qu'une attention aux

---

de recension en mathématiques, *Mathematical Reviews et Zentralblatt*, voir http://www.ams.org/ msc/pdfs/classifications2010.pdf.

[18] Ces renvois varient beaucoup selon la date de la MSC, suggérant d'intéressantes micro-réorganisations, par exemple la classification de 2000 met en avant la rubrique 68Q05, *Machines de Turing et autres modèles de calcul*.

[19] Voir Berlekamp, *Key Papers*. À quatre exceptions près, les autres articles – ils sont tous antérieurs à 1973 – sont recensés dans la section 94, celle d'informatique.

problèmes de codage s'est développée dans plusieurs branches. Il est aussi possible de constater certaines évolutions. Si la section 94 remonte aux origines des *Mathematical Reviews*, dans les années 1940, 94A, « Communication, information » est une sous-section apparaissant seulement en 1980, même si elle hérite de sous-sections et rubriques antérieures (dont « Coding Theory », présente entre 1973 et 1979). La rubrique 94A60, *Cryptography per se*, date en particulier de 1980. Il en est de même de 11T71, présente dès l'apparition de la section 11 (qui remplace alors l'ancienne section 10 consacrée à la théorie des nombres jusqu'alors). Si *Computer Science* est présente dès 1940, la sous-section 68P, « Theory of data », et en particulier 68P25, datent aussi de 1980 ; notons en revanche que 68P30, *Coding and information theory*, est plus récente, n'apparaissant qu'en 2000. Le lien à la géométrie algébrique ne bénéficie d'une rubrique spécifique 14G50 qu'en 2000, quant à 81P94, elle vient tout juste d'apparaître, en 2010.

La répartition des articles dans ces rubriques est par ailleurs tout à fait inégale. Depuis 1980, plus de 7 000 articles ont 94A60 comme code de classification principal, 7720 ont 94BX, contre seulement 316 items en rubrique principale 11T71. La plus récente rubrique 14G50 est principale pour 195 articles, alors que 81P94 l'est déjà pour 122. Toutes les rubriques, en revanche, témoignent d'une augmentation importante des publications dans la dernière décennie. La rubrique 94A60 augmente d'un facteur 3,4 entre les années 1990 et les années 2000 (1264 items recensés entre 1990 et 1999, 4380 entre 2000 et 2009), alors que les sections 94B et 11T71, à deux échelles différentes, augmentent d'un facteur 1,5. Structurer ces données, par pays, par lieux de publications (le rôle des *IEEE Transactions on Information Theory* a été maintes fois souligné) ou par séries (comme celle des actes des colloques *Eurocrypt*, dans la suite de celui de Burg Feuerstern), par les attaches institutionnelles des auteurs, mais aussi en suivant les liens internes de renvois bibliographiques, de thèmes, de méthodes, d'applications réciproques, à l'intérieur des mathématiques ou à d'autres terrains, serait nécessaire pour une approche sociologique plus approfondie de l'avènement d'une discipline mathématique associée à la cryptographie[20]. Je me contenterai de noter l'entrelacs des rubriques dans les références croisées, suggestif d'une circulation importante à l'intérieur d'une thématique globale « Cryptographie » au-delà des divisions de MSC. L'article fondateur de RSA, classé en 94A05, est en référence de 124 items dans la base des *Mathematical Reviews* : 70 environ relèvent encore principalement de la sous-section 94A (dont 57 en 94A60), une vingtaine de

[20] Pour des exemples de cette démarche, appliquée à la théorie des nombres, voir Goldstein et Schappacher, « A Book in Search of a Discipline » et « Several Disciplines and a Book », et Gauthier, « La Géométrie des nombres comme discipline ».

« Théorie des nombres » (dont moins d'une dizaine en code 11T71 principal ou secondaire). L'article le plus ancien recensé en 11T71 apparaît 79 fois en référence dans la base, dont une seule fois pour un article de même code principal.

Les catalogues de bibliothèques peuvent fournir quelques indications supplémentaires. Je n'évoquerai ici que la situation en France. La bibliothèque MIR (Mathématiques Informatique Recherche) des universités Pierre et Marie Curie et Paris Diderot par exemple propose environ 500 ouvrages pour le sujet « Cryptographie/Cryptologie ». Les deux plus anciens sont *Cryptography : the Science of Secret Writing*, de Laurence Dwight Smith (écrit en 1943, mais acquis dans l'édition de Dover de 1955) et *Cryptanalysis : a study of ciphers and their solution* (1956) d'Helen Fouché Gaines (1888-1940). Les deux ouvrages sont mathématiquement peu techniques ; ils ont été classés dans la section de la bibliothèque sur les récréations mathématiques. Viennent ensuite chronologiquement quelques ouvrages de la fin des années 1960, comme l'ouvrage de Berlekamp, *Algebraic Coding Theory* (1968), ou *Elementary Cryptanalysis : a Mathematical Approach* (1966), d'Abraham Sinkov (1907-98), incluant des programmes de Paul Irwin. Ces livres comprennent entre autres des chapitres de mathématiques plus avancées sur les corps finis ; or, en cohérence avec leur mode d'acquisition, c'est dans la partie informatique de la bibliothèque qu'ils sont situés. À partir des années 1980, le nombre de titres croît nettement et leur localisation se diversifie ; c'est à partir de ce moment qu'elle reproduit la répartition mise en évidence en observant MSC. La même recherche sur les bibliothèques de l'École Normale Supérieure (Ulm) produit 75 titres, principalement classés en informatique, mais aussi une vingtaine d'ouvrages dans la bibliothèque de lettres, liés soit à des ouvrages historiques sur le chiffre militaire et les langages cryptés à différentes périodes, soit au déchiffrement des langues. Sur une plus longue durée, une recherche analogue sur la base SUDOC donne 1250 ouvrages dont le plus ancien – la *Polygraphie en six livres* de Trithème, en latin – remonte au 16e siècle. Le mot « cryptographie » apparaît couramment dans les titres à partir du 19e siècle ; il est alors lié au déchiffrement de toutes sortes d'écritures secrètes et à ses usages, comme dans deux ouvrages de 1893, *De la cryptographie : essai sur les méthodes de déchiffrement*, de Paul L. E. Valerio, ou dans la *Cryptographie nouvelle, assurant l'inviolabilité absolue des correspondances chiffrées* de Félix M. Delastelle (1840-1902), amateur maintenant bien connu[21], également auteur de *Mathématiques appliquées, Traité élémentaire de cryptographie* en 1902. La localisation de ces ouvrages est significative : jusqu'à la Seconde Guerre Mondiale, ils sont

[21] Voir le chapitre « Du message chiffré au système cryptographique » p. 122 et le chapitre « La cryptologie gouvernementale française » p. 156.

hébergés principalement à la Bibliothèque Sainte-Geneviève, à la Bibliothèque nationale ou, pour ceux rédigés par des militaires, au CNAM, ce qui les situe alors hors du strict monde académique, incarné par la Faculté des sciences. Les bibliothèques des universités de province en ont peu avant une époque très récente : les fonds témoignent ici de la forte institutionnalisation de ces sujets dans les années 1990.

Ces éléments d'enquête font donc apparaître la complexité de l'histoire de la cryptographie comme discipline. La multiplicité des professions en jeu était déjà bien connue. Mais nous voyons ici que les liens concrets avec les mathématiques ne relèvent pas d'un simple transfert de connaissances, des mathématiques pures vers des applications que l'informatique serait venue renforcer et concrétiser. Qu'une bibliothèque d'informatique héberge les livres de mathématiques pures orientés vers le codage avant que le sujet n'apparaisse dans les bibliothèques de recherche en mathématiques indique une dynamique d'appropriation préalable par une communauté nouvelle. L'héritage des récréations mathématiques mériterait aussi un examen détaillé. Comme nous l'avons vu, c'est dans cette section des bibliothèques qu'on trouve quelques ouvrages de cryptographie dès les années 1950. Et c'est aussi dans ce cadre qu'Édouard Lucas (1842-91), à la fin du 19e siècle, construisit un environnement mathématique adéquat pour le jeu de Nim ou pour le baguenaudier (associé aux futurs codes de Gray)[22] ; ou que Martin Gardner (1914-2010) donna un large retentissement au système RSA en 1977 *via* sa colonne de jeux dans *Scientific American*[23]. Cette filiation, pour marginale qu'elle puisse sembler au regard des développements des dernières décennies, semble avoir servi sinon de stimulant, du moins de cadre possible pour la dissémination de certaines questions pertinentes sur une longue durée.

Du même coup s'explique la difficulté de mettre en place une mémoire collective commune : selon les rencontres, les opportunités, c'est l'appropriation d'un outil différent, d'un élément particulier qui apparaîtra comme décisif, et c'est l'histoire de cet élément de contact, redéployée vers le passé, qui sera décrite. Plusieurs caractérisations du domaine, insistant sur des aspects différents, ont ainsi été suggérées : la mécanisation des calculs, l'importance attachée à l'effectivité dans des domaines de mathématiques pures jusqu'alors, comme la théorie des nombres ou la géométrie algébrique ; une attention spécifique au temps – temps humain, temps d'exécution d'une tâche – ; des questions autour de l'aléa, du probable, des degrés de sécurité ; la réflexion sur le langage, sur le (dé)chiffrement, à la combinatoire des signes ; les liens entre art de la guerre, mathématiques,

[22] Décaillot, « Eugène Lucas : le parcours original d'un scientifique français », p. 168.
[23] Voir le chapitre « Pourquoi et comment la cryptologie vient de surgir dans le domaine public ? » p. 211.

industrie et pouvoirs politiques, liens de résultats et de méthodes, liens de personnes aussi. Or, de telles configurations, du point de vue des éléments qui les composent, ne sont pas propres à la période contemporaine. Il peut donc être utile de les désenclaver de l'histoire stricte de la cryptographie dans l'espoir de mieux mettre à jour quels aspects les attachent spécifiquement à cette histoire. Je me contenterai d'illustrer cette suggestion à partir de quelques exemples de résultats récents portant sur l'histoire de la théorie des nombres.

NOMBRES, TEMPS, LANGAGES, MACHINES AU 17e SIECLE

Il est banal, dans le cadre d'une histoire de la cryptographie, de repérer des travaux mathématiques pertinents dès le 17e siècle. Le petit théorème de Fermat[24], par exemple, est au cœur de l'algorithme RSA et l'énoncé apparaît bien explicitement, dans sa forme forte, sous la plume de Pierre Fermat (160?-1665). Dans une lettre du 18 octobre 1640, celui-ci écrit ainsi :

> « Tout nombre premier mesure infailliblement une des puissances –1 de quelque progression que ce soit, et l'exposant de la dite puissance est sous-multiple du nombre premier –1 ; et après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question.
> Exemple : soit la progression donnée
>
> | | | | | | | |
> |---|---|---|---|---|---|---|
> | 1 | 2 | 3 | 4 | 5 | 6 | |
> | 3 | 9 | 27 | 81 | 243 | 729 | *etc*. |
>
> avec ses exposants en dessus. Prenez par exemple le nombre premier 13. Il mesure la troisième puissance –1 de laquelle 3, exposant, est sous-multiple de 12, qui est moindre de l'unité que le nombre 13, et parce que l'exposant de 729, qui est 6, est multiple du premier exposant, qui est 3, il s'ensuit que 13 mesure aussi la dite puissance 729 – 1 »[25].

Ce résultat exprime pour nous que le groupe multiplicatif du corps fini $\mathbb{F}_p$ est cyclique, d'ordre $p-1$. En tant qu'élément de l'histoire de la cryptographie, la mention de ce théorème illustre en général l'idée que des mathématiques élaborées depuis longtemps pour elles-mêmes, de manière purement théorique, se trouvent utilisables dans des contextes appliqués.

Pourtant, le (petit) théorème de Fermat n'est pas originellement un résultat théorique et structurel, valorisé en tant que tel. L'objectif de Fermat est d'étudier la divisibilité, par différents nombres premiers, de suites de la

[24] Il s'agit du fait que, si p est un nombre premier et a un entier premier à p, alors $a^{p-1} \equiv 1 \mod p$ (c'est-à-dire que p divise $a^{p-1} - 1$). La notation actuelle utilisée ici (« ≡ ») remonte aux *Disquisitiones Arithmeticae* de C.F. Gauss, en 1801.
[25] Fermat, *Correspondance*, p. 209.

forme $a^n - 1$, l'entier a étant fixé (« une des puissances –1 de quelque progression que ce soit »). Il énonce donc qu'il existe toujours des exposants n pour lesquels cette divisibilité a lieu (« Tout nombre premier mesure infailliblement une des puissances –1 »), et que le plus petit de ces exposants est un diviseur (un « sous-multiple ») de $p - 1$ (Fermat oubliant ici de préciser que l'énoncé n'est valide que si les nombres premiers p ne divisent pas a). En termes actuels, il s'agit bien de déterminer l'ordre de a dans le groupe multiplicatif (cyclique) de $\mathbb{F}_p^*$, mais pour Fermat, a est fixé et p varie.

Cette différence de perspective est liée à la finalité de son résultat : pour Fermat et ses contemporains, l'intérêt est de raccourcir les calculs dans la recherche des nombres parfaits, c'est-à-dire des nombres égaux à la somme de leurs diviseurs propres, et plus généralement dans la recherche des nombres qui ont un rapport donné à la somme de leurs diviseurs propres. Comme c'est encore le cas, les nombres parfaits connus à l'époque de Fermat étaient ceux de la forme $2^{n-1}(2^n - 1)$, avec $2^n - 1$ premier ; il s'agit d'une application directe d'un théorème des *Éléments* d'Euclide. Déterminer les nombres parfaits implique donc d'examiner les diviseurs possibles de $2^n - 1$ (et plus généralement de $a^n - 1$). L'emploi de son théorème permet à Fermat de s'assurer qu'il n'y a pas de nombres parfaits à 20 ou 21 chiffres[26] ou de fabriquer des nombres très grands, sous-multiples donnés de la somme de leurs diviseurs propres, comme 1 802 582 780 370 364 661 760, qui vaut le quart de la somme de ses diviseurs propres. Le petit théorème de Fermat lie diviseurs premiers possibles et exposants ; il permet donc d'éliminer de nombreux nombres premiers des diviseurs possibles, et raccourcit considérablement les calculs. Plus généralement, la nécessité d'améliorer la recherche des facteurs premiers est clairement exprimée dès cette époque : Fermat se plaint ainsi des « fréquentes divisions qu'il faut faire pour trouver les nombres premiers ». Il loue particulièrement un de ses correspondants, Bernard Frenicle de Bessy (160?-74), pour « la vitesse de ses opérations » et propose une méthode pour déterminer plus efficacement si un nombre est premier ou composé, par différence de carrés[27].

L'intérêt pour ces questions n'est pas propre à Fermat, et relève bien d'enjeux collectifs[28]. Ceux-ci sont régulièrement évoqués dans les écrits, correspondances ou mémoires du cercle[29] de Marin Mersenne (1588-1648) – auquel appartient Frenicle et dont Fermat est correspondant – et frôlent l'histoire de la cryptologie de multiples façons. En témoignent les procédures mises en place pour contourner le manque de confiance dans la

[26] *ibid*., p. 248, p. 194 et p. 210.
[27] *ibid*., p. 187 et p. 257.
[28] Sur ces enjeux, et en particulier le rôle de la taille des nombres et du temps dans les questions mathématiques de ce milieu, voir Goldstein, « L'arithmétique de Fermat ».
[29] Voir le chapitre « L'ancrage de la cryptologie dans les jeux d'écriture » p. 47.

transmission scientifique à distance, comme celle d'échanger problèmes et solutions numériques, en lieu des méthodes ou des règles générales. En témoignent encore, l'intégration du temps dans *l'énoncé même des problèmes*. Voici par exemple la demande que reçoit Fermat de ce cercle, en avril 1643 :

> « Vous me demandiez ensuite si [100 895 598 169] est premier ou non, et une méthode pour découvrir dans l'espace d'un jour s'il est premier ou composé »[30].

Nous constatons donc, dans ce milieu, une prise de conscience des problèmes spécifiques liés à la taille des nombres en jeu et au temps imposé pour la résolution ; en revanche, nous n'avons pas de trace directe d'une véritable évaluation quantitative de ce temps dans les procédures de calcul.

Marin Mersenne et les membres de son entourage s'intéressent de près au problème des langues artificielles et à celui des chiffres, souvent perçus comme analogues[31]. Leurs correspondances, leurs ouvrages, montrent leur familiarité avec des auteurs passés associés à l'histoire des codes comme Jérôme Cardan (1501-76), Blaise de Vigenère (1623-96), ou François Viète (1540-1603), mais aussi avec des experts ès codes contemporains : un proche de Mersenne, Aimé de Gaignières (mort après 1661), amateur de codes, lance ainsi un défi à Antoine Rossignol (1600-82), cryptologue professionnel au service de l'État. En lien avec des problèmes de combinatoire, Mersenne propose dans son *Harmonie universelle* un moyen d'« escrire toutes sortes de lettres secrettes », tout en soulignant l'utilité de son ouvrage pour les affaires publiques. Or, tant Frenicle que Mersenne deviennent attentifs au fait que les deux opérations de chiffrer et de déchiffrer ne sont pas inverses l'une de l'autre de manière transparente. Frenicle dit ainsi, dans son *Abrégé des combinaisons* composé vers 1640, et publié à la fin du siècle :

> « Mais ce n'est pas assez de sçavoir écrire, si l'on ne sçait lire son écriture, & ce n'est pas peu de chose que de sçavoir lire celle-ci : car ceux mêmes qui l'auroient écrite ne la pourroient lire, s'ils n'en sçavaient la méthode, quoiqu'ils sçussent celle de l'écrire »[32].

---

[30] Fermat, *Correspondance*, p. 255. Le nombre est composé, produit de 898 423 et 112 303.

[31] Ces relations et leurs liens avec les mathématiques sont examinées dans la thèse d'Ernest Coumet, « Mersenne, Frenicle et l'élaboration de l'analyse combinatoire », ainsi que dans son article « Cryptographie et numération ».

[32] Cité dans Coumet, « Cryptographie et numération », p. 1021. L'histoire de la cryptographie, tout en soulignant l'importance de ces questions, ne retient d'ordinaire comme acteur de la période que Rossignol. Voir Kahn, *The Codebreakers*, ch. IV et V.

L'élaboration d'instruments et de machines aptes à implémenter ces combinatoires de signes est aussi à l'ordre du jour. C'est le fils d'un autre proche de Mersenne, et lui-même inséré jeune dans son cercle, Blaise Pascal (1623-62), qui conçoit d'ailleurs une machine arithmétique commercialisée et, rappelons-le, bénéficie même d'un privilège royal sur toute la production.

Nous trouvons donc dès le 17e siècle, non seulement les quelques éléments éparpillés usuels dans toute histoire de la cryptologie – le petit théorème de Fermat, un ou deux cryptologues proches du pouvoir royal, comme les Rossignol –, mais une configuration, tant épistémique que sociale, qui inclut un intérêt pour le chiffrement et le déchiffrement, une appréciation de ses enjeux politiques, une réflexion sur leurs liens complexes et sur la calculabilité, la construction de machines variées, des mathématiques liées à la combinatoire et à la primalité.

INDUSTRIE, ORDINATEURS ET THEORIE DES NOMBRES

Un autre scénario envisageable serait celui d'une rencontre entre industrie et théorie des nombres qui n'aurait pu avoir lieu que dans les années 1980. Ce scénario s'accommode bien d'une histoire franco-centrée des mathématiques selon laquelle l'esprit du groupe Bourbaki aurait dominé la scène mathématique entre 1950 et 1970, s'opposant à toute implémentation sérieuse des mathématiques appliquées, en particulier numériques[33], et promouvant une théorie des nombres alliée, non aux calculs, mais à la géométrie algébrique la plus absconse.

Ordinateurs et industries privées croisent pourtant la théorie des nombres bien avant les années 1980. Comme l'a montré Anne-Marie Décaillot[34], dès la seconde moitié du 19e siècle, Édouard Lucas s'intéresse explicitement à la cryptographie, il est en contact avec les milieux industriels, son travail de recherche concerne en priorité combinatoire et arithmétique. Plus spécifiquement, il examine la réciproque du théorème de Fermat, dans la perspective de tests de primalité : le fait que $(\mathbb{Z}/n\mathbb{Z})^*$ soit cyclique d'ordre $n-1$ caractérise les entiers n premiers. Autrement dit, n est premier si et seulement s'il existe un entier a (strictement inférieur à n) tel que n divise $a^{n-1}-1$, mais en revanche ne divise aucun des nombres $a^{(n-1)/q}-1$, $q>1$ étant un diviseur premier de $n-1$. La mécanisation même de tests de primalité ne lui était pas étrangère, bien que la machine qu'il imagine ne nous soit pas parvenue. Comme évoqué plus haut, Lucas a aussi relancé les études mathématiques de problèmes situés dans le cadre des recréations

[33] On trouvera dans Mounier-Kuhn, *L'informatique en France*, pp. 170-186 et 377-378 un exposé illustré par d'édifiantes citations de ce scénario et une discussion de ses limites.
[34] Décaillot, « L'arithméticien Édouard Lucas : théorisation et instrumentation ».

mathématiques, mais en en faisant apparaître la complexité, comme pour les tours de Hanoï. Un autre aspect remarquable de son activité est sa tentative d'appliquer ces recherches arithmétiques à des situations industrielles ; comme en témoignent les comptes-rendus de l'*Association Française pour l'Avancement des Sciences* (AFAS), il n'est pas un cas isolé à cette époque, même s'il est sans doute le plus célèbre à s'engager dans ces interfaces. Dans le cas de Lucas, il s'agit d'industrie textile, et non de sécurité de transmission, mais de modélisation et de mécanisation du tissage, des satins en particulier, par l'arithmétique modulaire[35].

Or, ni le passage à l'ordinateur, ni la traversée de l'Atlantique ne semblent modifier radicalement ces configurations, dans lesquelles de nombreux éléments que nous associons maintenant à l'avènement de la cryptographie sont en place, mais reliés de manière différente. C'est d'ailleurs par des machines analogiques, cribles électriques, engrenages empruntés à des vélos, que les Lehmer, Derrick Norman (1867-1938) et son fils Derrick Henry (1905-91), ont d'abord poursuivi leurs investigations sur les nombres premiers dans la lignée de Lucas. C'est le premier qui factorise en 1903 le nombre de Jevons, 8 616 460 799, auquel nous avons fait allusion au début de cet article. Quant au fils, il est associé au test de Lucas-Lehmer et est devenu une figure connue de l'histoire de la cryptographie.

Selon les historiens qui les ont étudiés[36], Leo Corry d'une part, Maarten Bullynck et Liesbeth de Mol d'autre part, plusieurs facteurs sont décisifs dans la création d'un *Institute for Numerical Analysis* aux États-Unis, institut qui joue un rôle important dans les liens entre informatique et théorie des nombres : la crise économique des années 30, qui contribue à lancer D. H. Lehmer et son épouse Emma (1906-2007), également mathématicienne, dans divers périples à la recherche de postes, et du même coup favorise leurs nombreux contacts dans des milieux variés ; la Seconde Guerre Mondiale, qui donne à D. H. Lehmer l'occasion de lancer un programme plus ambitieux avec des ordinateurs puissants ; la concurrence entre universités aux États-Unis, dont la mise au point du SWAC (*Standard Western Automatic Computer*) est une des retombées cruciales. Cet ordinateur très puissant pour l'époque soude de nouveaux liens entre universités et industrie : il est utilisé dans l'industrie locale de l'aviation, mais il permet aussi aux Lehmer et à leur équipe, dans l'intervalle des calculs industriels, d'en développer d'autres, orientés vers la théorie des nombres. Pourtant, cet épisode ne témoigne pas d'une exceptionnelle connivence entre mathématiciens professionnels et industriels autour des calculs et des machines, qui serait propre aux États-Unis. D'une part, parce

[35] Décaillot, « Édouard Lucas et l'AFAS ».
[36] Voir Corry, « FLT meets SWAC » et « Hunting Prime Numbers », ainsi que Bullynck et De Mol, « A week-end off».

que Lehmer insiste alors sur l'aspect désintéressé des mathématiques qu'il pratique, bien plus que sur l'applicabilité éventuelle de ses travaux: « Le désir le plus impérieux pour étudier les mathématiques » affirme-t-il en 1932 « ne vient pas de son application pratique à l'étude de la vie matérielle de chaque jour, mais réside dans la romance et la séduction qui entoure ses mystérieux secrets »[37]. Il s'agit donc bien, non d'un engagement systématique et fructueux des mathématiciens dans les problématiques industrielles, mais de la possibilité de « *week-end off* »[38], et d'une répartition harmonieuse du temps de calcul des ordinateurs. D'autre part, des rapprochements analogues se retrouvent dans d'autres pays tout au long du 20e siècle.

En France même, la Première Guerre Mondiale a été l'occasion de nouvelles synergies entre universitaires, militaires, industriels. L'entre-deux-guerres voit alors l'arrivée massive d'industriels et de militaires au sein de la *Société mathématique de France*[39]. À l'inverse, des mathématiciens purs se réorientent après-guerre, parfois sous l'effet de leurs activités de guerre, vers des domaines vraiment appliqués. C'est le cas de Jean Kuntzmann (1912-92) qui, après une thèse d'algèbre en 1934, se consacre aux mathématiques de l'ingénieur, puis aux mathématiques de l'informatique, et crée en 1951 le premier laboratoire de calcul à Grenoble[40]. C'est aussi le cas pour Albert Châtelet (1883-1960) dont la thèse en 1911 porte sur les matrices appliquées à la théorie des nombres[41]. Servant pendant la Première Guerre Mondiale au Centre d'essais balistiques de Gâvre où il est affecté aux calculs, il est chargé après-guerre de la reconstruction de l'université lilloise ; il y sera recteur avant de devenir une personnalité importante de l'éducation nationale dans les années 1950, créateur du CROUS (Centre Régional des Œuvres Universitaires et Scolaires), et même candidat à l'élection présidentielle de 1958. Avec Paul Dubreil (1904-94), il lance juste après-guerre, en 1947, un séminaire d'algèbre et de théorie des nombres qui fait la part belle aux avancées théoriques de ce domaine considéré comme l'un des plus abstraits des mathématiques (variétés algébriques, théorie des idéaux, théorie des groupes, ...), mais en même temps, il insiste, contrairement par

---

[37] « *The most compelling urge to the study of mathematics is not its practical application to the study of every day, bread-and-butter life, but lies in the romance and glamour surrounding its mysterious secrets* », cité dans Corry, « Hunting Prime Numbers ».

[38] Bullynck et De Mol, « A week-end off ».

[39] Aubin et al., « Les mathématiciens français dans la Grande Guerre », pp. 194-195.

[40] Mounier-Kuhn, *L'informatique en France*, pp. 241-260.

[41] Voir sa biographie par Condette, « Albert Châtelet, la République par l'école ». Sur ses activités de guerre et leurs effets, Gauthier, « Albert Châtelet, de la théorie des nombres à la politique universitaire ». Un autre exemple intéressant de la génération suivante est celui de René de Possel (1905-74), d'abord membre de Bourbaki : s'orientant vers l'analyse numérique et l'informatique, il fut le directeur de l'institut Blaise Pascal du CNRS dans les années 1960. Voir Mounier-Kuhn, *L'informatique en France*, pp. 278-292.

exemple au groupe contemporain rassemblé sous le nom de Bourbaki, sur l'importance des calculs effectifs, sur les problèmes spécifiques que posent ces calculs et sur l'applicabilité de ces domaines à la physique et à l'industrie. Dans sa propre notice sur travaux, Albert Châtelet établit avec soin des ponts entre ces différents aspects :

> « Lorsque le Faculté des sciences de Paris, en octobre 1940, voulut bien me charger de l'enseignement d'Arithmétique supérieure, qu'elle venait de créer, j'ai pu exposer dans mes cours les théories algébriques modernes […]. Il y a quelque intérêt à signaler que l'Algèbre abstraite, qui reprenait ainsi droit de cité dans le pays de Galois, de Jordan, d'Hermite et de Henri Poincaré, trouvait en même temps des applications fécondes, non seulement en physique théorique, mais encore dans la technique industrielle »[42].

Les travaux de recherche de Châtelet, peu nombreux au milieu de ses activités administratives et pédagogiques, ne semblent guère propices à l'ancrer dans une histoire de la cryptographie, même si leurs orientations sur les calculs effectifs, l'usage des matrices, tranchent quelque peu avec les injonctions de l'algèbre structurale, qui privilégie l'intrinsèque et néglige alors les questions d'effectivité. En revanche, il illustre des courants mal connus des mathématiques de l'immédiat après-guerre, dont l'effet sur l'essor de la cryptologie mathématique en France mériterait peut-être d'être réévalué. Son séminaire d'algèbre et de théorie des nombres, qui s'est poursuivi en deux branches et avec différents organisateurs (Dubreil-Pisot, Pisot-Delange, Pisot-Delange-Poitou, *etc*.) a servi de point de ralliement de tendances très variées en théorie des nombres ou en algèbre jusqu'aux années 1990. Notons simplement à titre d'exemple que c'est dans ce séminaire (Dubreil-Pisot) que Marcel-Paul Schützenberger (1920-96) a exposé en 1956 une « Théorie algébrique du codage »[43] ; les travaux de Schützenberger s'inscrivent ainsi au début sous la double influence de Châtelet et Dubreil du côté de l'algèbre – il a suivi le cours de Châtelet sur les treillis et celui-ci est un des trois membres de son jury de thèse en 1953,

---

[42] Châtelet, *Notice sur les titres et travaux universitaires*. Je remercie les Archives de l'Académie des sciences de m'avoir permis de consulter et de citer ce document. Albert Châtelet, qui n'avait pas les faveurs du gouvernement de Vichy, ne prit en fait ses fonctions à la Faculté des sciences de Paris que plus tardivement. Sa candidature à ce poste, en concurrence avec celle de Claude Chevalley (1909-84), membre fondateur de Bourbaki et mathématicien de premier plan, fit d'ailleurs l'objet de polémiques.

[43] Schützenberger, « Théorie algébrique du codage ». NdE. : Ce travail participe d'un mouvement d'algébrisation du codage dans les années 1950. Le mathématicien et médecin Schützenberger est alors tout particulièrement concerné par la cybernétique. Sa thèse de 1953 contient une reformulation mathématique qui généralise la notion d'information de Shannon. Segal, *Le zéro et le un*, pp. 295-300 et p. 547-53.

avec Maurice Fréchet (1878-1973) et Georges Darmois (1888-1960) – et de Darmois du côté des probabilités.

RENCONTRES

Cette excursion dans les rencontres de l'arithmétique avec la science du codage met en évidence deux écueils. Le premier serait, n'attrapant du passé que des bribes ponctuelles, pauvres et décontextualisées, de voir à trop bon compte dans les dernières décennies une rupture radicale, qui instaurerait pour la première fois des liens entre théorie des nombres, cryptologie, collectivités multiples, pouvoirs économiques, militaires et politiques. Couper complètement les fils qui relient au 17e siècle le professionnalisme d'un cryptographe comme Rossignol aux théorèmes d'un Fermat, pour les insérer dans deux histoires, qui seraient l'une celle du secret, l'autre celle des corps finis ; négliger les occasions variées, tout au long du 20e siècle, où calculs arithmétiques et ordinateurs ont réuni autour d'une même machine, dans un même lieu, à un même cours, acteurs oubliés de la politique universitaire et futurs héros de la cryptologie, empêche de comprendre les socles sur lesquels la cryptologie s'est finalement sédimentée.

Mais le second écueil serait de diluer complètement dans ce passé enrichi les innovations, la radicalité du changement, qualitatif et quantitatif, des dernières décennies. En ce sens, la mémoire constituée des cryptologues, pour parcellaire qu'elle soit par rapport à l'historiographie, est elle aussi à prendre au sérieux. L'enrichissement du passé doit plutôt nous aider à dégager les spécificités propres à la configuration actuelle, et à repenser les dynamiques concrètes. À scruter plus précisément comment le développement d'emplois ou d'autres enjeux économiques nouveaux, une utilisation quotidienne, familière, d'objets techno-mathématiques impliquant la cryptologie, se sont liés à la mise en place de formations universitaires systématiques et au recrutement de chercheurs dans diverses institutions. À intégrer la polarité complexe entre Paris et les provinces dans l'examen du renouveau explicite des années 1990. Ou à une toute autre échelle, non moins pertinente, à cerner comment une expression comme « partage de secret publiquement vérifiable » peut être certes pertinente pour décrire l'organisation d'échanges mathématiques au 17e siècle, mais, au 21e siècle, est devenue en soi un énoncé scientifique.

BIBLIOGRAPHIE

Aubin, D., Gispert, H. et Goldstein C., « Les mathématiciens français dans la Grande Guerre », *in* F. Bouloc, R. Cazals, A. Loez (éds.), *1914-1918. Identités troublées : les appartenances sociales et nationales à l'épreuve de la guerre*, Toulouse, Privat, 2011, pp. 183-197.

Berlekamp, E. R. (ed.), *Key Papers in The Development of Coding Theory*, New York, IEEE Press, 1974.

Beth, T. (ed.), *Cryptography. Proceedings of the Workshop on Cryptography*, Burg Feuerstein, Germany, March 29-April 2, 1982, Lecture Notes in Computer Science, 149, Berlin, Heidelberg, New York, Springer, 1983.

Bullynck, M. et De Mol, E., « A Week-end Off. The First Extensive Number-theoretical Computation on the ENIAC », *in* A. Beckmann, A. Dimitracopoulos et B. Löwe (eds.), *Logic and Theory of Algorithms. Computability in Europe 2008*, LNCS 5028, Heidelberg, Springer, 2008, pp. 158–168.

Châtelet, A., *Notice sur les Titres et Travaux scientifiques*, Paris, s.n., 1953.

Condette, J.-F., *Albert Châtelet. La République par l'école (1883-1960)*, Arras, Artois Presses Université, 2009.

Corry, L., « FLT Meets SWAC: Vandiver, the Lehmers, Computers and Number Theory (1930-1956) », *Annals of the History of Computing*, 2008, vol. 30 n° 1, pp. 38-49.

— « Hunting Prime Numbers from Human to Electronic Computers », *The Rutherford Journal – The New Zealand Journal for the History and Philosophy of Science and Technology*, www.rutherfordjournal.org, 2010, vol. 3.

Coumet, E., « Mersenne, Frenicle et l'élaboration de l'analyse combinatoire dans la première moitié du XVII[e] siècle », *Thèse de 3e cycle*, Université de la Sorbonne, Paris, 1968.

— « Cryptographie et numération », *Annales. Economies, Sociétés, Civilisations*, 1975, vol. 30, pp. 1007-1027.

Décaillot, A.-M., « Eugène Lucas (1842-1891) : le parcours original d'un scientifique français dans la seconde moitié du XIX[e] siècle », *Thèse de l'Université René Descartes*, Paris, 1999. http://www.univ-lille1.fr/bustl-grisemine/pdf/extheses/50416-1999-Decaillot-Laulagnet.pdf.

— « L'arithméticien Edouard Lucas (1842-1891) : Théorie et instrumentation », *Revue d'histoire des mathématiques*, 1998, vol. 4, pp. 191-236.

— « Edouard Lucas (1842-1891) et l'Association Française pour l'Avancement des Sciences : une théorie des nombres non académique ». *in* M.-J. Durand-Richard (éd.), *Les mathématiques dans la cité*, Paris, PUV, 2006.

Diffie, W. et Hellman, M., « New directions in cryptography », *IEEE Transactions on Information Theory*, novembre 1976, vol. IT-22, n° 6, pp. 644-654.

Fermat, P., *Correspondance, Œuvres de Fermat publiées par les soins de MM. Paul Tannery et Charles Henry*, Paris, Gauthier-Villars, 1894, tome deuxième.

Gauthier, S., « La Géométrie des nombres comme discipline (1890-1945) », *Thèse de doctorat de l'UPMC*, Paris, 2007, http://math.univ-lyon1.fr/~gauthier/recherche/theseGauthier.pdf.

— « Albert Châtelet, de la théorie des nombres à la politique universitaire », *in* C. Goldstein et D. Aubin (éds.), *La Grande Guerre des mathématiciens français*, à paraître.

Goldstein, C., « L'arithmétique de Fermat dans le contexte de la correspondance de Mersenne : une approche micro-sociale », *Annales de la Faculté des sciences de Toulouse*, 2009, vol. 18, n° spécial, pp. 25-57.

Goldstein, C. et Schappacher, N., « A Book in Search of a Discipline (1801-1860) », *in* C. Goldstein, N. Schappacher et J. Schwermer (eds.), *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae* New York, Berlin, …, Springer, 2007, pp. 3-65.

— « Several Disciplines and a Book (1860-1901) », *in* C. Goldstein, N. Schappacher, et J. Schwermer (eds.), *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, New York, Berlin, …, Springer, 2007, pp. 66-103.

Guntau, M. et Laitko, H. (dir.), *Der Ursprung der modernen Wissenschaften : Studien zur Entstehung wissenschaftlicher Disziplinen*, Berlin, Akademie Verlag, 1987.

Haubrich, R., « Gaussian Number Theory *vs* Algebraic Number Theory », *Talk at the Conference for the 200th Anniversary of C. F. Gauss's Disquisitiones Arithmeticae*, Oberwolfach, 2001.

Kahn, D., *The Codebreakers : The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Rev. Sub. Ed., New York, Scribner, 1996.

Kuhn, T., *La structure des révolutions scientifiques*, trad. L. Meyer, Paris, Flammarion, Seconde édition, 1983. *The Structure of Scientific Revolutions*, Chicago and London, University of Chicago Press, Second Edition, 1970.

Mounier-Kuhn, P.-E., *L'informatique en France de la Seconde Guerre Mondiale au Plan Calcul. L'émergence d'une science*, Paris, PUPS, 2010.

Rivest, R., Shamir, A. et Adleman, L., « A Method for Obtaining Digital Signatures and Public-key Cryptosystems », *Communications of the ACM*, 1978, vol. 21, nº 2, pp. 120–126.

— « The Growth of Cryptography », *Conference, Killian award*, 2001, http://people.csail.mit.edu/rivest/pubs/Riv11a.slides.pdf.

Rollet, L. et Nabonnand, P., « An Answer to the Growth of Mathematical Knowledge ? The 'Répertoire bibliographique des sciences mathématiques' », *European Mathematical Society Newsletter*, mars 2003, vol. 47, pp. 9-14.

Schützenberger, M. P., « Une théorie algébrique du codage », *Séminaire Dubreil. Algèbre et théorie des nombres*, 1955-1956, vol. 9, exposé n° 15, pp. 1–24, http://www.numdam.org/item?id=SD_1955-1956__9__A10_0.

— *Contributions aux applications statistiques de la théorie de l'information,* Paris, Publications de l'Institut de Statistique de l'Université de Paris, 1953.

Segal, J., *Le zéro et le un, Histoire de la notion scientifique d'information au 20e siècle*, Paris, Editions Syllepse, 2003.

Siegmund-Schultze, R., *Mathematische Berichterstattung in Hitlerdeutschland : der Niedergang des Jahrbuchs über die Fortschritte der Mathematik, Studien zur Wissenschafts-, sozial- und Bildungsgeschichte der Mathematik*, Göttingen, Vandenhoeck et Ruprecht, 1993, vol. 9.

Stern, J., *La Science du secret*, Paris, Odile Jacob, 1998.

Stichweh, R., *Études sur la genèse du système scientifique moderne*, trad. F. Blaise, Lille, PUL, 1991.

L'INFLUENCE DE LA CRYPTOLOGIE MODERNE SUR LES MATHEMATIQUES ET L'UNIVERSITE

Jean-Louis NICOLAS[1]

INTRODUCTION

Le 20 juillet 1969, au moment où l'homme marchait pour la première fois sur la lune, se tenait à la State University of New-York at Stony Brooke l'école d'été de l'AMS (*American Mathematical Society*) « Summer School in Number Theory », consacrée à la théorie des nombres. Parmi les exposés prestigieux, il y avait celui de Daniel Shanks (1917-96), « Quadratic Forms » dont on trouvera la rédaction dans les Compte-rendus de cette école d'été[2].

Par le biais du calcul du nombre de classes $h(\Delta)$ des formes quadratiques primitives $ax^2 + bxy + cy^2$ (où a, b, c sont des nombres entiers avec $a > 0$, $c > 0$ et pgcd$(a, b, c) = 1$) de discriminant négatif $\Delta = b^2 - 4ac$ fixé[3], Shanks proposait une méthode de factorisation entièrement nouvelle, permettant de calculer les facteurs premiers des nombres ayant jusqu'à 30 ou 40 chiffres.

---

[1] jlnicola@in2p3.fr, Université de Lyon, Université Lyon1, CNRS. UMR 5208, Institut Camille Jordan Bât. Jean Braconnier, 21 Avenue Claude Bernard F-69622 Villeurbanne cedex, France. http://math.univ-lyon1.fr/~nicolas/.

[2] Shanks, « Class number, a theory of factorization, and *genera* ».

[3] On dit que la forme $f(x, y) = ax^2 + bxy + cy^2$ représente le nombre entier N s'il existe des nombres entiers x_0 et y_0 tels que $f(x_0, y_0) = N$. Sur l'ensemble $Q(\Delta)$ des formes quadratiques primitives de discriminant Δ, on définit une relation d'équivalence telle que deux formes équivalentes représentent les mêmes nombres. L'ensemble quotient $H(\Delta)$ de $Q(\Delta)$ par cette relation d'équivalence est un ensemble fini dont le cardinal est $h(\Delta)$. Gauss (voir *Disquisitiones Arithmeticae*) a défini une loi de composition de deux formes quadratiques f' et f'' de même discriminant ayant la propriété suivante : si f' représente N' et f'' représente N'', alors la composée de f' et f'' représente le produit $N'N''$.

En écoutant l'exposé de Shanks en 1969, je n'ai pas pleinement compris l'intérêt de son algorithme, tant il était éloigné des préoccupations habituelles des mathématiciens de cette époque.

Je suis maintenant de plus en plus persuadé que ce travail de Shanks a été une étape importante dans l'orientation des mathématiques vers les mathématiques effectives, c'est-à-dire les mathématiques ne se contentant pas de définir les objets, mais donnant des algorithmes, si possible rapides, permettant de les calculer.

Une décennie plus tard, l'année 1978 voyait la publication du protocole de cryptographie à clé publique RSA[4]. Ce protocole, basé sur la relative facilité à construire de grands nombres premiers et l'impossibilité de trouver les facteurs premiers de certains grands nombres composés, allait donner à cette orientation vers les mathématiques effectives un essor encore plus formidable.

Nous exposerons d'abord quelques signes de cette évolution des mathématiques. Puis, nous verrons comment s'est traduite cette évolution en termes d'enseignement avec la mise en place à Limoges, en 1985, du premier diplôme français axé sur la cryptologie. Actuellement de tels enseignements à bac + 5 existent à Bordeaux, Caen, Grenoble, Lyon, Marseille, Paris (École Polytechnique et École Normale Supérieure[5]), *etc*.

Les notions de mathématiques ou de cryptographie évoquées dans cet article sont supposées connues, au moins superficiellement, par le lecteur[6].

INFLUENCE DE LA CRYPTOLOGIE SUR LES MATHEMATIQUES

Les mathématiques avant 1978

Dans les années 1960, on n'enseignait guère l'histoire des mathématiques. Mis à part quelques exceptions (théorème de Pythagore,

[4] Du nom de ses trois inventeurs Ronald Rivest, Adi Shamir et Leonard Adleman, « A method for obtaining digital signatures and public-key cryptosystems ». James Ellis avait découvert antérieurement la cryptographie à clé publique, sur laquelle il avait écrit en 1970 un rapport secret qui n'a été divulgué qu'en 1997. Voir par exemple http://fr.wikipedia.org/wiki/James_Ellis. W. Diffie et M. E. Hellman ont publié en 1976 un autre protocole de cryptographie à clé publique. Voir le chapitre « Les nouvelles orientations de la cryptographie » pp. 186-187, et le chapitre « Pourquoi et comment la cryptologie vient de surgir dans le domaine public », pp. 209-216.

[5] NdE. : Une telle formation existe aussi à l'Université Paris 8 Vincennes-Saint-Denis depuis 2003.

[6] Pour plus d'information, on pourra consulter les ouvrages suivants : Cohen, *A Course in Computational Algebraic Number Theory* ; Crandall et Pomerance, *Prime Numbers, a Computational Perspective* ; Menezes, Van Oorschot et Vanstone, *Handbook of Applied Cryptography.*

groupe de Galois, matrice de Jordan, somme de Darboux, théorème de Rolle, ...), on ne disait ni quand ni par qui avait été introduite une notion ou démontré un théorème.

Pour les objets introduits, on donnait en général une méthode de calcul dans les cas simples, mais on ne s'occupait pas d'évaluer cette méthode dans les cas plus compliqués. On apprenait ainsi à développer un déterminant d'ordre 3 par la règle de Sarrus ou à faire des combinaisons de lignes ou de colonnes pour calculer un déterminant d'ordre 4 ; mais on ne disait pas qu'un déterminant d'ordre n se calcule en $O(n^3)$ opérations par la méthode du pivot de Gauss, pourtant connue depuis longtemps.

Par l'algorithme d'Euclide, pour calculer le pgcd de deux nombres a_1 et a_2 (avec $a_1 > a_2$), pour $i = 3, 4, 5, \ldots$, on calcule a_i, le reste dans la division de a_{i-1} par a_{i-2} jusqu'à ce que a_i soit nul. Le pgcd de a_1 et a_2 est alors a_{i-1}. Combien de divisions faut-il exécuter lorsque les deux nombres initiaux a_1 et a_2 ont 100 chiffres décimaux ?

Cette question a été résolue par le théorème de Lamé (1845) qui démontre que, pour calculer le pgcd de deux nombres a_1 et a_2 avec $a_1 > a_2$, le nombre de divisions à effectuer est inférieur à 5 fois le nombre de chiffres décimaux de a_2.

Aucun professeur de mathématiques ne m'a enseigné le théorème de Lamé, que j'ai découvert dans le livre de Knuth[7]. Pourtant, Gabriel Lamé (1795-1870) est un mathématicien connu : il a résolu le cas de l'exposant 7 dans le grand théorème de Fermat en prouvant que l'équation $x^7 + y^7 = z^7$ n'a pas de solution entière vérifiant $xyz \neq 0$. Mais en 1960, les mathématiciens ne s'intéressaient que peu à l'évaluation des algorithmes, aux mathématiques effectives et aux ordinateurs[8].

Pourtant, il y avait des exceptions. Derrick Henry Lehmer (1905-91) connaissait[9] les méthodes de calcul rapide en arithmétique, en particulier l'évaluation de l'exponentielle modulaire $ab \bmod N$, et a effectué un énorme travail de calcul. La revue *Mathematics of Computation* lui a consacré un volume spécial en 1975, pour son soixante-dixième anniversaire[10]. Nous avons vu dans l'introduction que Daniel Shanks a découvert en 1969 une nouvelle méthode de factorisation. Arthur Oliver Lonsdale Atkin (1925-

[7] Knuth « The art of computer programming ».

[8] NdE. : Les recherches de Gabriel Lamé (1795-1870) ont été cependant effectuées dans un tout autre cadre. Lamé appartient à toute une génération de polytechniciens français qui ont développé une physique mathématique rationnelle. Menés en relation étroite avec l'étude des fonctions elliptiques, ses travaux sur les coordonnées curvilignes deviendront l'outil indispensable de la géométrie différentielle. Ils le conduiront à la théorie des nombres. Lamé est également connu pour son analyse de la complexité algorithmique de l'algorithme d'Euclide.

[9] Lehmer « Computer technology applied to the theory of numbers ». Voir le chapitre « Cryptographie et théorie des nombres » pp. 256-258.

[10] Collectif, « Special issues of mathematics of computation ».

2008) a utilisé les tout premiers ordinateurs et organisé le colloque *Computers in Number Theory* qui s'est tenu à Oxford[11] du 18 au 23 août 1969.

En France aussi, quelques mathématiciens commençaient à s'intéresser à ces questions ainsi qu'aux premiers logiciels de calcul formel ; citons notamment Maurice Mignotte à St-Denis[12] puis Strasbourg, Henri Cohen à Bordeaux et Grenoble, Georges et Marie-Nicole Gras à Grenoble puis Besançon. On lira en annexe l'échange de lettres en 1974 avec le grand informaticien Marcel-Paul Schützenberger (1920-96) sur la mise en place d'un centre de calcul spécialisé en arithmétique. Le colloque « Utilisation des ordinateurs en Mathématiques » a réuni à Limoges en septembre 1975 un ensemble de mathématiciens prêts à s'investir dans ces sujets[13].

En conclusion, on voit qu'il existait autour de l'utilisation des ordinateurs en théorie des nombres et du calcul formel un bouillonnement d'idées qui sera largement amplifié par la découverte de la cryptographie à clé publique. Le développement des logiciels de calcul formel Pari/GP, Sage, Magma, Maple, *etc*. en a grandement profité.

Questions développées sous l'influence de la cryptologie

Le protocole de cryptographie RSA et celui du logarithme discret font jouer un grand rôle aux nombres premiers et à la décomposition en facteurs premiers des nombres composés[14].

Un *test de primalité* prend en entrée un nombre N et, en sortie, déclare si le nombre est premier ou composé. Un *algorithme de factorisation* prend en entrée un nombre N garanti composé par un test de primalité et donne en sortie deux nombres différents de 1 dont le produit vaut N.

La méthode dite des divisions successives, qui consiste à diviser N par les nombres premiers inférieurs ou égaux à $\sqrt{N}$, est à la fois un test de primalité et un algorithme de factorisation. Mais la plupart des algorithmes de factorisation énumérés ci-après ne prouvent pas qu'un nombre est premier.

Plusieurs tests de primalité et algorithmes de factorisation ont été découverts dans les années 1970, mais il faudra attendre les années 1980 pour voir apparaître les algorithmes les plus efficaces.

---

[11] Ed. Atkin et Birch, *Computers in number theory*.

[12] NdE. : Maurice Mignotte a d'abord enseigné à l'université Paris XIII, qui avait une antenne dans la ville de Saint-Denis.

[13] Collectif, « Utilisation des ordinateurs en mathématiques ».

[14] Voir les chapitres « Nouvelles orientations de la cryptographie » p. 173 et « Pourquoi et comment la cryptographie vient de surgir dans le domaine public ? » p. 203.

Tests de primalité

La méthode des divisions successives est connue depuis l'Antiquité ; en dehors de la méthode $N - 1$ introduite par Édouard Lucas (1842-91) à la fin du 19e siècle[15], les autres méthodes décrites ci-dessous sont postérieures à 1970.

Méthode N – 1 ou N + 1. Elle permet de tester la primalité du nombre N lorsque l'on connait les facteurs premiers de $N - 1$ ou de $N + 1$.

Test probabiliste d'Artjuhov-Miller-Rabin. Ce test dit qu'un nombre est premier avec une très forte probabilité[16]. Cependant, il ne garantit pas que le nombre testé soit premier. Mais il est rapide et il faut l'utiliser avant d'appliquer l'un des tests non probabilistes cités ci-dessous.

Test probabiliste des suites de Lucas. Les suites de Lucas sont les suites récurrentes linéaires d'ordre 2, c'est-à-dire définies par leurs deux premiers termes x_0 et x_1 et par la relation de récurrence $x_{n+2} = ax_{n+1}+bx_n$. La plus célèbre est la suite de Fibonacci, avec $x_0 = 0$, $x_1 = 1$, $a = 1$, $b = 1$. Ces suites permettent de construire un test probabiliste qui, comme le test d'Artjuhov-Miller-Rabin, est rapide mais ne permet pas de garantir la primalité du nombre testé.

Test des sommes de Jacobi. Ce test a été publié en 1983 par Adleman, Pomerance et Rumely puis implémenté par Cohen et Lenstra[17]. Le temps nécessaire à prouver la primalité du nombre N est $O((\log N)^{\log\log\log N})$, ce qui est presque polynomial en $\log N$.

Test utilisant les courbes elliptiques. Shafi Goldwasser[18] et Joe Kilian ont publié en 1986 un premier test théorique. Le test ECPP (Elliptic Curve Primality Proving) publié par Atkin et Morain[19] en 1993 permet de tester de grands nombres au hasard[20]. En décembre 2012, le teste CIDE (*Cyclotomy Initialized by Dual Elliptic tests*) de Pedra Mihailescu a permis à Jens Franke, Thorsen Kleinjung, Andreas Decker et Anna Grosswendt de prouver la primalité du nombre de 30 008 chiffres : $8656^{2929} + 2929^{8656}$, ce qui est le record actuel pour un nombre « au hasard ».

Test AKS (Agrawal, Kayal, Saxena). Cet algorithme, publié en 2004, montre que l'on peut tester la primalité de N en $O((\log N)^c)$ étapes, autrement dit, que ce test est polynomial en $\log N$. Malheureusement,

---

15 Voir le chapitre « Cryptographie et théorie des nombres » pp. 258-259.

16 Voir plus loin le paragraphe « Nombres premiers avec une grande probabilité ».

17 Voir le chapitre « Pourquoi et comment la cryptologie vient de surgir dans le domaine public ? » p. 214.

18 *ibid.*, p. 217.

19 Atkin et Morain, « Elliptic curves and primality proving » ; « Finding suitable curves ».

20 Par le test ECPP, le nombre « au hasard » de 20 562 chiffres décimaux :
$(((((((((2^3 + 3)^3 + 30)^3 + 6)^3 + 80)^3 + 12)^3 + 450)^3 + 894)^3 + 3636)^3 + 70756)^3 + 97220$ a été prouvé premier en 2006, voir http://primes.utm.edu.

jusqu'à maintenant, cette vitesse n'est que théorique ; aucune version implémentée ne permet de rivaliser avec les deux précédents tests.

Méthodes de factorisation

CFRAC. Très peu de temps après la méthode de factorisation de Shanks (1969) apparaissait un autre algorithme de factorisation, la méthode CFRAC utilisant les fractions continues[21], qui donnait les deux facteurs premiers du nombre de Fermat $F_7 = 2^{128} + 1$, un nombre de 39 chiffres.

CLASSNO et SQUFOF. Après avoir publié son premier algorithme de factorisation CLASSNO[22], Shanks en découvrit un deuxième, SQUFOF, utilisant les formes quadratiques, cette fois à discriminant négatif. L'algorithme peut se programmer en peu d'instructions et travaille essentiellement sur des nombres dont le nombre de chiffres est inférieur à la moitié du nombre de chiffres du nombre à factoriser. En 1973, sont apparues les premières calculettes programmables, et l'algorithme SQUFOF implémenté sur ces machines, permettait de factoriser des nombres de 18 chiffres décimaux[23].

Algorithme de Lehman. Factoriser un nombre impair sous la forme $N = a \times b$ est équivalent à l'écrire sous forme d'une différence de deux carrés $N = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$. Par cette observation, Fermat avait trouvé une méthode simple pour décomposer en facteurs premiers les nombres qui ont deux facteurs voisins de $\sqrt{N}$. En améliorant la technique de Fermat, Sherman Lehman a obtenu un algorithme de factorisation (qui est aussi un test de primalité) en $O(N^{1/3})$.

La méthode ρ de Pollard. C'est un algorithme probabiliste, basé sur le paradoxe des anniversaires, très simple à programmer, dont le temps de calcul est $O(N^{1/4})$.

Les méthodes p – 1 et p + 1 de Pollard. Ces méthodes permettent de trouver les facteurs premiers p d'un nombre N tels que $p - 1$ (ou $p + 1$) n'ait que des petits facteurs premiers.

Le crible quadratique. Pour factoriser N, on considère le polynôme $P(x) = \left(x + \lfloor \sqrt{N} \rfloor\right)^2 - N$, et l'on recherche les petites valeurs de x telles que $P(x)$ soit friable, c'est-à-dire n'ait que des petits facteurs premiers. Cette recherche peut se faire rapidement par une technique de crible. Cet algorithme, publié en 1982 par Carl Pomerance (né en 1944), a permis en

[21] Morisson et Brillhart, « The Factorization of F_7 », « A Method of Factoring and the Factorization of F_7 ».
[22] Shanks, « Class Number, a Theory of Factorization ».
[23] Nicolas, « Une méthode de factorisation ».

1983 de factoriser le nombre $(10^{71} – 1)/9$ qui s'écrit avec 71 chiffres 1. La méthode MPQS (*Multiple Polynomial Quadratic Sieve*) remplace le polynôme $P(x)$ par d'autres polynômes du second degré.

L'algorithme ECM (Elliptic Curve Method). Soit p un facteur premier inconnu du nombre N à factoriser. On choisit au hasard une courbe elliptique $y^2 = x^3 + ax + b$, en espérant que son nombre de points sur le corps $\mathbb{F}_p$ soit friable, c'est-à-dire n'ait que des petits facteurs premiers. Cet algorithme a été publié en 1987 par Hendrik Lenstra Jr[24].

Le crible du corps de nombres. C'est actuellement la méthode la plus performante. Elle travaille à la fois dans le corps $\mathbb{Q}$ des nombres rationnels et dans un corps de nombres $\mathbb{Q}(\theta)$, où θ est un nombre algébrique bien choisi. La version initiale, suggérée par John Pollard en 1988, permettait de factoriser les nombres de la forme $a^n + b^n$, par exemple les nombres de Mersenne[25] ou de Fermat[26]. Généralisée aux nombres quelconques, cette méthode a permis la factorisation d'un nombre de 232 chiffres, ce qui est le record actuel. On lira avec intérêt l'article de Pomerance sur ce sujet[27].

En conclusion, on constate la variété des domaines mathématiques intervenant dans ces différents algorithmes de factorisation. Enfin, rappelons que si les ordinateurs quantiques fonctionnent un jour, ils résoudront rapidement le problème de factorisation.

Théorie de la complexité

Le principe du protocole de cryptographie RSA est basé sur la possibilité de construire de grands nombres premiers p et q (de, disons, 150 chiffres) et sur l'impossibilité actuelle de retrouver les facteurs premiers p et q à partir de leur produit (la fonction : $(p, q) \rightarrow p \times q$ est une fonction à sens unique[28]).

Mais cette impossibilité est-elle inhérente au problème ou bien est-elle due à notre ignorance actuelle ? Nous avons vu dans les tests de primalité que la méthode AKS testait la primalité d'un nombre N en temps polynomial par rapport au nombre de chiffres de N. Existe-t-il un algorithme polynomial de factorisation ?

En théorie de la complexité, la classe ***P*** réunit les problèmes qui peuvent être décidés en temps polynomial par rapport à la taille des données. Par l'algorithme AKS, le problème de primalité appartient à la classe ***P***. La

[24] Lenstra, « Factoring integers with elliptic curves ».
[25] Voir la note 28, p. 235.
[26] Voir page précédente.
[27] Pomerance, « A tale of two sieves ».
[28] Voir le chapitre « Les nouvelles orientations de la cryptographie » pp. 196-199, et plus loin le paragraphe « Fonctions à sens unique ».

classe ***NP*** contient les problèmes de décision qui admettent un algorithme polynomial capable de tester la validité d'une de leurs solutions. Le problème de factorisation appartient à la classe ***NP***. La fameuse conjecture[29] ***P*** = ***NP*** entraînerait que le problème de factorisation est dans la classe ***P*** et donc il existerait un algorithme de factorisation polynomial en le nombre de chiffres de l'entrée *N*.

Pour rendre le protocole RSA caduc, encore faudrait-il qu'un tel algorithme de factorisation soit performant en pratique.

Courbes elliptiques

Les courbes elliptiques sont les courbes les plus simples après les droites et les coniques. On peut ramener leur équation à la forme de Weierstrass :

$$y^2 = x^3 + ax + b, \qquad 4a^3 + 27b^2 \neq 0.$$

Sur une telle courbe on définit l'addition de deux points. L'élément neutre 0 de cette addition est le point à l'infini dans la direction [*Oy*), et trois points alignés ont pour somme 0. L'ensemble des points de la courbe muni de cette opération est un groupe abélien.

On peut considérer une courbe elliptique sur un corps fini, par exemple $\mathbb{F}_p$. C'est de cette façon que les courbes elliptiques interviennent dans les tests de primalité, dans la méthode de factorisation ECM et dans certains protocoles de cryptographie. Cela a suscité de nombreux travaux, par exemple sur le calcul du nombre de points d'une courbe elliptique sur un corps fini de grande taille.

L'algorithme LLL

Cet algorithme a été publié en 1982 par Henrik Lenstra, Arjen K. Lenstra et László Lovász pour trouver les facteurs irréductibles d'un polynôme à coefficients entiers. Depuis, il est devenu un outil incontournable tant en théorie algébrique des nombres qu'en cryptographie.

[29] Smale, « Mathematical problems for the next century ».

Quelques nouveaux concepts

Nombre premier avec « grande probabilité »

Le petit théorème de Fermat[30] affirme que, si p est un nombre premier, $2^{p-1} - 1$ est multiple de p. La réciproque n'est pas vraie ; il existe une infinité de nombres N composés, appelés pseudo-premiers en base 2, qui vérifient :

$$2^{N-1} - 1 \equiv 1 \pmod{N}. \quad (1)$$

Le plus petit est $341 = 11 \times 31$. Mais ces nombres sont très rares, et si le nombre N vérifie la congruence (1), on peut parier, avec de grandes chances de gagner, qu'il est premier.

Le test d'Artjuhov-Miller-Rabin est une condition nécessaire de primalité encore plus forte que le test donné par l'équation (1). Cohen dit qu'un nombre N qui passe le test d'Artjuhov-Miller-Rabin est un nombre premier de qualité industrielle : si l'on utilise un tel nombre dans la construction d'un protocole de cryptographie, la probabilité que ce nombre soit composé est beaucoup plus faible que la probabilité d'une erreur humaine dans la gestion de ce protocole.

Mais pour un mathématicien, un nombre est premier ou il ne l'est pas, et cette notion de nombre premier avec grande probabilité engendrée par les tests probabilistes a suscité de nombreuses discussions.

Certificat de primalité

Il est facile de vérifier le résultat d'un algorithme de factorisation qui annonce d comme diviseur de N : il suffit de calculer le reste dans la division de N par d, et de constater que ce reste est nul. La plupart des algorithmes cités dans les méthodes de factorisation s'appuient sur des raisonnements heuristiques et probabilistes, mais leur temps de calcul est non prouvé ; cependant en pratique, ils fonctionnent. Le cas des tests de primalité est très différent. Que penser d'un algorithme qui, après des heures de calcul, déclare « N est premier » ou « N est composé » ?

Il peut y avoir une erreur. Un certificat de primalité est un ensemble de données qui permet de vérifier que le nombre est bien premier. La méthode des divisions successives n'a pas de certificat de primalité.

La méthode $N - 1$ des tests de primalité donne comme certificat la liste des facteurs premiers de $N - 1$ accompagnés de leur certificat de primalité.

---

[30] Voir le chapitre « Cryptographie et théorie des nombres » pp. 255-258.

Les tests ECPP et CIDE admettent un certificat de primalité, mais pas le test des sommes de Jacobi.

Fonctions « à sens unique »[31]

Soit p et q deux nombres premiers; il est facile (c'est un problème de la classe $\boldsymbol{P}$)[32] de calculer le produit $N = p \times q$. Réciproquement, les mathématiques disent que N est un produit de facteurs premiers, mais il est difficile de calculer p et q à partir de N, c'est un problème de la classe $\boldsymbol{NP}$. On dit que l'application : $(p, q) \to N = p \times q$ est une fonction à sens unique. Chaque protocole de cryptographie à clé publique est basé sur une fonction à sens unique. L'application : $(p, q) \to N$ est à la base du protocole RSA.

Soit p un nombre premier. Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, c'est-à-dire qu'il existe un générateur g tel que les deux ensembles $\{1, 2, \ldots, p-1\}$ et $\{g \bmod p, g^2 \bmod p, \ldots, g^{p-1} \bmod p = 1\}$ coïncident. L'application : $a \to g^a \bmod p$ est une permutation de l'ensemble $\{1, 2, \ldots, p-1\}$. Par exemple, 3 est un générateur de $(\mathbb{Z}/7\mathbb{Z})^\times$; les puissances de 3 modulo 7 sont 3, 2, 6, 4, 5, 1.
À partir de a, le calcul de $x = g^a \bmod p$ est facile par l'algorithme des puissances. Mais, à partir de x, le calcul de a, appelé logarithme discret de x en base g, est en général plus compliqué. Nous avons là encore une fonction à sens unique.
La fonction à sens unique du logarithme discret existe aussi dans le groupe des éléments non nuls d'un corps fini (où p est premier) ainsi que dans le groupe des points d'une courbe elliptique sur un corps fini. Ces groupes sont utilisés en cryptographie.

Zéro connaissance[33]

Comment Alice peut-elle prouver à Bob qu'elle connaît un secret sans rien révéler de ce secret ? Cette situation se présente si Bob est le banquier d'Alice et si Alice veut retirer de l'argent à sa banque. Elle ne veut pas donner son secret à Bob pour ne pas risquer d'être escroquée, si celui-ci est malhonnête.

Alice doit fournir à Bob une preuve à divulgation nulle de connaissance. On trouvera sur le site http://fr.wikipedia.org/wiki/Preuve_ à_divulgation_ nulle_de_connaissance un schéma simple d'une telle preuve.

---

[31] Voir le chapitre « Les nouvelles orientations de la cryptographie » pp. 188-191.
[32] Voir plus haut le paragraphe « Théorie de la complexité ».
[33] Voir le chapitre « Pourquoi et comment la cryptologie a envahi le domaine public ? » pp. 217-225.

Le mathématicien et le cryptographe

Neal Koblitz est un mathématicien qui a suivi de près les mathématiques et leur rapprochement avec la cryptographie. Il a écrit plusieurs ouvrages sur le sujet[34].

Dans l'excellent article « The uneasy relationship between mathematics and cryptography » [35], il compare les méthodes de travail du cryptographe et du mathématicien. Le mathématicien, et particulièrement le théoricien des nombres, s'attaque à un problème ouvert, souvent ancien, et dans le meilleur des cas, le résout, mais, plus fréquemment, apporte une contribution positive en direction de la solution. Le cryptographe, comme le biologiste ou l'informaticien, est pris dans la spirale du temps et prépare activement sa présentation au prochain congrès, quelquefois aux dépens d'une réflexion approfondie.

Je recopie ci-dessous les dernières lignes de cet article :

> « *Cryptography has the excitement of being more than just an academic field. Once I heard a speaker of NSA complain about university researchers who are cavalier about proposing untested cryptosystems. He pointed out that in the real world if your cryptography fails, you lose a million dollars or your secret agent gets killed. In academia, if you write about a cryptosystem and then a few months later find a way to break it, you've got two newspapers to add to your résumé!*
> *Drama and conflict are inherent in cryptography, which, in fact can be defined as the science of transmitting and managing information in the presence of an adversary. The "spy* vs. *spy" mentality of constant competition and rivalry extends to the disciplinary culture of the field. This can get to be excessive – and even childish at times – but it also explains in part why it can be so much fun to do research in cryptography* ».

Il est sans doute bon d'avoir un regard sur les applications immédiates, sans perdre de vue les grands objectifs qui permettent les avancées de la Science. On notera que, dans les universités, la cryptographie est enseignée, tantôt en mathématiques, tantôt en informatique.

---

[34] Par exemple Koblitz, *A course in number theory and cryptography*.

[35] Cet article est traduit au chapitre « La relation agitée entre mathématiques et cryptographie » pp. 285-303.

INFLUENCE DE LA CRYPTOLOGIE SUR L'UNIVERSITE

Création du DEA de Limoges

Au début des années 1980, il n'y avait pas d'enseignement de troisième cycle en mathématiques à l'Université de Limoges. Pourtant, le département de mathématiques, avec une trentaine d'enseignants, en avait le potentiel ; mais le MEN (Ministère de l'Éducation Nationale) ne souhaitait pas augmenter le nombre d'universités habilitées à délivrer un diplôme de troisième cycle. Il fallait donc trouver une idée un peu originale pour avoir quelques chances d'obtenir une habilitation.

Or, au printemps 1984, Pomerance a passé trois mois comme professeur invité à Limoges. De plus, le congrès *Eurocrypt*, qui avait eu lieu en 1982 à Burg Feuerstein[36] (Allemagne) et à Udine (Italie) en 1983, se tenait à la Sorbonne en mai 1984, et, pour la première fois, sous les hospices de l'IACR (*International Association of Cryptology Research*). À l'automne 1984, au moment de préparer les dossiers de demande de création de nouvelles filières, les enseignants limougeauds se dirent que la cryptographie pourrait être un atout.

Il n'était pas clair, à cette époque, de prévoir combien d'étudiants pourraient trouver un emploi dans la cryptographie. À côté de l'équipe de recherche en théorie des nombres, calcul formel et cryptographie, il y avait une équipe d'analyse numérique, spécialisée dans les problèmes d'optimisation. Il nous a semblé qu'une formation à Bac + 5, donnant aux étudiants les notions de base dans les domaines de ces deux équipes et accompagnée d'une bonne pratique de l'informatique ainsi que d'un stage en entreprise devrait permettre à ces étudiants d'obtenir un travail intéressant. La branche « Cryptographie » de Thomson-CSF (maintenant THALES) promettait d'accueillir nos étudiants en stage.

C'est sur ce schéma que fût adressée au Ministère de l'Éducation Nationale la demande de création du DEA[37] de mathématiques avec la mention « Cryptographie et Optimisation ». Dans la commission d'étude des dossiers, il y avait Jean-Louis Stehlé, qui travaillait alors chez IBM, et qui a fortement soutenu notre dossier ; finalement, ce DEA fût habilité.

Il semble que c'était la première fois qu'un enseignement de cryptographie se faisait en dehors d'un établissement militaire. Je me rappelle avoir envoyé au Service du Chiffre le programme détaillé de chacun des modules de ce DEA.

---

[36] Voir le chapitre « Cryptographie et théorie des nombres » p. 252.

[37] Diplôme d'Études Approfondies. Cet enseignement à Bac + 5 correspond maintenant à la deuxième année de Master.

Les premiers cours eurent lieu à l'automne 1985. Dans les deux premières promotions il y eut comme étudiant François Morain, actuellement professeur à l'École Polytechnique et Thierry Berger maintenant professeur à l'Université de Limoges.

En 2012-2013, la cryptologie continue d'être enseignée à l'Université de Limoges[38].

Influence sur la Recherche

En juillet 1988, l'AMS (*American Mathematical Society*) organisait dans le Maine un colloque présidé par Pomerance sur le sujet « Computational Number Theory »[39]. Daniel Barsky, qui présidait alors la commission du CNRS, favorisa la mise en place d'un PICS (Projet International de Coopération Scientifique) du CNRS avec les États-Unis qui permit de financer le voyage d'une vingtaine de mathématiciens français pour participer à ce colloque.

Peu après, sous la direction de Jacques Martinet, se créait à Bordeaux le laboratoire A2X (Équipe de Théorie des Nombres et d'Algorithmique Arithmétique), qui officialisait le travail important accompli par plusieurs mathématiciens bordelais dans l'utilisation des ordinateurs en théorie des nombres. Ce laboratoire s'est naturellement ouvert vers la théorie des codes et la cryptographie ; en particulier, les questions développées sous l'influence de la cryptologie y ont fait l'objet d'études fructueuses et tout laisse à penser que ces recherches ne s'arrêteront pas de sitôt.

Le DESS de Lyon

Nommé à Lyon en octobre 1988, je souhaitais y introduire un enseignement de cryptologie. Justement, l'Université Claude Bernard (Lyon 1) mettait en place à la rentrée 1989 un DESS[40] d'Ingénierie mathématique. Il comprenait un tronc commun et trois options, Analyse Numérique, Statistiques et Finances.

Dans le tronc commun, il y avait une initiation à la cryptographie et aux mathématiques sous-jacentes. Trois ans plus tard, s'ouvrit une quatrième option, Mathématiques Discrètes, qui recrutait plus particulièrement des étudiants de la Maîtrise de Mathématiques Discrètes, et qui incluait un

[38] Voir le site http ://www.cryptis.fr.
[39] Collectif, « Joint Summer Research Conference ».
[40] Diplôme d'Études Supérieures Spécialisées. Comme le DEA, cet enseignement à Bac + 5 correspond maintenant à la deuxième année de Master.

enseignement complémentaire de cryptographie. Plusieurs étudiants de cette option ont fait leur stage en entreprise dans le domaine de la cryptographie.

Au moment de la mise en place des Masters, les enseignements de cryptographie de ce DESS ont été transférés en deuxième année du Master de Lyon, mention Mathématiques et applications, Ingénierie mathématique et y sont encore en place[41] en 2012-2013.

BIBLIOGRAPHIE

Atkin, A. O. L. et Morain, F., « Finding Suitable Curves for the Elliptic Curve Method of Factorization ». *Mathematics of Computation*, 1993, vol. 60, pp. 399-405

— « Elliptic Curves and Primality Proving ». *Mathematics of Computation*, 1993, vol. 61, pp. 29-68.

(eds.) Atkin A. O. L. et Birch B. J., « Computers in Number Theory ». *Proceedings of the Science Research Council Atlas Symposium n°. 2*, held at Oxford, from 18-23 August 1969, Londres, New-York, Academic Press, 1971.

Collectif, « Special Issue of Mathematics of Computation dedicated to D. H. Lehmer », *Mathematics of Computation*, 1975, vol. 29.

Collectif, « Utilisation des ordinateurs en mathématiques, Colloque de Limoges, septembre 1975 », *Bulletin de la Société Mathématique de France*, 1977, Mémoire 49-50.

Collectif, « Joint Summer Research Conferences in the Mathematical Sciences », Bowdoin College, Brunswick, Maine, July 9 to July 15, *Computational Number Theory*, Notices of the American Mathematical Society, 1987, n° 34, pp. 1134-1135.

Cohen, H., *A course in Computational Algebraic Number Theory*. Graduate texts in Mathematics n° 138, Berlin, Springer Verlag, 1993.

Crandall, R. et Pomerance, C., *Prime Numbers, A Computational Perspective*, Berlin, Springer Verlag, 2001.

Gauss, C. F., *Disquisitiones Arithmeticae*, Traduit et prefacé par A. A. Clarke, révisé par W. C. Waterhouse, C. Greithe et A. W. Grootendorst New York, Springer Verlag, 1986.

Knuth, D. E., *The Art of Computer Programming*, vol. 2, *Seminumerical Algorithm*. New York, Addison-Wesley, 1981, 2e édition.

Koblitz, N., *A course in number theory and cryptography*, Graduate Texts in Mathematics, vol. 114. New York, Springer Verlag, 1987.

[41] Voir le site http://mastermath.univ-lyon1.fr.

— « The Uneasy Relationship between Mathematics and Cryptography », *Notices of the A.M.S.*, 2007, vol. 54, pp. 972-979.

Lehmer, D. H., « Computer Technology Applied to the Theory of Numbers ». *in* (éd.) W. J. Leveque, *Studies in Number Theory*, Washington D. C. Mathematical Association of America, 1969, pp. 117-151.

Lenstra, H., « Factoring integers with elliptic curves », *Annals of Mathematics*, 1987, 2nd series, vol. 126, n° 3, pp. 649-673.

Menezes, A. J., van Oorschot, P. C. et Vanstone, S. A., *Handbook of Applied Cryptography*, Boca Raton, CRC Press, 1997.

Morrison, M. A. et Brillhart, J., « The Factorization of F_7 », *Bulletin of the American Mathematical Society*, 1971, vol. 77, n° 2, pp. 264-264.

— « A Method of Factoring and the Factorization of F_7 », *Mathematics of Computation*, 1975, vol. 28, n° 129, pp. 183-205.

Nicolas. J.-L. « Une méthode de factorisation utilisant les formes quadratiques à discriminant positif », *L'Iremois, publication de l'IREM de Limoges*, 1981, n° 6, pp. 3-12.

Pomerance, C., « A tale of two sieves », *Notices of the American Mathematical Society*, 1996, vol. 43, n° 12, pp. 1473-1485.

Rivest, R. L., Shamir, A. et Adleman, L., « A Method for Obtaining Digital Signatures and Public-Key Cryptosystems », *Communications of the Association for Computing Machinery*, 1978, vol. 21, n° 2, pp. 120-126.

Shanks, D., « Class Number, a Theory of Factorization, and Genera », 1969, Number Theory Institute, Stony Brooke, N. Y., *Proceeding of the Symposium on Pure Mathematics*, American Mathematical Society, 1971, vol. 20, pp. 415-440.

Smale. S. « Mathematical Problems for the Next Century ». *The Mathematical Intelligencer*, 1998, vol. 20, n° 2, pp. 7-15. Traduction *in* « Problèmes mathématiques pour le prochain siècle », *Gazette de la Société Mathématique de France*, 2000, n° 83, pp. 11-27.

ANNEXE

Lettre de J.-L. Nicolas à M.-P. Schützenberger[42] Limoges, le 2 mai 1974,

Cher Monsieur,

Je vous envoie le menu des prochaines journées arithmétiques (27 mai – 1er juin) à Bordeaux. J'ai écrit à P. Damey, organisateur, pour qu'il vous envoie les renseignements techniques. Avec quelques autres arithméticiens qui s'intéressent aux calculs sur ordinateur (dont Mignotte de Paris XIII = St Denis), nous souhaiterions organiser quelque chose comme un centre de calcul spécialisé (au moins en partie) en arithmétique. L'idée est vaste et peu précise et je voudrais profiter des journées de Bordeaux pour la préciser. Vous avez sûrement des idées intéressantes sur ce sujet et vous connaissez plusieurs personnes qui en ont aussi. C'est une raison de plus d'espérer votre venue à Bordeaux.

Avec mes meilleurs sentiments,

J.-L. Nicolas

[42] Voir note p. 43, p. 261.

Lettre de M.-P. Schützenberger à
J.-L. Nicolas

jeudi

Cher ami,

Merci de votre retransmission.

J'aimerais avoir plus de détail sur la réunion de Bordeaux où je voudrais beaucoup avoir la possibilité de venir

Peut-être que nous nous y rencontrons

Amitié

M-P Schützenb-

97 rue du Ranelagh-
Paris XVI
647-67-02.

LA RELATION AGITEE ENTRE MATHEMATIQUES ET CRYPTOGRAPHIE[1]

Neal KOBLITZ[2]
Traduction Marie-José DURAND-RICHARD et Philippe GUILLOT

Au cours des six mille premières années, jusqu'à l'invention des clés publiques dans les années 1970, les mathématiques utilisées en cryptographie n'étaient généralement pas très intéressantes. Même au vingtième siècle, les cryptographes utilisaient peu les concepts de pointe des mathématiques. En effet, les mathématiciens qui s'intéressaient à la cryptographie dans ces années-là auraient volontiers adhéré à la déclaration méprisante de Paul Halmos[3] : « les mathématiques appliquées sont de mauvaises mathématiques »[4].

Il y a cependant quelques exceptions. Dans les années 1940, Alan Turing, le père de la science informatique, a travaillé intensivement en cryptographie. Il a en particulier montré comment utiliser des techniques statistiques sophistiquées pour décrypter un code[5]. Claude Shannon, le père

---

[1] NdT. : la version originale de cet article a été publiée sous le titre « The Uneasy Relationship between Mathematics and Cryptography » dans *Notices of the AMS*, septembre 2007, vol. 54, n° 8, pp. 972-979. Nous tenons à remercier Neal Koblitz et l'AMS pour nous avoir gracieusement accordé le droit de publier cette traduction.

[2] Neak Koblitz est professeur de mathématiques à l'Université de Washington, Seatle. Son courriel est *koblitz@math.washington.edu.*

Cet article repose sur une conférence invitée donnée à la réunion de l'AMS au *Steven Institute of Technology* à Hoboken, NJ, le 14 avril 2007. Certaines parties sont extraites du chapitre sur la cryptographie de son ouvrage à venir *Random Curves : Journeys of a Mathematician*, à paraître chez Springer Verlag. [NdT. : Ce livre est paru en 2008].

[3] NdT. : Paul R. Halmos (1916-2006) est un mathématicien d'origine hongroise, émigré aux États-Unis en 1929, et spécialiste de la théorie des ensembles. Il est l'auteur d'une autobiographie intitulée *I Want to Be a Mathematician. Automathography* (1985).

[4] NdT. : *Applied Mathemathics is Bad Mathematics in* L. A. Steen (ed.), *Mathematics Tomorrow*, New-York, Springer Verlag, 1981.

[5] NdT. : Voir le chapitre « L'ancrage de la cryptologie dans les jeux d'écriture » p. 59.

de la théorie de l'information, a travaillé sur les fondements de la cryptographie[6].

Dans la même décennie, G. H. Hardy a écrit, dans son *Apologie d'un mathématicien* :

> « À la fois Gauss et de moindres mathématiciens peuvent se réjouir qu'il y ait une science [la théorie des nombres] qui de toutes façons, et selon eux, devrait rester éloignée des activités humaines ordinaires, et rester noble et propre ».

Du temps de Hardy, la plupart des applications des mathématiques étaient militaires, et un pacifiste comme lui était heureux de constater que la théorie des nombres n'était pas étudiée pour son utilité pratique, mais seulement pour sa valeur esthétique intrinsèque.

Cette image d'une théorie des nombres « noble et propre » a eu un grand succès jusqu'en 1977, lorsque trois chercheurs en informatique du *Massachusetts Institute of Technology* – Ron Rivest, Adi Shamir et Len Adleman – ont inventé un système cryptographique radicalement nouveau. Un article paru dans *Scientific American* de Martin Gardner a décrit l'idée du RSA, expliqué sa signification, et provoqué un regain soudain d'intérêt populaire pour la cryptographie et la théorie des nombres[7].

Dans ces années-là, le RSA était la principale façon de réaliser ce qui allait devenir la « cryptographie à clé publique ». Les systèmes antérieurs pour brouiller les messages convenaient aux applications militaires ou diplomatiques, où seule une hiérarchie arrêtée de personnes était autorisée à connaître les clés secrètes. Mais dans les années 1970, de larges pans de l'économie se sont rapidement informatisés, les limites de la cryptographie classique devinrent manifestes. Supposons par exemple qu'un grand réseau de banques veuille pouvoir échanger des messages chiffrés pour autoriser les transferts d'argent. En cryptographie traditionnelle, deux banques doivent toujours s'accorder sur leur propre clé secrète pour échanger en toute confiance sur un service de messagerie. Le nombre de paires possibles atteint facilement les centaines de millions. Par conséquent, la cryptographie antérieure, dite « à clé privée » (ou « à clé symétrique »), devient extrêmement peu maniable.

En cryptographie à clé publique, la clé nécessaire pour embrouiller un message est une donnée publique. Chaque utilisateur du système (par exemple, chaque banque) dispose de sa propre clé publique, inscrite dans un annuaire un peu comme un numéro de téléphone. N'importe qui peut chiffrer

---

[6] NdT. : voir les chapitres « Du message chiffré au système cryptographique » pp. 127-142 et « Pourquoi et comment la cryptologie a envahi le domaine public ? » pp. 203-207.

[7] NdT. : voir le chapitre « Pourquoi et comment la cryptologie a envahi le domaine public ? » pp 209-216.

un message en utilisant cette clé publique. Toutefois, le processus de déchiffrement exige la connaissance d'une clé totalement différente, que le destinataire garde secrète. La procédure pour embrouiller un message est appelée une « fonction à sens unique avec trappe »[8]. Cela signifie qu'une fois que nous avons la clé publique de la banque, il est facile de calculer (à l'aide d'un ordinateur) le message chiffré à envoyer. Si toutefois, nous voulons aller dans l'autre sens – désembrouiller le message – cela est mathématiquement impossible, à moins de posséder une information supplémentaire, à savoir la clé secrète.

Rivest, Shamir et Adleman ont conçu un moyen ingénieux – et simple – pour réaliser une fonction à sens unique avec trappe, en utilisant la théorie élémentaire des nombres. Leur construction repose sur la multiplication de deux grands nombres premiers p et q pour obtenir un nombre composé $N = pq$. On peut supposer qu'il s'agit d'un processus à sens unique, en ce sens que factoriser N pour retrouver p et q est très difficile.

Ainsi, la sécurité de la cryptographie RSA est entièrement tributaire de la difficulté présumée de la factorisation de grands nombres entiers. Pour cette raison, l'invention du RSA a donné une impulsion considérable à l'étude des méthodes de factorisation des entiers, et aussi des méthodes pour produire aléatoirement de grands nombres premiers. Au début des années 1980, les points forts de la cryptographie mathématique étaient pour la plupart dans ce domaine – par exemple, le développement par Carl Pomerance de l'amélioration des techniques de crible pour les algorithmes de factorisation, et la preuve déterministe de primalité en temps quasi polynomial d'Adleman-Pomerance-Rumely à l'aide des sommes de Jacobi[9].

Dans une veine un peu différente, Don Coppersmith mit au point un algorithme qui pouvait trouver le logarithme discret dans le groupe multiplicatif de F_{2^n} en temps $\exp(n^{1/3+\varepsilon})$, ce qui est bien plus rapide que les méthodes antérieures de calcul de logarithme. Cela a également eu un impact en cryptographie, du fait qu'El Gamal a proposé une alternative au chiffrement RSA[10] reposant sur la difficulté présumée à inverser la fonction : $x \mapsto g^x$ (où g est fixé) dans un corps fini.

[8] NdT. : voir le chapitre « Les nouvelles orientations de la cryptographie » p. 192.
[9] NdE. : le lecteur trouvera de nombreuses références aux travaux de Carl Pomerance dans le chapitre « L'influence de la cryptologie moderne sur les mathématiques et l'université » notamment p. 267.
[10] NdT. : contrairement au RSA, le système fondé par Taher El Gamal n'a jamais été protégé par un brevet. Il est utilisé par le logiciel libre GNU *Privacy Guard*, par de récentes versions de PGP, et d'autre systèmes de chiffrement.

FACTORISATION ET COURBES ELLIPTIQUES[11]

En 1984, Hendrik Lenstra a diffusé en une page la description d'une nouvelle méthode qu'il avait développée pour factoriser les entiers en utilisant les courbes elliptiques[12]. L'algorithme astucieux et élégant était assez simple pour que je puisse le comprendre à partir d'une esquisse d'une page, même si une analyse détaillée de son temps d'exécution en a pris beaucoup plus. Ce fut la première fois que les courbes elliptiques étaient utilisées en cryptographie, et quand j'ai lu la page que Lenstra m'avait envoyée, j'ai senti qu'il avait d'un seul coup élevé les mathématiques de la cryptographie à un tout nouveau niveau de sophistication.

Peu de temps après, j'ai passé un semestre en Union Soviétique, où personne ne travaillait ouvertement sur la cryptographie. J'ai cependant continué à réfléchir sur ce sujet, et bientôt il m'est apparu qu'il devrait être possible d'utiliser les courbes elliptiques d'une manière tout à fait différente de ce que Lenstra avait fait, à savoir, pour construire des systèmes basés sur le problème difficile du calcul des logarithmes sur la courbe. Comme je ne connaissais personne en Union Soviétique avec qui je pouvais en parler, j'ai écrit une lettre à Andrew Odlyzko[13], puis aux *Bell Labs*, décrivant mon idée d'utiliser le groupe d'une courbe elliptique pour construire un cryptosystème. Odlyzko était alors un des rares mathématiciens à avoir produit un travail majeur à la fois dans les domaines théoriques et pratiques. Aujourd'hui, il n'est pas si inhabituel de concilier les mathématiques pures et appliquées, mais dans le milieu des années 1980, Odlyzko était le seul dans ce cas parmi les mathématiciens que je connaissais personnellement.

Les courriels n'existaient pas encore, et les lettres entre l'URSS et les États-Unis prenaient deux semaines dans chaque direction. Il a donc fallu attendre un mois pour recevoir une réponse d'Odlyzko. Il disait que mon idée de ce nouveau type de cryptographie était bonne, et en fait, dans le même temps, Victor Miller[14] d'IBM a proposé exactement la même chose. L'attrait de la cryptographie à courbe elliptique (ECC *Elliptic Curve Cryptosystem*) résidait dans ce que le problème du logarithme discret sur une courbe elliptique paraissait être (et semble l'être encore vingt-deux ans

---

[11] NdT. : les titres des paragraphes ne figurent pas dans l'article original.

[12] NdT. : voir le chapitre « L'influence de la cryptologie moderne sur les mathématiques et l'université » p. 273.

[13] NdT. : le mathématicien et informaticien Andrew Odlysko (né en 1949) fut responsable du *Digital Technology Center* de l'université du Minnesota. Il a abondamment publié en théorie analytique et en théorie algorithmique des nombres, ainsi qu'en théorie de la complexité et en cryptographie.

[14] NdT. : Victor S. Miller (né en 1947), co-inventeur de la cryptographie par les courbes elliptiques, travaille au Centre de Recherche en Communication de l'*Institute for Defense Analysis* à l'université de Princeton. Il est l'auteur de plusieurs algorithmes cryptographiques.

plus tard) un problème beaucoup plus difficile que celui de la factorisation des nombre entiers.

Dans un premier temps, ni Victor ni moi n'imaginions que l'ECC prendrait une importance commerciale, nous l'avions plutôt pensée comme une belle construction théorique. Rétrospectivement, le plus surprenant n'est pas que je ne pensais pas à commercialiser l'idée, mais que Victor Miller, qui travaillait chez IBM, ne pensait pas non plus en termes concrets. Il n'a même pas déposé de demande de brevet, même si à l'époque comme aujourd'hui à IBM, la politique était d'encourager vivement tous les employés à faire tout leur possible pour déposer des brevets, même sur le plus futile des sujets. Ainsi, la question de transformer l'ECC en un produit commercial aura attendu que d'autres personnes s'y intéressent.

LA LIBERTE DE TON DANS LES REUNIONS DE CRYPTOGRAPHIE

Après être revenu aux États-Unis, j'ai commencé à fréquenter les conférences de cryptographie. Les plus importantes étaient les réunions annuelles *Crypto* en août à Santa Barbara, en Californie. Dans les années 1980, j'ai trouvé l'atmosphère à *Crypto* rafraîchissante et stimulante. Les réunions étaient vraiment pluridisciplinaires, avec des participants venant de l'industrie, du gouvernement, et du milieu universitaire dans des domaines allant des mathématiques à l'informatique, et de l'ingénierie aux affaires.

Il y avait une sorte de « fruit défendu » dans la première décennie des conférences *Crypto*. Au début des années 1980, la *National Security Agency* (NSA) avait mené une tentative lourde (mais infructueuse) pour limiter la recherche ouverte en cryptographie. Ainsi, inaugurer les conférences *Crypto* en 1981 était en soi un acte de défiance.

La liberté de ton des réunions dans ces années reflète les personnalités hautes en couleur et excentriques de certains des premiers fondateurs et des chercheurs en cryptographie à clé publique. Tel a été Whit Diffie, un libertaire brillant, excentrique et imprévisible, qui avait co-écrit en 1976 (avec Martin Hellman) l'article le plus célèbre de l'histoire de la cryptographie[15]. Diffie avait l'habitude de donner des « sessions impromptues » *(rump sessions*), où les présentations informelles, irrévérencieuses, et souvent humoristiques étaient la norme. Il a été chahuté au point qu'on a dû imposer des restrictions sur ce qui pouvait être jeté à l'orateur (d'accord pour des canettes de bière vides, mais pas pleines).

L'influence des entreprises était alors beaucoup plus faible. Il s'est passé beaucoup de temps entre l'invention de la cryptographie à clé publique et

[15] NdT. : cet article est ici traduit au chapitre « Les nouvelles orientations de la cryptographie » p. 173.

son acceptation dans le monde commercial. Jusqu'à la fin des années 1980, les entreprises ne manifestaient généralement que peu d'intérêt pour la question de la sécurité des données. Presque aucun chercheur en cryptographie n'a jamais signé d'« accord de non divulgation » limitant ce qu'il pourrait dire publiquement – en fait, la plupart d'entre nous n'avions jamais entendu parler d'une telle chose.

C'est à *Crypto* que j'ai rencontré Scott Vanstone[16], un mathématicien de l'Université de Waterloo qui a dirigé un groupe pluridisciplinaire et amélioré les algorithmes pour l'arithmétique dans les corps finis. Avec cette expérience, il était bien outillé pour travailler sur l'ECC. Vanstone, avec deux autres professeurs de Waterloo, l'un en mathématiques et l'autre en ingénierie, ont formé une société, qui s'appelle maintenant la *Certicom Corporation*, pour développer et commercialiser l'ECC.

Les courbes elliptiques ne sont pas le seul type de courbes qui peut être utilisé pour la cryptographie. En 1989, j'ai proposé d'utiliser les groupes de jacobiennes des courbes hyperelliptiques. Ces dernières années, beaucoup de recherches, en particulier en Allemagne, ont été consacrées aux cryptosystèmes à courbes hyperelliptiques.

DES MATHEMATIQUES TOUJOURS PLUS SOPHISTIQUEES

Au début de septembre 1998, quelques jours avant de partir pour une année sabbatique à l'Université de Waterloo, j'ai reçu un e-mail de Joe Silverman[17], mathématicien à l'Université Brown, qui avait écrit un excellent manuel en deux volumes pour étudiants de troisième cycle sur les courbes elliptiques. Son message décrivait un nouvel algorithme, qui se proposait de résoudre le problème du logarithme discret elliptique, en un mot, de casser la cryptographie à courbe elliptique.

Silverman a appelé son algorithme « *xedni calculus* » comme « *index* » épelé à l'envers. Son idée générale était d'exécuter les étapes semblables à celles de l'algorithme de calcul du logarithme (*index calculus*), mais dans l'ordre inverse.

La raison pour laquelle Silverman pensait que son algorithme pouvait éventuellement être efficace reposait sur une relation profonde et difficile qu'on appelle la conjecture de Birch et Swinnerton-Dyer. Ironie du sort, dans un livre intitulé *Algebraic Aspects of Cryptography*, que j'avais publié quelques mois auparavant, j'avais inclus une discussion de cette conjecture

---

[16] NdT. : il est le co-auteur d'un important manuel de cryptologie, *Handbook of Applied Cryptography*.

[17] NdT. : Joseph H. Silverman (né en 1955), professeur de mathématiques à Brown University, a fondé la *NTRU Cryptosystems* en 1996 avec plusieurs collègues pour commercialiser leurs algorithmes cryptographiques.

dans une section que j'avais appelée « Bagage Culturel ». Mon ton était plein d'excuses envers mes lecteurs qui prenaient de leur temps pour lire des mathématiques qui, en dépit de leur grand intérêt pour les théoriciens, avaient peu de chances, disais-je, d'être jamais appliquées à la cryptographie. Puis, pendant une année, j'ai intensivement étudié l'attaque de Silverman sur l'ECC, qui reposait justement sur l'idée sous-jacente de cette conjecture. Cela montre qu'il est imprudent de prédire que certaines mathématiques ne seront jamais utilisées en cryptographie.

Scott Vanstone et ses collègues de Certicom étaient extrêmement inquiets de l'algorithme de Joe Silverman, parce qu'ils craignaient que les concurrents doutant de l'ECC, en particulier à la *RSA Company*, ne s'en emparent comme un argument contre l'utilisation des courbes elliptiques.

Les premiers mois de mon année sabbatique furent consacrés à une analyse approfondie de l'algorithme de Silverman. En octobre, j'ai trouvé un argument théorique, reposant sur le concept de « hauteur » de points, montrant que, pour des groupes de courbes elliptiques très grands, l'approche *xedni* serait extrêmement inefficace. Cependant, avec cette ligne générale de raisonnement, je ne pouvais pas être plus précis sur les tailles pour lesquelles l'algorithme ne serait pas applicable. Il était concevable, même si je le pensais peu probable, que l'algorithme ne soit pas totalement inapplicable pour les courbes dans la gamme de taille qui est utilisée en cryptographie.

Il est important de comprendre qu'une quelconque garantie de sécurité ne peut pas s'appuyer sur un résultat asymptotique, tel mon argument théorique établissant l'inefficacité de *xedni* comme limite lorsque la taille du groupe augmente. Il faut plutôt analyser l'algorithme pour les tailles de courbes elliptiques employées en cryptographie. L'argument asymptotique peut être utile comme un guide, et il nous a certainement fait espérer que nous serions en mesure de démontrer que *xedni* était impraticable pour les courbes réellement utilisées, mais il ne peut servir de substitut à une analyse concrète de sécurité. Il s'est avéré être beaucoup plus difficile et plus long de mener à bien cette analyse que cela ne l'avait été pour arriver au résultat asymptotique avec l'argument théorique.

Afin de répondre à la question cruciale de l'efficacité de *xedni* pour les courbes elliptiques utilisées en pratique, j'ai travaillé avec un groupe pluridisciplinaire de jeunes mathématiciens et informaticiens au Centre de Recherche Cryptographique Appliquée de Waterloo, en particulier avec Edlyn Teske, Andreas Stein, et Michael Jacobson. Nous étions en constante communication avec Joe Silverman, qui nous a donné des suggestions sur la meilleure façon de tester son algorithme. Finalement, vers la mi-décembre, nous avions fait assez de calculs et Silverman a convenu que son algorithme n'était pas applicable. En fait, c'est un euphémisme – il s'est avéré que son

algorithme est probablement le plus lent jamais imaginé pour trouver le logarithme discret sur une courbes elliptique.

C'était néanmoins une idée élégante, et notre étude sur *xedni* fut un projet stimulant. La tentative d'attaque de Silverman sur la cryptographie à courbe elliptique illustre l'utilisation croissante de l'arithmétique et de la géométrie algébrique en cryptographie à clé publique.

Dans les années 1990, un autre exemple de la plus grande sophistication de la cryptographie mathématique a été la proposition de Gerhard Frey[18] d'utiliser la descente de Weil[19] pour trouver les logarithmes discrets sur les courbes elliptiques. Des algorithmes sous-exponentiels pour les logarithmes discrets sur courbes hyperelliptiques de genre élevé avaient déjà été mis au point sur une idée d'Adleman et Huang, et l'idée de Frey était de transférer le problème du logarithme discret sur une courbe elliptique vers une courbe hyperelliptique de genre élevé. La proposition de Frey a été étudiée par Galbraith, Gaudry, Hess, Menezes, Smart, Teske, et d'autres, et il a été démontré que cela conduisait à un algorithme plus rapide dans un petit nombre de cas.

Des progrès ont été également accomplis dans la recherche de méthodes très rapides pour compter le nombre de points sur une courbe elliptique générée aléatoirement. La première étape dans ce sens a été accomplie par Schoof dans un document de 1985, utilisant les polynômes de division. Par la suite, de meilleurs algorithmes ont été mis au point en utilisant les formes modulaires et des techniques *p*-adiques.

Le rapport annuel des séries de conférences ECC, qui est maintenant dans sa onzième année (voir http://www.cacr.math.uwaterloo.ca), indique bien la quantité de recherche consacrée aux applications cryptographiques des courbes elliptiques ces dernières années.

Un tout nouveau type de cryptographie à courbe elliptique a été développé aux environs de l'année 2000, à la suite des idées d'Antoine Joux, Dan Boneh, et Matt Franklin. Il s'est avéré que les appariements de Weil et Tate sur les courbes elliptiques pourraient être utilisés pour réaliser des fonctionnalités cryptographiques qui n'étaient pas possibles auparavant (ou avaient été réalisées inefficacement), notamment, le chiffrement avec l'identité (où la clé publique est, disons, l'adresse e-mail) et des signatures numériques ultra-courtes. La cryptographie avec appariement a été un domaine actif de la recherche. En juillet 2007, la première d'une série de

[18] NdT. : Gerhard Frey (né en 1944) est un mathématicien allemand spécialiste de la théorie des nombres, qui a enseigné dans plusieurs universités des États-Unis. Ses recherches sur les courbes elliptiques ont alimenté la preuve de Wiles du grand théorème de Fermat.

[19] André Weil (1906-98) fut un des membres fondateurs du groupe Bourbaki, et initiateur de la cohomologie galoisienne. Ses importants travaux concernent essentiellement la géométrie algébrique et la théorie des nombres.

conférences entièrement consacrées à ce type de cryptographie à courbe elliptique a eu lieu au Japon[20].

LA DIVISION DE LA COMMUNAUTE MATHEMATIQUE

En dépit de ces merveilleux exemples d'applications de mathématiques intéressantes en cryptographie, il y a eu aussi un inconvénient, en fait, deux inconvénients. Ce sera l'objet de la suite de cet article.

Tout d'abord, il y a eu un effet d'entraînement. Un jour, dans les années 1990, le *Canadian Natural Sciences and Engineering Research Council* m'envoya une longue proposition à évaluer, émanant d'un groupe dirigé par un mathématicien de premier plan, affirmant que la recherche proposée serait importante en cryptographie. Après avoir lu la description du projet, il fut clair pour moi que (1) la proposition était solide d'un point de vue mathématique, et (2) ils ne connaissaient rien en cryptographie. Il est triste que sous la pression, certains mathématiciens éprouvent le besoin de présenter leurs recherches comme ayant un lien avec la cryptographie.

À la fin des années 1980, la NSA s'est rendu compte qu'elle avait commis une erreur en divisant la communauté mathématique plusieurs années auparavant, et elle voulait rétablir les relations. La meilleure façon de se réconcilier avec le milieu universitaire était de donner de l'argent. Ils ont donc mis en place un système de subventions qui est devenu une source majeure de financement dans certains domaines comme la théorie des nombres.

La plupart du temps, il est bénéfique que davantage d'argent arrive pour les mathématiques – quels que soient les motifs du donateur. Cependant, cela peut aussi engendrer de subtils effets négatifs. Il y a plusieurs années, William Thurston (NdT. : 1946-2012) et d'autres nous ont avertis des dangers d'une trop grande dépendance vis-à-vis du financement militaire. Et l'année dernière dans les *Notices,* David Eisenbud a écrit[21] ce que j'ai considéré comme une réfutation éloquente de l'argument (sur la base des avantages supposés de la collecte de fonds) en faveur d'un programme de bourses de l'AMS (*American Mathematical Society*).

Au début des années 1990, j'ai reçu une proposition de la NSA pour le financement d'une conférence sur les modules de Drinfeld. La conférence semblait être une bonne idée, et j'en ai fait un rapport positif dans son ensemble. Cependant, le ton d'une partie de la proposition m'ennuyait. Dans un paragraphe sur « l'effet de la conférence sur la compétitivité des

[20] NdT. : il s'agit de la conférence *Pairing* : http://www.pairing-conference.org/2007/.
[21] NdT. : Eisenbud, D., « Science or Politics at the AMS ? – A Divisive Proposal », august 2006, vol. 53, n° 7, pp. 757-758.

mathématiques américaines », les auteurs tentaient de diviser le terrain entre mathématiques américaines et non-américaines, et promouvaient la conférence au motif qu'elle augmenterait la position concurrentielle des premières. J'ai commenté :

> « Les mathématiques sont sans doute la plus internationale des disciplines intellectuelles. Interaction et travail en commun traversent facilement les frontières nationales. Ainsi, il est généralement impossible de déterminer – et il ne sert à rien de chercher à le faire – la proportion de crédit à attribuer à chaque pays. Un tel ton chauvin n'est pas en harmonie avec l'esprit coopératif et international de la profession mathématique... Qu'ils aient écrit cet article à partir d'une inquiétude sincèrement ressentie sur la « compétitivité des mathématiques américaines » ou que ce soit en réponse à ce qu'ils pensaient être l'état d'esprit à la NSA, j'espère vraiment que dans l'avenir, ils supprimeront de telles absurdités dans les appels à projets ».

Apparemment, la disponibilité de l'argent de la NSA avait eu un effet corrupteur sur certains mathématiciens, qui ont commencé à penser en termes nationalistes et chauvins, jusqu'à rédiger leur proposition d'une façon qui selon eux plairait à la NSA.

LES MATHEMATICIENS PRENNENT EN MARCHE LE TRAIN DE LA CRYPTOGRAPHIE

En même temps que les mathématiciens essayaient de prendre en marche le train de la crypto, les cryptographes ont découvert la puissance que l'aura de la certitude mathématique peut avoir dans les situations de compétition. Ils ont commencé à démontrer des théorèmes mathématiques censés garantir la sécurité de leur système, l'idée étant de convaincre les autres que leur système était sûr à 100 %. Il s'agit du deuxième « côté obscur » qui s'est développé dans la relation entre mathématiques et cryptographie, chaque groupe cherchant des moyens pour exploiter le statut de l'autre groupe afin de faire progresser son propre intérêt. Avant d'expliquer cette utilisation (ou mauvaise utilisation) des mathématiques plus en détail, je voudrais commenter un choc des cultures entre mathématiques et recherche cryptographique.

En 1996, j'ai été président du comité de programme de la conférence *Crypto*. Pour une personne de formation mathématique, ce fut une expérience troublante. Environ les deux tiers des soumissions sont arrivés par la poste dans les 48 heures avant l'échéance finale. Un bon nombre d’entre elles avait de toute évidence été élaboré dans la précipitation, pleines d'erreurs typographiques. Un auteur m'avait envoyé uniquement les pages

impaires. Quelques-uns avaient violé l'obligation d'anonymat (il y avait une politique de rapporter en double-aveugle). Plusieurs n'avaient pas tenu compte des lignes directrices qui avaient été mises à leur disposition. Et dans de nombreux cas, les documents étaient peu originaux, ils n'étaient que de légères améliorations de publications des mêmes auteurs l'année précédente ou une modification mineure du travail d'un autre.

À certains égards, la situation a encore empiré avec les soumissions électroniques. Alfred Menezes, le président de programme de *Crypto* 2007, m'a dit que sur 197 soumissions, 103 sont arrivées dans les onze heures précédant la date limite et 35 sont arrivées dans la dernière heure.

La publication de travaux mathématiques fonctionne différemment. Tout d'abord, la plupart des articles sont publiés dans des revues, pas dans des actes de conférences – et les revues n'ont pas d'échéance. En second lieu, les mathématiciens ont tendance à avoir une piètre opinion des auteurs qui se précipitent pour publier un grand nombre de petits articles – le terme péjoratif est LPU (*Least Publishable Unit*, plus petite unité publiable), plutôt que d'attendre d'être prêts à publier un traitement exhaustif du sujet dans un seul article.

Les départements de mathématiques pensent en général que :

CONJECTURE. *Pour le développement des mathématiques, il est préférable pour une personne de publier un excellent article en* n *années plutôt que* n *documents sans valeur en un an.*

Dans certains autres domaines scientifiques – y compris malheureusement la science informatique et la cryptographie – la conjecture similaire, bien que probablement tout aussi vraie, n'est généralement pas admise.

La cryptographie a été fortement influencée par la culture disciplinaire de la science informatique, qui est tout à fait différente de celle des mathématiques. Certaines explications de la divergence entre les deux domaines pourraient être une question d'échelle de temps. Les mathématiciens, qui héritent d'une riche tradition millénaire, perçoivent le temps qui passe à la manière d'un éléphant. Dans cette façon de voir, il y a peu de conséquences si leur grand article paraît cette année ou la suivante. La science informatique et la cryptographie, au contraire, sont influencées par le monde des entreprises de haute technologie, avec leur course frénétique pour être la première à apporter de nouveaux gadgets sur le marché. Les cryptographes voient ainsi le temps passer à la manière d'un colibri. Les meilleurs chercheurs s'attendent à ce que pratiquement toutes les conférences incluent un ou plusieurs documents vite faits par eux ou par leurs élèves.

Ces dernières années, Alfred Menezes et moi avons écrit une série de documents qui critiquent le domaine de la cryptographie connu sous le nom

de sécurité prouvable. (voir http://eprint.iacr.org/2004/152.pdf, http://eprint.iacr.org/2006/229.pdf, et http://eprint.iacr.org/2006/230.pdf). Bien que les documents aient été largement téléchargés et la plupart des réactions favorables, notre travail dans ce domaine n'a pas été bien accueilli par tout le monde. Beaucoup de spécialistes en cryptographie théorique ont mal perçu notre intrusion dans leur domaine.

Dans les années 1980, il semblait que tous les cryptographes étaient heureux de voir affluer les mathématiciens. Vingt ans plus tard, cependant, j'ai l'impression que certains d'entre eux préféreraient simplement nous voir partir.

L'idée de « sécurité prouvable » est de donner la preuve mathématiquement rigoureuse d'une garantie conditionnelle de la sécurité d'un protocole de chiffrement. Elle est *conditionnelle* en ce qu'elle est généralement de la forme « notre protocole n'est à l'abri d'une attaque de type X qu'à la condition que le problème mathématique Y soit calculatoirement difficile »[22].

Ici, le mot « protocole » désigne une suite particulière d'étapes qui se trouvent réalisé dans une application particulière de la cryptographie. Depuis les débuts de la cryptographie à clé publique, il est traditionnel d'appeler deux utilisateurs *A* et *B* du système par les noms d'« Alice » et de « Bob ». Donc, une description d'un protocole peut être : « Alice envoie à Bob ..., puis Bob répond avec ..., puis Alice répond avec ... », et ainsi de suite.

La forme que prennent les preuves de sécurité est vue comme une *réduction*. La réduction d'un problème à un autre survient implicitement tout au long des mathématiques ; en informatique, les réductions sont le principal outil utilisé pour comparer et classer les problèmes selon leur difficulté.

Dans les articles sur la sécurité prouvable, les auteurs tentent de prouver que le problème mathématique qui est généralement considéré comme difficile, tel que la factorisation des entiers ou la recherche du logarithme discret sur une courbe elliptique, est *réductible* à la réussite d'une certaine attaque contre leur protocole cryptographique. Cela signifie que toute personne qui pourrait briser leur cryptosystème peut aussi, avec seulement un peu plus d'effort, résoudre le problème mathématique supposé difficile. Comme par hypothèse, cela n'est pas possible, il est donc prouvé que le protocole est sûr.

Pour les mathématiciens qui étudient la littérature sur la sécurité prouvable, comme Menezes et moi l'avons fait, il y a plusieurs raisons d'être inquiets. De toute évidence, un théorème de sécurité prouvable s'applique uniquement aux attaques d'un genre spécifié et ne dit rien sur les attaques astucieuses qui pourraient ne pas être incluses dans le théorème. En outre, le

[22] Voir le chapitre « Les nouvelles orientations de la cryptographie » p. 192.

résultat est fortement conditionnel. Contrairement aux mathématiques, où une condition sur un théorème signifie habituellement quelque chose comme « en supposant que l'hypothèse de Riemann est vraie » (ce qui est presque certain), en cryptographie la condition est du type « en supposant que personne ne trouve d'amélioration pour un algorithme résolvant un certain problème de maths » ce qui est une totale énigme. L'histoire n'a pas été concluante pour ce dernier type d'hypothèse. Par exemple, à la fin des années 1980 et au début des années 1990, le développement de l'algorithme de factorisation du crible du corps de nombres pour un module RSA a entraîné une diminution drastique du temps d'exécution des algorithmes de calcul de logarithme et de factorisation de $\exp(\log(n)^{1/2+\varepsilon})$ à $\exp(\log(n)^{1/3+\varepsilon})$.

SECURITE PROUVABLE ?

Les résultats de sécurité prouvable sont souvent utilisés pour impressionner ceux qui sont étrangers au domaine et qui comprennent peu leur véritable signification. Supposons que certaines personnes utilisent la cryptographie à clé publique pour protéger des numéros de carte de crédit pour l'e-commerce, afin de préserver la confidentialité des dossiers médicaux, ou de créer des signatures numériques. Comment peuvent-elles être certaines que le système est sécurisé ? Pour les non-spécialistes, « sécurité prouvable » signifie qu'il y a une garantie à toute épreuve comme peut l'être une preuve du théorème de Pythagore. À notre avis, ceci est très trompeur.

Il y a aussi une difficulté qui vient de la culture disciplinaire de la cryptographie que j'ai commentée plus haut. Habituellement, des articles sont écrits sous la pression de l'échéance, davantage à la manière d'un journaliste que d'un mathématicien. Et ils ont rarement lu les articles d'autres auteurs avec soin. En conséquence, même les meilleurs chercheurs publient parfois des documents contenant des erreurs graves qui vont passer inaperçues pendant des années.

En 1994, deux des plus grands spécialistes dans ce nouveau domaine qu'est la sécurité prouvable, Mihir Bellare et Phillip Rogaway, ont proposé une méthode de chiffrement basée sur RSA qu'ils ont appelé OAEP[23] (le O est pour « optimal », un mot bien galvaudé dans le monde hyper branché de la *high-tech*). Ils ont estimé que les preuves de sécurité devaient être suffisamment détaillées pour obtenir des garanties concrètes pour des tailles

[23] NdT. : Bellare M., Rogaway P., *Optimal Asymmetric Encryption – How to encrypt with RSA*. Extended abstract in A. De Santis (ed.), *Advances in Cryptology - Eurocrypt '94 Proceedings*, Lecture Notes in Computer Science, vol. 950, New-York, Springer Verlag, 1995.

de clés et un choix de paramètres spécifiés. En partie grâce à la preuve de sécurité qui accompagnait OAEP, il a été adopté pour servir dans une nouvelle norme de cartes *Visa* et *MasterCard*. Il s'est avéré, cependant, que la preuve était fausse, comme Victor Shoup l'a découvert sept ans plus tard[24]. Ce fut un peu un scandale qui a conduit beaucoup de gens à s'interroger sur la qualité du contrôle des documents de sécurité prouvable.

Si un lecteur attentif et perspicace se livre à un examen sérieux – et Alfred Menezes est un tel lecteur –, alors les erreurs dans les preuves sont découvertes beaucoup plus rapidement. Une affaire qui à bien des égards est encore plus frappante que celle de OAEP est la panique récente autour d'un ensemble d'« améliorations » de protocoles d'échange de clés conçus par Hugo Krawczyk. En février 2005, Krawczyk, un chercheur de premier ordre en matière de sécurité prouvable qui travaille pour IBM, a présenté un document à *Crypto* 2005, dans lequel il prétendait avoir trouvé des failles dans le système d'échange de clés Menezes-Qu-Vanstone (MQV). Il l'a remplacé par une version modifiée (HMQV) qui selon lui, était à la fois plus efficace et prouvée sûre. Si ses revendications avaient été valides, cela aurait été une source d'embarras majeur, non seulement pour Menezes et ses co-auteurs, mais aussi pour la NSA, qui avait accordé une licence à MQV de *Certicom*, et que ses experts avaient étudié attentivement.

Krawczyk n'avait pas envoyé son papier à Menezes ni aux autres concepteurs de MQV avant de le soumettre, ce qui aurait été considéré comme une courtoisie standard dans le monde scientifique. Mais ce qui me semble plus scandaleux, c'est que personne non plus, au sein du comité de programme de *Crypto* 2005, ne l'avait fait. Ils se sont apparemment précipités pour accepter le papier après une simple lecture superficielle. Lorsqu'enfin Menezes a obtenu une copie du document – après qu'il ait été accepté par le comité de programme – il a tout de suite vu que les défauts que Krawczyk a listés dans MQV reposaient sur des malentendus ou étaient des points théoriques mineurs sans signification pratique.

Plus important encore, Menezes a constaté que le principal argument de l'article était fallacieux. Krawczyk a affirmé que dans son système d'échange de clé modifié, il pourrait augmenter l'efficacité en éliminant une certaine vérification de sécurité (appelée « validation de clé publique ») mise dans MQV pour empêcher des attaques connues. C'est sa « preuve » de sécurité qui lui a donné la confiance nécessaire pour le faire. Mais Menezes a rapidement constaté que certains des protocoles HMQV succombent aux mêmes attaques que MQV si ces contrôles de sécurité n'avaient pas été mis en place. Ensuite, voyant que quelques-unes des conclusions des théorèmes de Krawczyk étaient fausses, Menezes a commencé la lecture soigneuse de

[24] NdT. : Shoup, V., « OAEP reconsidered », 2001, *in Crypto '01 Proceedings of the 21rst Annual International Cryptology Conference on Adavances in Cryptology*, pp. 239-259.

la « preuve » jusqu'à ce qu'il tombe sur une lacune manifeste dans l'argumentation.

Krawczyk et les rapporteurs du comité de programme avaient été tellement hypnotisés par la « preuve » qu'ils n'ont pas réussi à utiliser le sens commun. Toute personne travaillant en cryptographie devrait réfléchir avec soin avant d'abandonner une étape de validation mise en place pour prévenir des problèmes de sécurité. Certes, quelqu'un ayant l'expérience et l'expertise de Krawczyk n'aurait jamais fait une telle bourde s'il n'avait pas été trop confiant en raison de sa « preuve » de sécurité. Comme beaucoup d'autres idées à la mode – des abris souterrains des années 1950 au bouclier anti-missile des années 1980 – les « preuves » de sécurité d'un protocole cryptographique donnent souvent une fausse confiance qui aveugle quant aux dangers véritables.

Dans notre premier article sur la sécurité prouvable, Menezes et moi nous sommes opposés à cette terminologie :

> « Il y a deux connotations malheureuses du mot « preuve » qui viennent des mathématiques et qui rendent le mot inapproprié dans les discussions sur la sécurité des systèmes cryptographiques. La première est la notion de certitude à 100 %. La plupart des gens qui ne travaillent pas dans une spécialité donnée voient un « théorème » qui est « prouvé » comme quelque chose qu'ils devraient accepter sans broncher. La seconde connotation est une suite compliquée et hautement technique d'étapes. D'un point de vue psychologique et sociologique, une « preuve d'un théorème » est une notion intimidante : c'est quelque chose que personne en dehors d'une élite étroite de spécialistes n'est susceptible de comprendre dans le détail ni de mettre en doute. Autrement dit, une « preuve » est quelque chose qu'un non-spécialiste ne s'attend pas vraiment à lire ni à examiner.
>
> Le mot « argument », que nous préférons ici, a des connotations très différentes. Un « argument » est quelque chose qui devrait être largement accessible. Et même un argument raisonnablement convaincant n'est pas supposé être à 100 % définitif. Contrairement à la « démonstration d'un théorème », un « argument à l'appui d'un énoncé » suggère quelque chose que toute personne bien éduquée peut essayer de comprendre, voire d'interroger ».

Menezes et moi avons également étudié certains des problèmes subtils d'interprétation des résultats de la sécurité prouvable. Même lorsque les preuves sont correctes, elles masquent souvent un grand saut d'« ajustement ». Cela signifie que dans l'argument de réduction, l'attaque sur le protocole doit être répétée des millions de fois pour résoudre le problème calculatoirement difficile. Dans ce cas, la garantie pratique que l'on obtient est très faible. Menezes a trouvé quelques exemples extrêmes de ce problème de « non ajustement » dans quelques cas bien connus d'articles sur des générateurs de nombres aléatoires. Dans un article, il s'est avéré que,

si vous suivez attentivement l'argument de l'auteur avec la valeur recommandée du paramètre, tout ce qu'il a vraiment prouvé, c'est qu'un attaquant aurait besoin d'au moins 10^{-40} nanosecondes pour casser le système. C'est beaucoup moins de temps que ce que met la lumière pour parcourir un micron.

Ce qui s'est passé, c'est que les valeurs des paramètres avaient été recommandées sur la base d'un théorème asymptotique. Ce théorème dit que, quand N tend vers l'infini, vous pouvez en toute sécurité générer $O(\log \log N)$ symboles binaires pseudo-aléatoires à chaque fois que vous effectuez une élévation au carré modulo le nombre N composite (ici, « en toute sécurité » signifie, *grosso modo*, que personne ne peut distinguer entre la séquence produite et une séquence vraiment aléatoire par un algorithme qui fonctionne dans un temps raisonnable). Cependant, comme je l'ai mentionné lors de la discussion du calcul *xedni* de Joe Silverman, il est fallacieux d'utiliser un résultat asymptotique comme une garantie pratique de sécurité. On a plutôt besoin d'effectuer une analyse détaillée pour une gamme réaliste de paramètres. Il est souvent beaucoup plus difficile (comme pour *xedni*) de mener à bien cette analyse concrète que de prouver le théorème asymptotique, et parfois les conclusions ne sont pas ce que l'on pourrait espérer. Dans le cas du générateur pseudo-aléatoire de symboles binaires, l'analyse (si l'on suppose que $\log_2 (\log_2 N)$ symboles binaires sont pris à chaque itération, comme recommandé) conduit à une minoration absurde de la quantité de temps dont un adversaire aurait besoin pour attaquer avec succès le générateur.

L'HYPOTHESE DE L'ORACLE ALEATOIRE

L'histoire de notre premier article sur la « sécurité prouvable » a une suite amusante. Juste avant de devoir paraître dans *Journal of Cryptology* et presque deux ans après avoir été accepté pour publication, un membre du comité de rédaction s'est fermement opposé à son acceptation par le journal. Bien qu'il ait été trop tard pour bloquer la publication, le rédacteur en chef avait été suffisamment inquiété pour écrire une préface dans l'édition de janvier 2007 où il justifiait sa décision de publier.

Le membre du conseil éditorial qui s'opposait à notre article était Oded Goldreich de l'Institut Weizmann, qui est l'un des chefs de file israélien en science informatique et un grand nom (certains diraient LE grand nom) de la cryptographie théorique. Lorsqu'il fut incapable d'empêcher la publication de notre article dans le *Journal of Cryptology*, il a posté sur le serveur de prépublications en cryptographie ePrint, un essai de 12 pages intitulé « La Cryptographie Postmoderne » qui s'en prenait à nous sur des positions

philosophiques (voir http://eprint.iacr.org/2006/461)[25]. Il a accusé Menezes et moi d'être « post-modernes » et « réactionnaires », car nos critiques de la sécurité prouvable « faisaient le jeu des adversaires du progrès ».

La partie de notre article qui semble avoir le plus irrité Goldreich, est notre explication de la raison pour laquelle nous n'avons pas été convaincus par certains arguments que lui et d'autres ont avancé dans le but de se débarrasser de la prétendue hypothèse de « l'oracle aléatoire ». L'hypothèse de l'oracle aléatoire concerne ce qu'on appelle les « fonctions de hachage » (de courtes chaînes de symboles qui agissent comme une sorte d'« empreinte digitale » d'un message). Cette hypothèse dit essentiellement que l'empreinte digitale donnée par une fonction de hachage, bien que construite, est en pratique impossible à distinguer d'un échantillon d'une chaîne aléatoire de symboles. Il s'agit d'une hypothèse intuitivement raisonnable, et dans notre document, nous avons fait valoir que toutes les tentatives visant à s'en débarrasser – même celles que les auteurs affirmaient être d'intérêt pratique – utilisaient en fait des constructions qui ne respectent pas les principes cryptographiques de base et donc n'ont aucun rapport avec la cryptographie du monde réel. Nous avons conclu notre discussion en disant que « notre confiance dans l'hypothèse de l'oracle aléatoire reste inébranlable ».

Goldreich a répondu à cela en ramenant sur nous la colère de l'Ancien Testament. Nous accusant de faire de l'oracle aléatoire un « fétiche », il a raconté une histoire de la Bible que notre article lui rappelait (dans ce qui suit, j'ai conservé la mise en forme, la casse, et l'orthographe de l'original) :

> « En effet, ce qui s'est passé avec le modèle de l'oracle aléatoire nous rappelle le récit biblique du Serpent d'airain, reproduit ci-après. (voir Nombres (21:4-8) et 2 Rois (18:4).). Pendant le voyage du peuple d'Israël dans le désert, le Seigneur a ordonné au prophète et dirigeant Moïse de réaliser un « serpent ardent » comme un moyen symbolique pour guérir les gens qui avaient été mordus par des serpents (qui avaient auparavant été envoyés par le Seigneur comme une punition pour un péché antérieur). Plusieurs centaines d'années plus tard, le serpent de bronze fabriqué par Moïse est devenu une idole objet d'un culte. Cela a conduit le roi juste Ezéchias (fils d'Achaz) à émettre l'ordre de réduire ce serpent de bronze en pièces. Laissez-nous affirmer que l'ordre du roi était *de détruire un objet qui a été construit sur l'instruction directe du Seigneur*, parce que cet objet est devenu un fétiche. En outre, cet objet ne sert plus le but pour lequel il a été construit. Cette histoire illustre le processus par lequel une bonne chose peut devenir un fétiche, et ce qu'il faut faire dans un tel cas.... Compte tenu du tournant que prend cette affaire, il nous semble bon d'abolir le modèle de l'oracle aléatoire ».

[25] NdT. : voir aussi Godereich, O., « On Post-Modern Crytpography », *Journal of Cryptology*, http://www.wisdom.weizmann.ac.il/.

Goldreich se voit comme le roi juste Ezéchias du vingt-et-unième siècle, défendant les chercheurs en sécurité prouvable contre les infidèles et post-modernes fétichistes comme Menezes et moi. Il est clair dans son essai qu'il n'avait pas lu notre article attentivement avant d'écrire sa réponse. Il ne semble pas non plus avoir été au courant de nos deux autres articles critiquant la sécurité prouvable. Mais bien sûr, il n'était pas nécessaire de lire vraiment les détails techniques de nos trois articles[26] pour nous dénoncer sur des bases religieuses et philosophiques.

Les réactions de colère de quelques chercheurs qui semblent percevoir notre travail comme une menace contre leurs intérêts ne sont pas le genre de choses qui se rencontre normalement en mathématiques théoriques[27], où habituellement les seules questions qui peuvent conduire quelqu'un à objecter un document sont une erreur ou une omission de la reconnaissance d'un travail antérieur (qui n'a été trouvée dans aucun de nos trois articles sur la sécurité prouvable). Mais loin d'être dérangé par les accusations formulées par Goldreich et d'autres, je me trouve encouragé par celles-ci, car elles montrent au moins que les gens y prêtent attention.

CONCLUSION

La cryptographie a ceci d'excitant d'être bien plus qu'un simple champ académique. Une fois, j'ai entendu un orateur de la NSA déplorer que les chercheurs universitaires puissent proposer de manière cavalière des cryptosystèmes non testés. Il a souligné que, dans le monde réel, si votre cryptographie échoue, vous perdez un million de dollars ou votre agent se fait tuer. Dans le milieu universitaire, si vous écrivez sur un cryptosystème, et que vous trouvez un moyen de le casser quelques mois plus tard, cela vous fait deux publications à ajouter à votre CV !

Drames et conflits sont inhérents à la cryptographie qui, en fait, peut être définie comme la science de la transmission et de la gestion des informations en présence d'un adversaire. La mentalité « espion contre espion », faite de compétition et de rivalité permanente s'étend à la culture

[26] NdT. :
– Koblitz N., Menezes A., J., « Another Look at 'Provable Security' », 2007, *Journal of Cryptology*, vol. 20, Issue 1, pp. 3-37,
– Koblitz N., Menezes A., J., « Another Look at 'Provable Security'. II », 2006, *Progress in Cryptology – INSOCRYPT 2006, Lecture Notes in Computer Science*, vol. 4329, pp. 148-175.
– Koblitz N., Menezes A., J., « Another Look at generic groups », *Advances in Mathematics of Communications (AMC)*, 2007, vol. 1, issue 1, pp. 13-28.

[27] NdT. : des débats métaphysiques ont pourtant eu lieu dans l'histoire des mathématiques, par exemple au sujet de la légitimité des nombres négatifs et des nombres imaginaires au 16e siècle, ou encore sur le caractère naturel des nombres entiers que Leopold Kroneker (1823-91) attribuait à Dieu, les autres ensembles numériques étant élaborés par l'homme.

du champ disciplinaire. Cela peut devenir excessif, et même enfantin à certains moments, mais cela explique aussi en partie pourquoi il peut être si amusant de faire de la recherche en cryptographie.

TABLE DES MATIERES