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

Marie-José Durand-Richard, Philippe Guillot

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 20e 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

[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.

dégager les procédures qui aujourd'hui s'expriment mathématiquement, la 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].

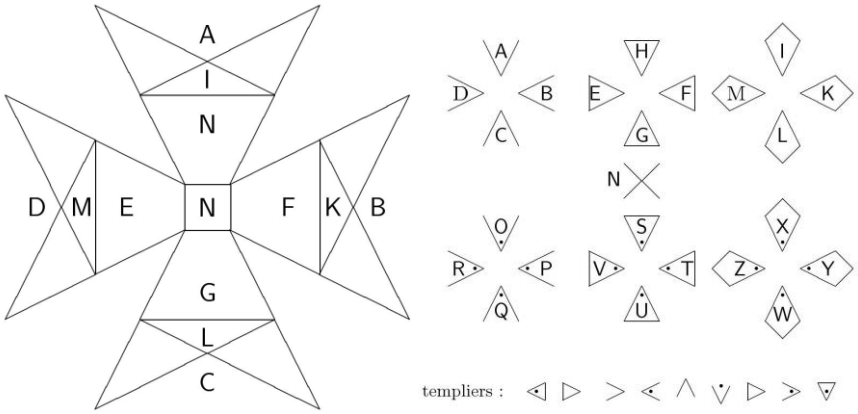

Fig. 2. Le code des Templiers (13e siècle). Illustration P. Guillot.

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.

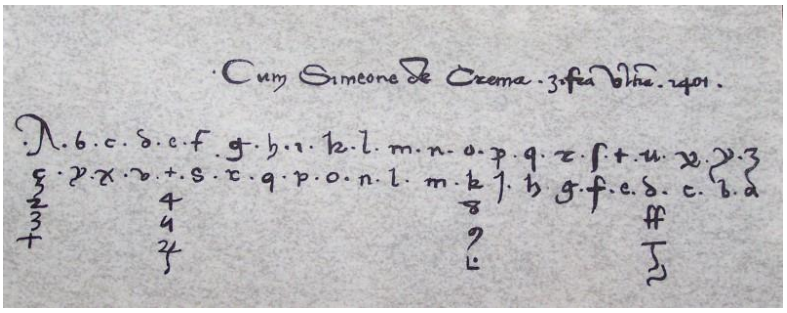

Fig. 3. Chiffrement homophone de Simeone de Crema. Kahn, p. 107.

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.

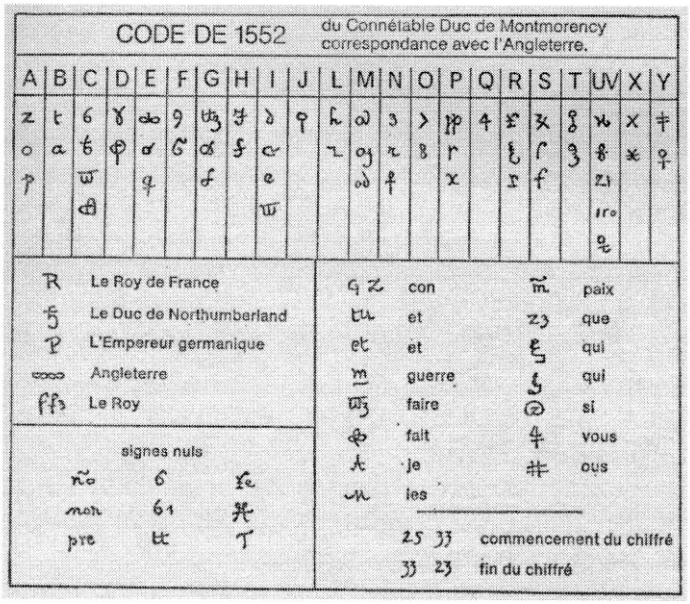

Fig. 4. Code du duc de Montmorency de 1552, Lerville, *in* Hébrard p. 61.

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].

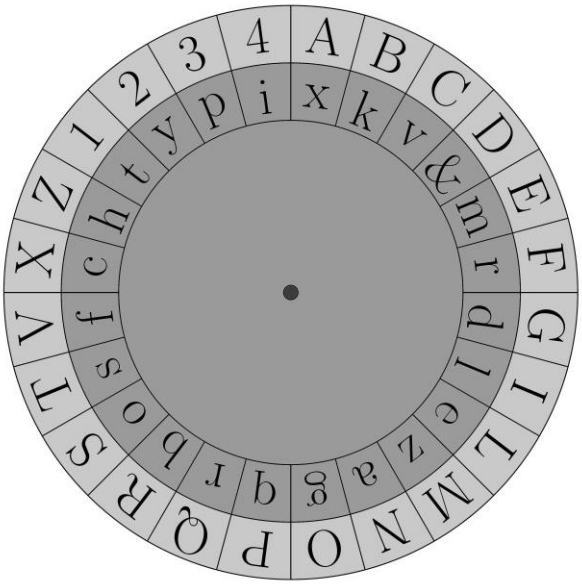

Fig. 5. Le disque d'Alberti. Illustration P. Guillot.
Exemple de cryptogramme : BqxboGqvgiMteRkomcoyvXilya

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 23, 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].

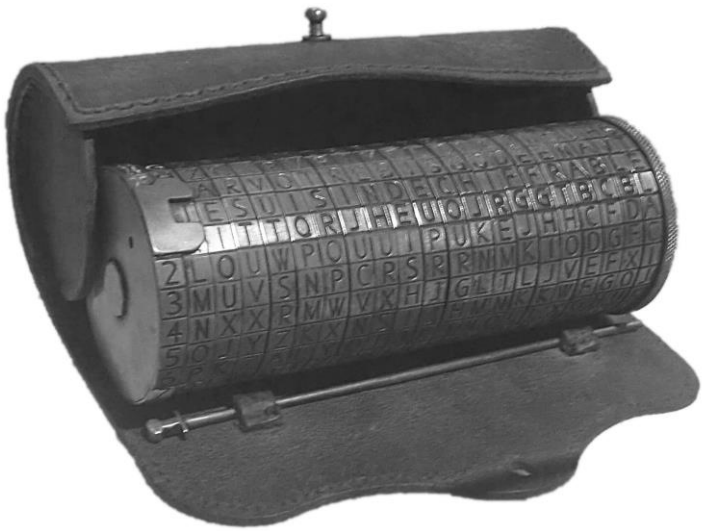

Fig. 6. Le cylindre de Bazeries. Exemplaire exposé au Musée des Télécommunications de Rennes. Photographie P. Guillot

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**Erreur ! Source du renvoi introuvable.**.

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.

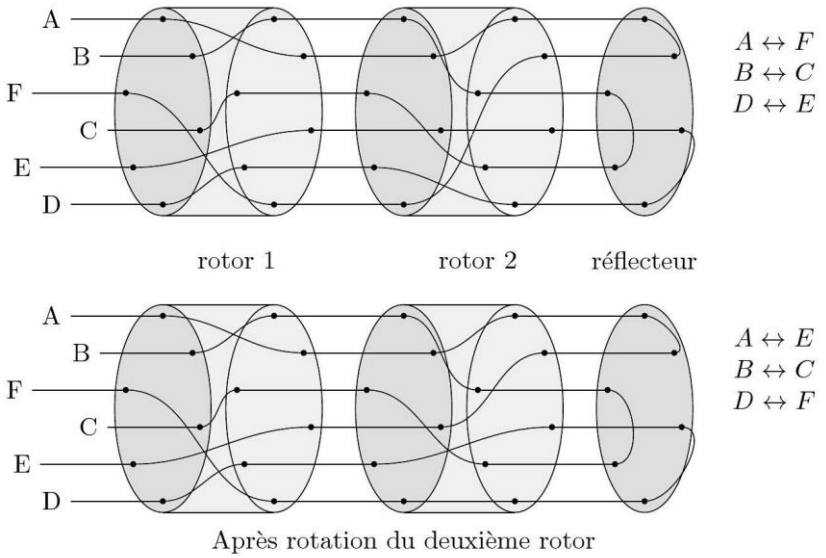

Fig. 8. Mode de fonctionnement d'une machine à 2 rotors. Illustration P. Guillot.

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.