Bibnum
Textes fondateurs de la science
Calcul et informatique

Auguste Kerckhoffs et la cryptographie militaire

Philippe Guillot

Édition électronique
URL : http://journals.openedition.org/bibnum/555
ISSN : 2554-4470

Éditeur
FMSH - Fondation Maison des sciences de l'homme

Référence électronique
Philippe Guillot, « Auguste Kerckhoffs et la cryptographie militaire », *Bibnum* [En ligne], Calcul et informatique, mis en ligne le 01 mai 2013, consulté le 19 avril 2019. URL : http://journals.openedition.org/bibnum/555

Auguste Kerckhoffs et la cryptographie militaire

Philippe Guillot
Maître de conférences en informatique
Université Paris-VIII

Figure 1 : Auguste Kerckhoffs (1835-1903) (WikiCommons, in *Eugen Drezen,* Historio de la Mondo Lingvo*, Leipzig, 1931, p. 102).*

L'article « La cryptographie militaire » est paru en deux parties dans le *Journal des Sciences militaires* en janvier et février 1883. Cet article, dont seule la première partie est analysée ici, concentre en une soixantaine de pages d'une concision remarquable, un inventaire très complet et très documenté des méthodes et des instruments de chiffrement connus à l'époque. Pas moins de vingt-six articles ou ouvrages de cryptologie sont cités. Mais sont surtout examinées les conséquences organisationnelles, pour les services militaires du Chiffre, de l'extension du télégraphe.

L'article s'impose rapidement comme une référence, contribuant fortement au renouveau des études cryptographiques en France. Entre 1883 et 1914, vingt-quatre ouvrages ou brochures sur la cryptologie y seront publiées, contre seulement six en Allemagne, ce qui conférera à la France une position dominante en Europe et un avantage notable pendant le conflit mondial de 1914-1918.

HEC & Arago

Kerckhoffs signe son article comme « professeur à l'École des hautes études commerciales et à l'École Arago ».
L'École des hautes études commerciales (aujourd'hui HEC) avait été fondée en 1881, sous l'impulsion du président de la Chambre de commerce de Paris, le négociant Gustave Roy (1821-1906). Installée boulevard Malesherbes à Paris, « elle forme aux affaires de banque, au commerce, à l'industrie, prépare aux carrières consulaires et administratives » (*Le Nouveau Larousse illustré*, 1898-1907), et a pour projet d'être pour le commerce ce que l'École centrale (fondée en 1828) est pour l'industrie.

Figure 2 : L'entrée du 108, boulevard Malesherbes, Paris VIII^e^. *Ç'a été l'adresse d'HEC de sa fondation en 1881 jusqu'à 1964 date du déménagement à Jouy-en-Josas, où le nouveau campus est inauguré par le général de Gaulle. Cet immeuble est maintenant affecté à l'université Paris-IV Sorbonne.*

Quant à l'école Arago (aujourd'hui lycée Arago, place de la Nation à Paris), elle a été édifiée en 1880 en tant qu' « école primaire supérieure » : ces écoles avaient été instituées par la loi Guizot de 1833 visant à la démocratisation de l'enseignement secondaire.

POLYGLOTTE ET ADEPTE DU VOLAPÜK

Jean-Guillaume-Hubert-Victor-François-Alexandre-Auguste Kerckhoffs von Nieuwenhof est né en 1835 en Hollande, d'une grande famille d'un duché flamand. Il commence des études religieuses au petit séminaire près d'Aix-la-

Chapelle, puis vit un an en Angleterre pour parfaire son anglais. Il accompagne un jeune Américain, Clarence Prentice, pendant un an et demi comme secrétaire de voyage en Angleterre, en Allemagne et en France. Il enseigne pendant dix ans les langues en France, à Meaux et Melun, à partir de 1863. Il fait montre d'éclectisme, étudiant tout autant les langues modernes et anciennes, les mathématiques, l'histoire et l'archéologie. Il est naturalisé français en 1873, puis reprend des études aux universités de Bonn et de Tübingen où il passe son doctorat. Il gagne ensuite sa vie comme précepteur du jeune comte São Memede, qui deviendra secrétaire du roi du Portugal.

Il commence à être en contact avec le milieu militaire comme titulaire de la chaire d'allemand à l'École Militaire, qu'il perdra rapidement, un employé ayant omis de signaler sa récente naturalisation. En 1881, il devient professeur d'allemand à l'École des Hautes Études Commerciales et à l'École Arago. C'est à cette époque, à 47 ans, qu'il écrit l'article « La cryptographie militaire ». Les renseignements sont rares sur ce qui l'a mené à s'intéresser à la cryptographie. Ses relations avec le monde militaire restent assez obscures ; l'historien de la cryptographie David Kahn nous apprend qu'il aurait été mêlé à des difficultés d'ordre politique après la défaite française contre la Prusse en 1870, mais rien n'indique dans sa biographie comment il a été conduit à publier un article aussi important, dans le *Journal des Sciences Militaires*, en janvier et février 1883.

@@@@@@@

Après la publication de cet article, il s'investit pour introduire en France une langue nouvelle, le Volapük (langage du monde), inventée en 1885 par un prêtre catholique allemand Joan Martin Schleyer (1831-1912). Ce nouveau langage international connaît un succès important, mais éphémère, pendant la décennie 1880. Kerckhoffs est directeur de l'académie nationale de Volapük à Munich en 1887. Il existe à cette période plus de 180 manuels de Volapük et de nombreuses publications.

Un conflit entre Schleyer et Kerckhoffs sur le rôle et la fonction de cette langue va les séparer. Kerchoffs confirme l'esprit pragmatique qu'il montre en cryptographie : pour lui, cette nouvelle langue doit être la plus simple et la plus pratique possible, utilisable pour le commerce et les sciences. Ce conflit est à l'image des tensions sur les enjeux de la constitution des nations en cette fin de XIXe siècle, et sur le mode d'organisation sociale pour ces États. Cette langue

doit-elle atteindre la perfection littéraire ou bien doit-il s'agir d'une langue universelle ? Le mouvement Volapük décroît pour s'éteindre à partir de 1890. De 210 000 membres en 1890, il n'en reste plus que 150 en 1902.

Figure 3 : Le premier emblème de l'organisation Volapük (ca. 1880). *Menad bal – Pük bal = une humanité – une langue (in ouvrage de Charles E. Sprague, 1888)*

LA CRYPTOGRAPHIE DANS SON CONTEXTE

L'article de Kerckhoffs « La cryptographie militaire » est une des rares présentations qui met la cryptographie en perspective avec le contexte social et politique, dans une double approche, mêlant science et humanités. Alors que depuis la Renaissance, les dépêches chiffrées sont transmises par des messagers, assurant le règne des répertoires de codes et des nomenclateurs pour en établir la confidentialité, le déploiement du télégraphe optique des frères Chappe par la Convention à partir de 1793, puis du télégraphe électrique, en Angleterre à partir de 1832 et en France à partir de 1844, marque le début d'un changement fondamental de la façon de penser la cryptographie. Kerckhoffs va être un observateur attentif de cette mutation provoquée par l'apparition du télégraphe, où l'on passe du problème de la confidentialité du message à celui de la protection du système de communication. En effet,

> *il faut bien distinguer entre un système d'écriture chiffrée imaginé pour un échange momentané de lettres entre quelques personnes isolées et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux.* [p.12]

Kerckhoffs publie son article après le conflit franco-prussien de 1870 qui voit la défaite de la France. Il en tire les conséquences :

On a pu voir par les articles nécrologiques publiés en 1879 dans les journaux allemands, à l'occasion de la mort du capitaine Max Hering, le chef du service télégraphique, qui découvrit en 1870 le câble de la Seine, quels services a rendus aux assiégeants l'absence d'un système sûr de correspondance secrète entre l'armée de Paris et les généraux de la province. [p.10]

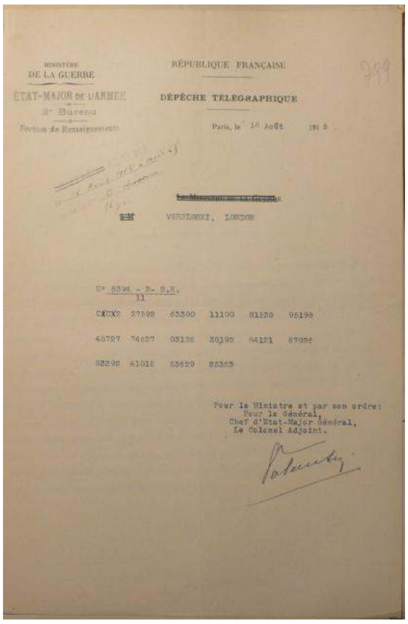
Il identifie les propriétés du télégraphe et en tire les conséquences pour l'organisation de l'Armée, qui comprend plusieurs niveaux de responsabilité et fait participer de nombreux intervenants. Il explicite les conditions à remplir pour rendre compatible cet usage collectif avec la confidentialité des échanges à l'extérieur comme à l'intérieur de ce réseau.

Comme toute méthode d'écriture cryptographique destinée aux besoins de l'armée doit pouvoir être appliquée à la télégraphie, nous n'avons à nous préoccuper que des systèmes qui sont uniquement basés sur l'emploi des lettres ou des chiffres arabes […] [p.27]

Sont en particulier exclus les symboles ésotériques et autres signes cabalistiques dont la cryptographie traditionnelle s'auréolait pour entourer de mystère les messages chiffrés.

Il précise aussi que « la séparation des mots ne doit pas être indiquée dans le texte chiffré » ; mais un fractionnement du texte est indispensable pour éviter les erreurs de transcription. C'est à Kerckhoffs que l'on doit l'usage de regrouper les lettres du cryptogramme par groupes de cinq :

Comme l'administration des télégraphes compte les dépêches secrètes par groupes de cinq, le fractionnement en pentagrammes est préférable [p.26]


MINISTÈRE
DE LA GUERRE
ÉTAT-MAJOR DE L'ARMÉE
2e Bureau
Section de Renseignements

RÉPUBLIQUE FRANÇAISE

DÉPÊCHE TÉLÉGRAPHIQUE

Paris, le 16 Août 1915

VERULOSKI, LONDON

N° 8394 - 2- S.R.

C?CX2 27592 63300 11100 81538 95198
46727 74627 03126 38192 54121 67096
83292 61016 53629 28353

Pour le Ministre et par son ordre:
Pour le Général,
Chef d'Etat-Major Général,
Le Colonel Adjoint.

***Figure 4 :** Une dépêche télégraphique de 1915, avec chiffres regroupés par cinq.*

@@@@@@@

La première partie de l'article contient des considérations historiques particulièrement bien documentées. Il dresse un inventaire très complet de l'usage du chiffre depuis l'Antiquité. De nombreux détails montrent que l'auteur a soigneusement étudié toutes ses sources.

> *Nous ne possédons cependant que des renseignements fort incomplets sur les procédés cryptographiques proprement dits en usage chez les Anciens ; en dehors des commentaires d'Ænéas-le-tacticien*[1]*, on ne rencontre au sujet de la question qui nous occupe, que des passages isolés dans Polybe, Plutarque, Dion Cassius, Suétone, Aulu-Gelle, Isidore et Jules l'Africain* [p.6]

Une seconde contribution essentielle de l'article de Kerckhoffs est de réaffirmer le rôle prépondérant du travail de décryptement – un déchiffrement sans la clé – pour évaluer la sécurité d'une méthode cryptographique. Comme le faisait déjà remarquer Charles Babbage dans un échange du *Journal of the Society of Arts* en 1854, on ne peut proposer un chiffre sûr que si l'on a soi même décrypté des chiffres très difficiles.

> *Je suis stupéfait de voir nos savants et nos prédécesseurs enseigner et recommander pour les usages de la guerre des systèmes dont un déchiffreur tant soit peu expérimenté trouverait certainement la clé en moins d'une heure de temps.* [p.10]

Pour cette raison, l'exposé des méthodes de chiffrement est systématiquement suivi d'une façon de les décrypter. Kerckhoffs démontre ainsi que la cryptanalyse est l'éclairage indispensable du cryptographe, et ce n'est qu'en en réalisant cet ingrat travail de déchiffrement sans clé que l'on peut être assuré de la sécurité d'un système de chiffrement.

Kerckhoffs expose une liste de six exigences, connues aujourd'hui sous le nom de *principes de Kerckhoffs*, que doit satisfaire un système de chiffrement pour protéger pendant un temps illimité les correspondances entre les membres d'une organisation comme l'armée :

1. *Le système doit être matériellement, sinon mathématiquement indéchiffrable ;*

1. Ænéas-le-tacticien est un militaire grec du quatrième siècle avant J.-C., auteur d'un *Traité sur la défense des places* dans lequel il expose, au chapitre XXXI, la façon d'envoyer des lettres secrètes : « Pour ce qui regarde les lettres que l'on envoie en secret, il y a différentes manières de les faire parvenir; mais il faut auparavant que ceux qui s'écrivent soient convenus de quelques points. Les exemples suivants sont les plus sûrs à imiter… »

2. *Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;*

3. *La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;*

4. *Il faut qu'il soit applicable à la correspondance télégraphique ;*

5. *Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;*

6. *Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.* [p.12]

Ces exigences expriment une situation idéale et Kerckhoffs admet lui-même qu'il doit être très difficile de les satisfaire toutes. L'exigence la plus paradoxale est bien la seconde. Comment assurer la confidentialité sans secret ? Elle s'oppose de façon radicale aux répertoires de codes ou autres dictionnaires chiffrants en usage dans les échanges diplomatiques, qui exigent de disposer en permanence du répertoire, et qui n'assurent plus aucune plus aucune protection dès l'instant où l'ennemi est arrivé à se le procurer.

> *L'administration* […] *doit absolument renoncer aux méthodes secrètes, et établir en principe qu'elle n'acceptera qu'un procédé qui puisse être enseigné au grand jour dans nos écoles, que nos élèves seront libres de communiquer à qui leur plaira, et que nos voisins pourront même copier et adopter si cela leur convient.* [p. 14]

Le secret des dépêches chiffrées doit uniquement reposer sur le secret d'une clé aisément mémorisable et modifiable. Conscient de la difficulté de concevoir un système mathématiquement indéchiffrable sans secret, il se contente, dans la première exigence, de ce qu'il appelle un système *matériellement indéchiffrable* – ce qu'il faut comprendre comme indéchiffrable *en pratique*. C'est cette sécurité pratique qui retient toute l'attention de Kerckhoffs, bien plus que la garantie mathématique. Le temps du décryptement est mis en parallèle avec la durée du secret, qui, dans le cas des campagnes militaires, n'excède pas souvent la journée.

LES DIFFÉRENTES MÉTHODES DE CRYPTOGRAPHIE

L'article se poursuit avec la description des principales méthodes de chiffrement connues, qu'il classe en trois catégories : les méthodes par transposition, les méthodes par interversion, appelées aujourd'hui méthodes par substitution, et les dictionnaires chiffrés. Ces derniers sont décrits dans la seconde partie de l'article qui paraîtra en février 1883 dans la même revue.

Les méthodes par transposition ne font que changer l'ordre des lettres. Elles sont repérables lorsque la fréquence des lettres dans le cryptogramme vaut exactement celle de la langue dont il est issu. Une méthode élégante est la grille tournante ou grille de Fleissner, du nom du colonel autrichien Edouard Fleissner von Wostrovitz (1825-1888) qui l'a présentée en 1881 dans son manuel de cryptographie. Ce procédé est décrit dans le roman de Jules Verne, *Mathias Sandorf*, en 1885. Le cryptogramme est disposé dans un carré, et en plaçant sur celui-ci une grille ajourée, les premières lettres du message clair apparaissent. La suite du cryptogramme est lue de manière similaire en tournant successivement la grille d'un quart de tour. Le défaut rédhibitoire de cette méthode est d'exiger le secret de la grille. Kerckhoffs présente toujours comme préférable une méthode consistant à décrire la transposition par une clé convenue.

La grille de transposition de *Mathias Sandorf*

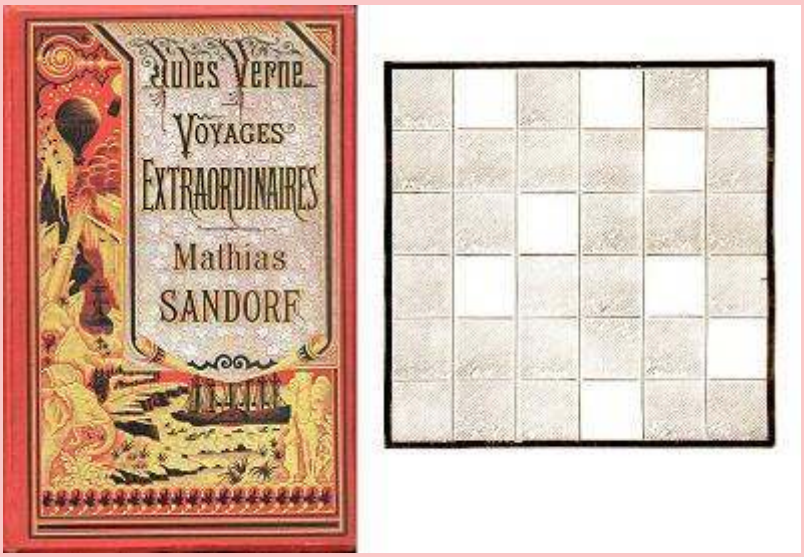


Figure 5 : L'édition originale (Hetzel 1885) de l'ouvrage, et la grille de déchiffrement qui y figure *(WikiCommons).*

Les conspirateurs y reçoivent le message chiffré suivant :

ihnalz zaemen ruiopn
arnuro trvree mtqssl
odxhnp estlev eeuart

aeeeil ennios noupvg
spesdr erssur ouitse
eedgnc toeedt artuee

Ils appliquent la grille ci-dessus à la première colonne (six mots de six lettres), puis font tourner trois fois la grille d'un quart de tour (le signe plus indique la position de la grille – nous ne faisons figurer que les deux premières étapes).

+

Dans cette position, ce qui était à l'origine en bord supérieur (tel qu'en figure 5) a tourné avec la grille : c'est devenu le bord latéral droit.

En appliquant aux deux autres colonnes le même procédé[2], les conjurés obtiennent la phrase suivante : « Tout est prêt. Au premier signal que vous nous enverrez de Trieste, tous se lèveront en masse pour l'indépendance de la Hongrie. Xrzah. »

2. Le lecteur pourra voir sur le site BibMath ou ici l'explication complète donnée par Jules Verne dans son roman. On peut voir aussi sur le site Apprendre-en-ligne un exemple de cryptage avec la méthode Sandorf (méthode de la grille tournante).

Les méthodes par interversion, quant à elles, procèdent au remplacement de chaque lettre du texte par un caractère convenu donné par un alphabet de substitution. Dans les systèmes à simple clé, l'alphabet est fixe et

> *chaque lettre de l'alphabet est* […] *représentée par le même caractère ou le même signe.* [p. 20]

À l'opposé, dans les systèmes à double clé, l'alphabet de substitution change à chaque mot ou à chaque lettre. Kerckhoffs va jusqu'à proposer un système à triple clé où la convention de changement de substitution est guidée par une troisième clé.

@@@@@@@

Troisième méthode, les dictionnaires chiffrés sont les successeurs des répertoires et autres nomenclateurs très largement utilisés dans les échanges diplomatiques depuis la Renaissance. Ils ont étés actualisés avec l'apparition du télégraphe et la loi du 13 juin 1866 qui autorise le public à correspondre en chiffre sur le territoire français.

Un des premiers codes commerciaux, destiné tout autant à cacher le sens des messages qu'à réduire la taille du télégramme taxé au caractère, est le code Sittler de 1868. Les mots et les expressions courantes sont rangés dans l'ordre alphabétique et numérotés sur chaque page de 0 à 99. Une dépêche télégraphique contient alors des séquences de quatre chiffres, indiquant le numéro de la page et l'index du mot dans la page selon une convention admise par les correspondants.

Le plus grand reproche qu'on puisse faire aux dictionnaires chiffrés, c'est d'exiger le secret, et de constituer, par le fait même de leur adoption, un obstacle à la généralisation de la correspondance cryptographique. Cette condition du secret peut d'ailleurs causer les plus graves embarras. Dans la présentation des procédés, Kerckhoffs identifie clairement ceux, comme la grille tournante, qui ne peuvent convenir pour la raison qu'ils exigent impérieusement le secret.

Il met en avant ceux dont le fonctionnement repose sur une clé. Une clé numérique peut se déduire d'un mot-clé plus facilement mémorisable :

> *On le transforme en formule numérique, en mettant à la place de chaque lettre un chiffre arabe, et en s'y prenant de telle façon que la valeur des chiffres corresponde au rang des lettres dans le classement alphabétique* [p.17]

Clé numérique, un exemple donné par Kerckhoffs

Ainsi, le mot-clé *Champigny* se traduira-t-il en clé numérique par [p.20]:

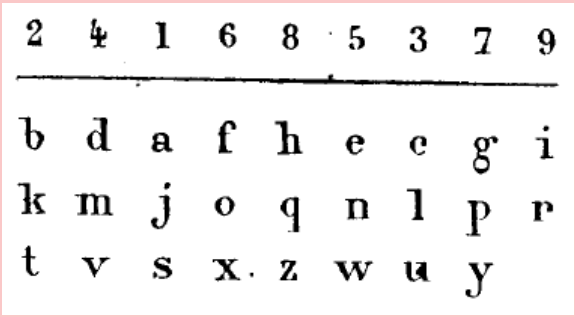
étape 1

ACGHIMNPY ↔ CHAMPIGNY

123456789 ↔ 241685379

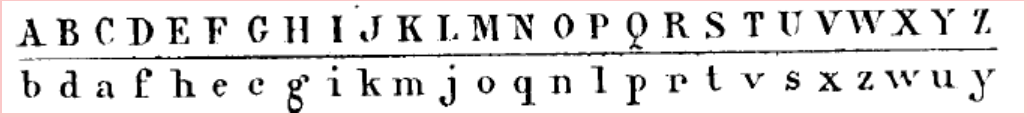
(à droite, on met les lettres dans l'ordre alphabétique, et on leur attribue le chiffre d'ordre correspondant)

étape 2



(la clef 241685379 nous permet de classer les lettres ainsi – le lecteur s'en convaincra aisément)

étape 3



(on reporte l'alphabet créé en étape 3 ce qui donne le tableau de correspondance des lettres)

Même lorsqu'elles n'exigent pas le secret et reposent sur l'utilisation d'une clé, ces méthodes par transposition sont déclarées ne pas convenir en raison de leur faiblesse. Elles ne satisfont pas le premier desideratum sur l'indéchiffrabilité :

> *Quelque compliquée que cette transposition puisse nous paraître, le déchiffrement du cryptogramme* […] *ne saurait jamais présenter de difficultés insurmontables* [p.18]

Les interversions à simple clé ne valent guère mieux. Leur décryptement est présenté en détail en reprenant les étapes qu'avait énoncé Al-Kindi (801-873) dès le IX^{e} siècle dans son traité sur l'extraction de l'obscurité :

> *Le déchiffrement d'un cryptogramme dont on n'a pas la clé comporte deux opérations bien distinctes : un calcul de probabilité et un travail de tâtonnement* [p.23]

Le calcul de probabilité repose sur l'observation de la fréquence et la rareté des caractères, et le tâtonnement sur l'étude, dans la langue du texte, des combinaisons possibles et impossibles de lettres. Sur la sécurité des interversions à simple clé, le verdict de Kerckhoffs est sans appel :

> *En thèse générale, il suffit* […] *de connaître le caractère qui représente la lettre E, pour être assuré de trouver* […] *la signification de toutes les autres* [p.24]

E = 185	N = 71	D = 42	F = 14	B	= 5
S = 88	T = 65	M = 36	Q = 10	H	= 4
R = 78	O = 57	C = 34	G = 8	Z	= 3
I = 74	U = 52	P = 24	X = 7	Y	= 1
A = 72	L = 46	V = 16	J = 6	K et W	= 0

Figure 6 : Fréquences d'occurrence des lettres données par Kerckhoffs [p. 24] : *« Un calcul que j'ai fait sur quelques circulaires du Ministre de la guerre m'a donné une moyenne de 560 consonnes et 440 voyelles sur 1000 lettres », se répartissant comme ci-dessus.*

Un système adapté à l'usage militaire ne peut reposer que sur une interversion à double, voire à triple clé. Ces méthodes, dont l'origine remonte à la Renaissance italienne, sont présentées dans toutes leurs variantes, ainsi que les dispositifs qui aident à leur mise en œuvre : la réglette de Saint Cyr (p. 31) et le cadrant chiffrant (p. 33). Leur décryptement est beaucoup plus difficile. Il est le résultat d'avancées alors récentes de Babbage (non publiées en 1846)[3] et de Kasiski (1863). Ceci est présenté dans la deuxième partie de l'article.

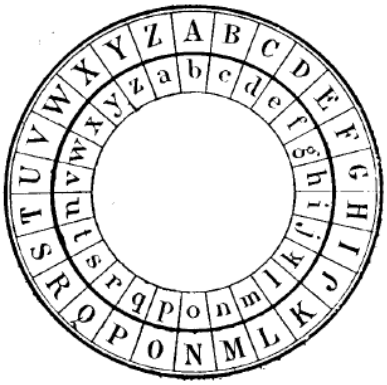


Figure 7 : Un exemple de « cadran chiffrant » *(illustration Kerckhoffs p. 33)*

3. Deux raisons sont invoquées pour expliquer que Babbage n'ait finalement pas publié sa méthode : 1°) Esprit inventif particulièrement productif, son travail n'était pas compatible avec la publication qui impose un arrêt au processus d'invention. Il existe les traces d'un projet d'ouvrage *Philosophy of Deciphering* qui n'a jamais vu le jour ; 2°) Il a entretenu une relation suivie avec l'amiral Beaufort, et, l'Angleterre étant impliquée dans la guerre de Crimée entre 1853 et 1856, il est possible qu'on lui ait demandé de taire ses découvertes.

Le principe de Kerckhoffs

Il est notamment une des six règles de Kerckhoffs [p.12] bien connue de nos jours, la seconde (« Il faut que [le système] n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi »).
Qu'entend-on par là, puisque tous les systèmes de sécurité dépendent du fait de garder quelque chose secret ? En fait, ce qui est gardé secret doit être ce qui est le moins coûteux à changer si le secret s'avérait divulgué.

Un mécanisme de chiffrement peut par exemple être réalisé par un matériel informatique et des logiciels associés qui sont largement diffusés et utilisés par de nombreuses personnes. Si la sécurité exigeait de tenir ce matériel secret, alors, s'il venait à être divulgué, il faudrait mener un travail considérable de développement, de tests et de logistique pour mettre à disposition les nouveaux algorithmes. À l'opposé, si le secret de l'algorithme n'est pas important, et si seul celui de la clé l'est, alors sa compromission sera moins gênante : il suffit de générer une nouvelle clé et la distribuer. Tout secret est un point de faille possible : moins l'on a d'éléments secrets, moins l'on a de difficultés à rétablir un système après qu'il soit cassé.
Les systèmes actuels à double clé (clé publique / clé privée), fondés sur les grands nombres premiers, répondent bien à cet impératif. Par exemple, dans l'algorithme RSA, lorsque la clé vient à être « cassée », il suffit de trouver deux nombres premiers plus grands permettant de produire de nouvelles clefs, sans changer le système lui-même.

Kerckhoffs avait détaillé son principe de manière visionnaire quand il disait que le secret était un défaut [p. 14] :

Et ici j'entends par secret, non la clef proprement dite, mais ce qui constitue la partie matérielle du système : tableaux, dictionnaires ou appareils mécaniques quelconques qui doivent en permettre l'application [NdA : ce qui correspond aux logiciels et ordinateurs mentionnés plus haut]

@@@@@@@

Ne pas exiger le secret n'implique pourtant pas que la méthode employée doive être décrite publiquement. En raison de leur culture du secret, les militaires maintiennent secrètes les méthodes qu'ils utilisent. Les lecteurs pourront s'amuser de la contradiction portée dans la conclusion de la deuxième partie de l'article, maniant à la fois le secret et le non-secret :

> *II vient d'être présenté à la Commission de télégraphie militaire un nouveau système de cryptographie, qui me paraît réaliser tous les*

desiderata que j'ai exposés en commençant : indéchiffrabilité complète, simplicité, non-nécessité du secret ; des considérations de haute convenance m'empêchent d'en dire davantage pour le moment.

Il n'en reste pas moins que les principes énoncés par Kerckhoffs dans son article restent d'une grande actualité. Encore aujourd'hui, une **méthode publique** est présentée comme plus sûre après avoir résisté aux nombreuses attaques d'une communauté ouverte et active de cryptanalystes acharnés. Kerckhoffs, en tirant les conséquences de l'apparition du télégraphe, a initié un mouvement qui s'est poursuivi pendant près d'un siècle, voyant décroître progressivement la part secrète d'un système cryptographique. Ce mouvement a vu son aboutissement avec l'introduction en 1976 de la cryptographie à clé publique dans laquelle même la clé de chiffrement peut être rendue publique, seule la clé pour déchiffrer devant être maintenue secrète.

Il conclut ainsi sa présentation, à la fin de l'article de février 1883 :

Je tiens, en terminant, à insister sur ce point, que la valeur d'un système de cryptographie destiné aux besoins de la guerre est en raison inverse du secret qu'exige son maniement ou sa composition. Il dépendra donc de l'Administration d'assurer l'avenir de la cryptographie militaire, en n'accordant ses suffrages qu'à l'invention qui s'appuiera sur le principe que Du Carlet, un des maîtres de notre art au XVII^e^ siècle, avait inscrit comme devise en tête de sa méthode[4], principe qui résume d'ailleurs toute ma thèse, à savoir qu'un chiffre n'est bon qu'autant qu'il reste indéchiffrable pour le maître lui-même qui l'a inventé : Ars ipsi secreta magistro[5].

■

(mai 2013)

4. [note de bas de page de Kerckhoffs] *La Cryptographie, contenant une très subtile manière d'escrire secrètement, composée par maistre Jean Robert* Du Carlet ; 1644.
5. « un art caché au maître lui-même » : même l'inventeur du cryptage ne doit pas pouvoir décrypter un message codé avec sa technique, qui ne lui serait pas adressé.