1. DE LA CRYPTOGRAPHIE CLASSIQUE À LA CYBER-SÉCURITÉ MODERNE

1.1. INTÉRÊT HISTORIQUE DE LA CRYPTOGRAPHIE CLASSIQUE

S'il s'agissait seulement de « bachoter » un concours, il n'y aurait aucune utilité à aborder même brièvement l'histoire de la cryptographie. Mais on peut croire qu'il y aura dans le futur des épreuves orales où les connaissances littéraires ou historiques des candidats pourront être utiles. Le deuxième objectif est donc de proposer un bref exposé historique actualisé par rapport aux ouvrages et cours des grands cryptologues de la fin du XIX^{e} siècle et du début du XX^{e} siècle comme Bazeries, Givierge ou Sacco. Restituer les procédés dans leur contexte facilite leur assimilation et la compréhension des limites. On découvre l'efficacité de certaines techniques du XIX^{e} siècle comme le calcul d'indices de coïncidence basés sur la distribution des lettres, des bigrammes et trigrammes pour deviner le type de chiffrement, voire la longueur des clés. L'exposé est très loin d'être exhaustif et n'a pas la prétention d'être complet comme des études récentes à but exclusivement historique.

Des cryptologues éminents ont publié des « traités de cryptographie ». Citons en chronologiquement quelques-uns : Al-Kindi (801-873, Bagdad) redécouvert récemment, Charles Babbage (1791-1871), Friedrich Kasiski, Marcel Givierge, Étienne Bazeries, André Lange, Felix Delastelle, Gaëtan de Viaris en France, Luigi Sacco en Italie, William Friedman aux États-Unis. La modernisation permet d'exposer l'ensemble des principales méthodes historiques qu'ils exposent dans un volume beaucoup plus court et facile à appréhender. Moderniser l'exposé de cette cryptographie classique, c'est ramener ces systèmes de chiffrement à des permutations, soit sur le rang alphabétique des caractères du message, les méthodes de substitution (le chiffre de César est un des premiers), soit sur leur ordre, les méthodes de transposition (le bâton de Plutarque ou scytale des Spartiates).

En cryptographie classique, le chiffrement est symétrique, émetteur du message en clair et récepteur ont besoin initialement de partager un même secret, la « clé », un mot, une phrase et dans le cas des systèmes à dictionnaire, celui-ci. L'impossibilité pratique de cet échange d'information secrète entre utilisateurs anonymes et sites Internet a conduit à une avancée majeure : la cryptographie asymétrique à clé publique + clé privée conceptualisée par Diffie et Hellman en 1976. Une fois mise en œuvre dans le chiffrement RSA (1977), elle a permis le développement des transactions informatiques sécurisées *sans que l'initiateur (avec un navigateur) ait eu à échanger un secret par des moyens physiques sécurisés* avec le site auquel il se connecte, il n'y a pas besoin de canal protégé préétabli pour échanger les clés, on le crée. Cet *échange de clé initial* permet d'établir une clé secrète *symétrique* connue des seules parties

pour *le chiffrement-déchiffrement ultérieur* du flux d'informations beaucoup plus rapide fait par des algorithmes symétriques comme DES, IDEA, AES 256 réalisés par des circuits électroniques pour implémenter des méthodes sophistiquées mais basées sur les approches de la cryptographie classique (transposition, substitution). Donc la vitesse de l'échange RSA est sans importance, puisqu'il ne sert brièvement qu'au début de la transaction et *on peut augmenter la taille du RSA* autant que l'on veut sans inconvénient pratique.

1.2. EXPOSÉ DU PLAN

Voici le contenu des chapitres dont on n'a pas parlé jusqu'à présent.

1.2.1. Méthodes de substitution

Nous suivrons approximativement l'ordre historique des méthodes de chiffrement, puisqu'il y eut co-existence entre elles. Le chapitre 2 est donc celui des méthodes de substitution : un caractère est remplacé par un autre ou un couple (bi-gramme) comme dans le chiffrement de Polybe ou celui de Playfair.

1.2.2. Dictionnaires chiffrés

À partir du XVI^{e} siècle l'utilisation de dictionnaires chiffrés s'est répandue, c'est le Chapitre 3. Pendant longtemps on a exigé des systèmes que le chiffrement-déchiffrement puisse se faire très vite avec du papier et un crayon et par des chiffreurs d'un niveau de base (lire et écrire). C'était le cas des systèmes à dictionnaire chiffré (un code remplace une lettre, syllabe ou un mot usuel) popularisés par le chiffre de Louis XIV ou celui de Napoléon 1er. Les méthodes par dictionnaire chiffré (table chiffrante et table déchiffrement) ont donc continué à fleurir au XIX^{e} siècle pour la correspondance commerciale et militaire. Bien que des méthodes algébriques comme le chiffre de Vigenère (1586) aient été connues, les dictionnaires offraient l'avantage de la rapidité tant pour le chiffrement que le déchiffrement. Dans la situation où le dictionnaire n'est pas connu mais où on connaît un corpus de messages chiffrés ou déchiffrés, on pourrait appliquer les méthodes de « *deep learning* » pour approcher la reconstitution de ces dictionnaires. En l'absence d'un nombre suffisant de messages, cette approche ne permettra de reconstituer que très partiellement un dictionnaire militaire français de 1870-1890, dans le chapitre 3. Pour l'historien il n'est pas inutile de s'assurer que tous les messages chiffrés avec des procédés anciens continuent à pouvoir être déchiffrés. On a vu dans un film de 2019 sur l'affaire Dreyfus le rôle joué par le télégramme secret de Panizzardi dans le dossier d'accusation. Saurait-on encore les décoder ? Sans aucun doute, puisque le procédé de dictionnaire chiffrant peut-être reproduit, c'est un dictionnaire du commerce, le Baravelli, qui est disponible. Mais pour des systèmes militaires « à dictionnaire »

de la fin du XIX^{e} siècle, dont les dictionnaires ont disparu et pour lesquels seuls les messages déchiffrés sont archivés (jamais les chiffrés ou les brouillons de calcul), il s'avèrerait impossible, le fameux Étienne Bazeries n'étant plus là, de déchiffrer des messages chiffrés dont on découvrirait l'existence.

1.2.3. Chiffrement par transposition

Simultanément avec les dictionnaires, les méthodes de transposition, notamment les grilles à trous, se sont développées au XVI^{e} siècle, elles sont, au XIX^{e}, devenues le principal système de l'armée austro-hongroise, on les exposera au chapitre 4.

1.2.4. Machines cryptographiques

À la fin du XIX^{e} siècle sont apparus des appareils destinés à faciliter l'utilisation des méthodes de substitution simple ou plus compliquées, abaques mécaniques, cercle chiffrant, cylindre de Bazeries, téléimprimeur chiffrant utilisés par tous les belligérants de la Seconde Guerre mondiale. Ils ont été utilisés aussi bien pour les communications longue distance (TSF) que tactique (TPS, télégraphie par le sol) entre les lignes. Dans les années 1920, naîtra la fameuse Enigma. Les machines cryptographiques seront décrites dans le chapitre 5.

1.2.5. Chiffrements modernes : symétriques par bloc et RSA, extraction de racines carrées

Avant la cryptographie symétrique, le dernier perfectionnement des méthodes classique est le chiffrement symétrique par bloc DES de 1970. Il y a eu des épreuves de sélection Alkindi basées sur les schémas de Feistel permettant de construire les permutations du DES, d'où l'inclusion du chapitre. Pour la préparation des TP sur le sujet en terminal scientifique, il y a une section brève mais complète sur le protocole RSA par clé publique et l'échange de la clé symétrique de session (échange Diffie-Hellman) en s'appuyant sur des exercices avec la boîte à outils Python. Cela permet de donner au lecteur une vision moins naïve du RSA qu'avec les simples schémas Bob-Alice qu'on trouve abondamment et qui omettent le « mode hybride » RSA puis chiffrement symétrique avec AES notamment utilisés dans la réalité. Il y a aussi un exposé sur le crypto-système de Rabin basé sur la difficulté d'extraire les racines carrées dans un groupe Z/nZ si on ne connaît pas la factorisation de n, de même qu'on résout le RSA si on la connaît.

1.2.6. Autres chapitres

Les autres chapitres sont décrits dans cette introduction notamment le chapitre 7 : « boîte à outils Python », et bien sûr, le chapitre 8 pour les annales Alkindi corrigées. Dans la boîte à outil il n'y a que les listings Python des algorithmes les plus

élémentaires (Euclide, etc.) avec un lien sur le site de l'éditeur pour les autres. Le chapitre 9 est le chapitre pour spécialiste de télécommunication et de cyber-sécurité dont j'ai justifié le rôle dans la démarche de formation des élèves. Le dernier chapitre est un dictionnaire d'acronyme en cryptographie et en telecoms.

1.3. NE PAS RÊVER AVEC LA CRYPTOGRAPHIE QUANTIQUE

Dans ce livre, il n'y a aucun exposé sur les recherches en cryptographie quantique, l'auteur ne croyant pas que ceux-ci soient opérationnels pour des cryptanalyses réelles au moins pour les 30 années à venir et cela ne le concernera alors largement plus. En effet, plus vite que le progrès en nombre de qbits dans des machines dont le cœur est à 1 °K ou moins, le chiffreur peut augmenter la taille des mots chiffrés (4 096 ou même 8 192 en 2019) alors que le maximum technologique d'aujourd'hui (2020) est de moins de 100 bits et qu'il a fallu attendre 20 ans pour cela depuis les premières démonstrations IBM en 1998 (2 qbits) or il faudrait 1 024 bits pour casser du petit RSA.

À partir de la démonstration de l'algorithme de factorisation de Schor [1.29], 1994, pour les nombres entiers, on n'a toujours pas construit de machine qui casse le RSA 2048 pourtant obsolète. Y en aurait-il au bout des milliards dépensés à travers le monde, qu'une réunion de normalisation du protocole TLS (sympathique et arrosée dans un bel endroit comme par exemple à Beaune) rendrait tous ces progrès vains en décidant, dans la liste des clés supportées, de multiplier le nombre de bits par 2 sans aucun coût (les participants se donnant une grande tape dans le dos à la fin de la réunion). Ils auraient pu multiplier par 4 mais souhaitaient se revoir avant trop longtemps, les relations amicales s'étant nouées ou mieux si affinité, ils avaient déjà décidé de Bordeaux pour la réunion suivante. La tortue-Sisyphe hyperfinancée ne rattrapera pas le lièvre, voilà un cas indiscutable où la défense gagne à coup sûr. Les demandes du NIST US (*National Institute of Standards and Technology)* pour des systèmes de chiffrement plus sûrs que le RSA, y compris le RSA courbes elliptiques, sont intéressantes d'un point de vue théorique mais surdimensionnées par rapport au besoin. Sans une nouvelle voie révolutionnaire dans la technologie des machines quantiques, ce besoin de sécurité est éternellement satisfait par une augmentation de l'ordre des groupes algébriques. On peut donc partager l'opinion de Serge Haroche [1.10], prix Nobel de Physique 2012 : « les ordinateurs quantiques utilisables pour les vrais problèmes ne verront jamais le jour » ; partagée ou non, cette position permet à des étudiants de montrer qu'ils ont réfléchi au sujet, et c'est déjà un résultat.

1.4. PYTHON POUR LE DÉVELOPPEMENT DE SYSTÈMES CRYPTOGRAPHIQUES PAR LES ÉLÈVES DU SECONDAIRE

Anticipons un peu. Les ordinateurs, actuellement interdits, seront introduits dans les concours et Python est aussi le langage enseigné dans l'Éducation nationale depuis la classe de seconde à partir de la rentrée 2019. Le tout Python est certes exagéré puisqu'on trouve des ingénieurs sortant de grandes écoles françaises réputées qui ne connaissent que ce langage informatique. Ce sont les mêmes dont les entreprises qu'ils rejoignent se plaignent de leur niveau. Éternel débat sur la culture générale. Ce choix de Python étant fait, le 3^{e} objectif du livre est donc de l'enseigner autour de l'application cryptographique, cela est efficace comme le montre d'autres ouvrages qui donnent envie d'apprendre Python comme [1.3], [1.15]. Pour en souligner l'importance, rappelons que les élèves ont le droit à une calculatrice au Bac à condition qu'elle ait le « MODE EXAMEN » : c'est un nouveau mode mis en place par les constructeurs depuis quelques années à la demande de l'Éducation nationale. Il permet de verrouiller l'accès aux programmes personnalisés dans la calculatrice et donc d'éviter la triche. Par conséquent les élèves ne peuvent pas venir *au Bac* avec leur boîte à outils d'algorithmes personnels, *par contre dans les séances de TP de préparation*, cela permet de gagner du temps pour se concentrer sur la maîtrise des concepts. Les programmes se chargent sur le site de l'éditeur et, avantage de pérennité des livres « papier », peuvent aussi être récupérés à partir de l'impression.

En revanche, l'usage du logiciel Sage a été écarté (pourtant préconisé par l'Éducation nationale dans les universités mais un peu méprisé par les enseignants pratiquant le calcul formel, car n'étant pas assez industrialisé (!)), ainsi que Mathematica ou Mathlab pour la programmation des algorithmes, bien qu'ils fussent beaucoup plus rapides grâce, dans le domaine de la cryptographie, aux opérations sur les anneaux d'entiers Z/nZ qui évitent de programmer les opérations de base même élémentaires comme l'inversion des éléments de ces anneaux. Ils comprennent aussi les meilleurs algorithmes pour la factorisation des entiers ou le log discret ainsi que de multitudes d'autres fonctions merveilleuses. Ce n'est pas du reste encore au programme du secondaire. C'est pour cela que dans la boîte à outils Python on trouve l'algorithme d'Euclide étendu qui permet de construire beaucoup de choses, et l'inversion de matrices dans Z/nZ (utilisé pour le déchiffrement de Hill).

Les références sont présentées à la fin de chaque chapitre, on trouvera pour les copies papier des ouvrages anciens, le nom de la bibliothèque où on peut les consulter, Service Historique de la Défense (Vincennes), BNF, Bibliothèque Sainte-Geneviève, Centre de Documentation de l'École militaire. C'est un grand plaisir de pouvoir consulter ces ouvrages, le papier montre vraiment l'ancienneté et inspire le respect pour ces anciens cryptologues. Ces références ont toutes été contrôlées avec des commentaires pour distraire de l'aridité de ce type de lecture.

Voici donc les objectifs de ce livre. Ce sera un succès s'il aide des enseignants ou des candidats à avoir de meilleurs résultats aux concours de cryptographie ou au Bac, ou à des étudiants pour élargir un peu leurs connaissances en cryptographie au-delà simplement de la cryptologie algébrique universitaire, qui ignore presque complètement la cryptographie classique en l'absence de matière à faire des maths autres qu'élémentaires.

Remerciements

Je remercie les enseignants et intervenants de Paris-Sorbonne en cryptologie algébrique et calcul formel dans le cadre des maîtrises de math M1 et M2 ou de la préparation à l'agrégation de maths, Leonardo Zapponi, Pierre-Vincent Koseleff, Fabrice Rouiller (par ailleurs président d'Aromath), Razvan Barbulescu, Antonin Guilloux, Antoine Joux, Damien Vergnaud.

De même pour les enseignants de cryptographie de l'ENS, Jacques Stern, David Pointcheval : leur cours de MPRI M1 est très différent mais destiné plutôt à apprendre les rudiments de l'ingénierie des systèmes cryptographiques avec entre autres les compromis temps de calcul-taille mémoire et les systèmes de preuve sans divulgation de connaissance.

Mes remerciements à Romain Giuge, professeur agrégé de maths dans un lycée parisien ; il a résolu Alkindi 2016 n°4 sur lequel l'auteur séchait. Son aide a aussi été précieuse pour calibrer mes exercices de cryptographie pour le Bac scientifique. Nous avons collaboré aussi pour les vérifications et solutions de Alkindi 2020, qui est un très bon cru pour l'astuce des exercices. Les deux exercices finaux de 2020 et 2019 sont conçus pour ne pas être résolubles sans les auteurs de ces énigmes… ce qui montre les limites du principe cryptographique de Kerckhoffs [1.41].

Remerciements à Ahmed Friaa pour ses descriptions des méthodes de chiffrements par carré magique et à Pascal Adjamagbo enseignant à Paris-Sorbonne pour les améliorations de rédaction concernant l'algèbre du chiffrement de Hill, afin de l'adapter à la population visée.

Geneviève Bellissard a édité ce nouveau livre avec soin, comme elle l'avait fait pour deux livres précédents sur d'autres sujets. Christian Sauzereau a fait aussi une relecture détaillée très efficace.

Juin 2020.

Références

Traités de cryptographie historique, ouvrages anciens et récents :

[1.1] Bauer, Friedrich, *Decrypted Secrets: Methods and Maxims of Cryptology*, Springer, 2013, 449 pages*, l'introduction donne une histoire récente de la cryptologie assez détaillée mais biaisée (le seul cryptologue français cité est François Viète !, toujours la jalousie de Koch vis-à-vis de Pasteur).*

[1.2] Bazeries, Étienne (C^{dt}) (1846-1931), *Cours de cryptographie*, 1920, CDEM patrimoniale.

[1.3] Bro Frédéric, Rémy Chantal, *Python et les 40 problèmes mathématiques - Python par l'exemple et pour les maths, avec corrigés détaillés*, éd. Ellipses, 2016.

[1.4] Delastelle, Felix, Marie (1840-1902), *Traité élémentaire de cryptographie*, éd. Gauthier-Villars, 1902.

[1.5] Davys, John, *An Essay on the Art of Decyphering*, Biographia Britannica*, 1737, comporte la description des déchiffrements de John Wallis pendant la guerre civile en Grande-Bretagne (chiffrements par alphabet secret).*

[1.6] Delastelle, Felix-Marie, *Traité élémentaire de cryptographie*, éd. Gauthier-Villars, 1902.

[1.7] della Porta, Giovanni-Battista, *De furtivis litterarum notis, vulgo de ziferis*, Naples, 1563, *un des premiers systèmes de substitution polyalphabétiques.*
[1. 8] Givierge, Marcel (Général) (1871-1931, X1892), *Cours de cryptographie*, éd. Berger-Levault, Paris 1925, CDEM patrimoniale, *systèmes à dictionnaires, chap XV.*
[1.9] Guillot, Philippe, *Cryptologie, l'art des codes secrets*, éd. EDP Sciences, 2013.
[1.10] Haroche, Serge, *Intrication et information quantique,* Collège de France, 2006.
[1.11] Kahn, David, *The codebreakers*, Mc Millan Company éd., 1967. *Il y a une biographie d'Alberti, Leon, Battista (1404-1472), l'inventeur du cadran chiffrant avant Kronberg et Jefferson (voir chapitre 5), premier chiffrement polyalphabétique, et du chiffrement avec plusieurs substitutions pour la même lettre afin de combattre l'analyse de fréquence pour le déchiffrement. Il peut ainsi étaler l'histogramme des symboles utilisés.*
[1.12] Lacroix, Paul, *Les secrets de nos pères*, vol. II, « La cryptographie », éd. Adolphe Delahays, 1858-1859, BNF. *4e partie : méthodes à répertoires (très bref sans utilité), la langue française a 8 000-8 500 mots communs.*
[1.13] Lange André, Soudart E. A., *Traité de cryptographie*, éd. Felix Alcan, 1925, *CDEM patrimoniale, Section III, Chap. III, Dictionnaires chiffrés. Aborde p. 203 le décryptement d'un cryptogramme chiffré avec un dictionnaire tenu secret. On classe les mots les plus fréquents du message en face des groupes fréquents.*
Sur 1 865 mots :

de	la	et	être	les	avoir	le	des	d'	à	dans	qui	du	en	il	ou	l'	ce	que	un	une	par	s'	on
94	52	50	46	39	38	38	34	30	27	26	26	23	23	20	20	19	18	18	17	17	15	14	13

[1.14] de Lastours, Sophie, *1914-1918 : la France gagne la guerre des codes secrets*, éd. Taillandier, 1998, 262 pages.
[1.15] Lecouvey, Nicolas, *100 énigmes mathématiques résolues avec Python*, éd. Ellipses, 2018.
[1.16] Müller, Didier, *Les codes secrets décryptés*, City Éditions, 2011, 2e édition *(existe aussi 3e édition en e-book).*
[1.17] Sacco Luigi (Général) (1883-1970), *Manuel de Cryptographie*, éd. Payot, 1951, préface Lcol. R. Léger.
[1.18] Singh, Simon, *Histoire des codes secrets : de l'Égypte des Pharaons à l'ordinateur quantique*, éd. J.-C.Lattès, 1999, 430 pages, *un ouvrage de vulgarisation agréable écrit par un journaliste scientifique.*
[1.19] Stern, Jacques, *La science du secret*, Odile Jacob éd., janvier 1998, v*oir aussi Cours de cryptographie, MPRI M1, ENS Ulm.*
[20] Valerio, Paul, *De la cryptographie. Essai sur les méthodes de déchiffrement*, éd. Baudoin, Paris, 1893, 230 pages.
[1.21] Vergnaud, Damien, *Exercices de Cryptographie*, Masson, Chapitre 1, 3e édition, 2018.
[1.22] de Viaris, Gaëtan, Henri, Léon (1847-1901), *L'art de chiffrer et déchiffrer les dépêches secrètes*, éd. Gauthier-Villars, G. Masson, 1893, 175 pages, Bibliothèque Sainte-Geneviève et http://hdl.handle.net/1908/4096, provenance Univ. de Lille. *Le livre sert essentiellement à de Viaris pour présenter sa nouvelle méthode et alimenter sa polémique avec E. Bazeries dont il veut montrer qu'il a pu déchiffrer son cylindre chiffrant. Lu 17/1/2020.*
[1.23] Viète, François (1540-1603), *Viète était chargé de déchiffrer les codes secrets des ennemis de la France. Inventeur de la notation symbolique en algèbre, il n'a laissé qu'un court manuscrit indiquant quelques méthodes de déchiffrement pour les méthodes de substitution, à la source de cette discipline.*
[1.24] de Vigenère, Blaise, *Traités des chiffres ou secrètes manières d'escrire*, Paris, 1586.
[1.25] Gomez, Joan. Codage et Cryptographie, RBA ed., traduction 2019, *un ouvrage très général facile à lire mais pas destiné à la préparation d'épreuves.*
[1.26] Schneier, B., *Applied Cryptography*, Wiley ed., 1999.

Articles, études, sites internet :

[1.27] Concours Alkindi, http://www.concours-alkindi.fr
[1.28] Al-Kindi, *Manuscript on Deciphering Cryptographic Messages*, *ouvrage qui aurait été retrouvé en 1987, début de sa notoriété moderne.*

[1.29] Shor, P.W., Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE Comput. Soc. Press, 1994, p. 124-134.
[1.30] Durand-Richard Marie-José, Guillot Philippe, http://images.math.cnrs.fr/Comment-les-mathematiques-ont-investi-la-cryptologie-1.html
[1.31] Arboit, Gérald, *L'émergence d'une cryptographie militaire en France*, Note Historique N° 15, Juillet 2008, CF2R.
[1.32] Bardin, Étienne-Alexandre (Général) (1774-1841) *Dictionnaire de l'Armée de terre*, éd. J. Correard, 1849, BNF, *Ne traite pas des dictionnaires chiffrés, donné comme référence pour éviter de chercher des dictionnaires chiffrés.*
[1.33] Baudoin, Roger (Capitaine), *Éléments de cryptographie*, éd. A. Pedone, 1939.
[1.34] Bazeries, Étienne (1846-1931), *Les chiffres secrets dévoilés, étude historique sur les chiffres appuyée de documents inédits tirés des différents dépôts d'archives*, éd. Eugène Frasquelle, 1901, 275 pages, microfiches BNF, CDEM patrimoniale. *Ouvrage historique présenté comme général mais destiné en réalité à vanter les mérites du cylindre chiffrant du Cdt Bazeries.*
[1.35] Bazeries, Étienne, *Les chiffres secrets dévoilés*, éd. Carpentier, 1901, CDEM patrimoniale, *un historique des méthodes et le déchiffrage de codes d'actualité à la fin du XIX^e siècle [celui du Général Boulanger, celui du duc d'Orléans (un système trivial avec remplacement des lettres par un code parmi 26 entre 1111 et 1137), communards, anarchistes].*
[1.36] Bazeries, Étienne, *Les chiffres de Napoléon 1^er, pendant la campagne de 1813 : épisodes du siège de Hambourg : documents inédits trouvés a Aix-la-Chapelle, tirés des Archives nationales et du Dépôt de la guerre*, éd. M. Bourges, 1896, 57 pages.
[1.37] Givierge, Marcel, *Premières notions de cryptographie*, éd. Berger-Levault, Paris, 1935.
[1.38] Givierge, Marcel, *Au service du chiffre, 18 ans de souvenirs, 1907-1925*.
[1.39] Givierge, Marcel, *Étude historique sur la section du chiffre*.
[1.40] Kerckhoffs, Auguste, *La Cryptographie militaire, ou, des chiffres usités en temps de guerre : avec un nouveau procédé de déchiffrement applicable aux systèmes à double clef*.
[1.41] Kerckhoffs, Auguste, « La cryptographie militaire », *Journal des sciences militaires*, vol. IX, p. 5-38, Janvier 1883, p. 161–191, Février 1883, *énonce les 6 principes de Kerckhoffs dont le fameux N° 2 : « Il faut qu'il (le système cryptographique) n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi », page 12. Le secret n'est pas l'algorithme, c'est la clé en termes modernes,* https://www.petitcolas.net/kerckhoffs/crypto_militaire_1.pdf
[1.42] de Lestours, Sophie, *La France gagne la guerre des codes secrets*, Taillandier, 23 oct. 1998, 262 pages.
[1.43] Colonel Olivari, *Souvenirs du Service de renseignement cryptographique militaire*.
[1.44] Schneider L. (Cdt), *Description d'un système de cryptographie à l'usage de l'armée*, éd. L. Fournier, 1912, CDEM patrimoniale, *Système sans dictionnaire, on ne trouve pas trace d'une utilisation par l'Armée, il écrit « il remplacerait très avantageusement en temps de paix le dictionnaire actuellement en cours dans l'armée, il ne nécessite que papier et crayon ».*
[1.45] *Dictionnaires, codes et cryptographie,* 1re partie, « Le secret de la correspondance », https://www.dicopathe.com/dictionnaire-codes-et-cryptographie-1ere-partie/
[1.46] *Dictionnaires, codes et cryptographie*, 2e partie, « Le temps des espions »,
https://www.dicopathe.com/dictionnaires-codes-et-cryptographie-2eme-partie-complots-et-espionnage/
[1.47] Shannon, Claude, « Communication Theory of Secrecy Systems », Bell System Technical Journal, vol. 28, p. 656-715, oct. 1949. *Les principes de confusion (substitutions pour cacher les symboles) et de diffusion (transpositions pour cacher la position d'un symbole).*
[1.48] Concours TRACS, https://tracs.viarezo.fr, *organisé par Viarezo et la DGSE, 2e édition 14/12/2019 à Centrale Supelec.*
[1.49] Nguyen Nicolas, Daniel Stéphane, Fontes Mathieu, *Mathématiques expertes*, éd. Ellipses, *cours de terminale, nouveaux programmes 2020.*