



[Les 3000 premières années \(2000 av. J.-C. - 1000\)](#)







[L'éveil de l'occident \(1000 - 1800\)](#)



[L'essor des communications \(1800 - 1970\)](#)

[La cryptologie moderne \(de 1970 à nos jours\)](#)

Les 3000 premières années (2000 av. J.-C. - 1000)




Les écritures secrètes semblent être nées spontanément dès que, dans un pays, une partie importante de la population a su lire.







DATES	SOURCES	IMAGES	COMMENTAIRES
Environ 1900 avant J.-C.	Kahn p. 1		Un scribe égyptien a employé des hiéroglyphes non conformes à la langue correcte dans une inscription. Kahn le qualifie de premier exemple documenté de cryptographie écrite.
1500 avant J.-C.	Kahn p. 5		Une tablette mésopotamienne contient une formule chiffrée pour la fabrication de vernis pour les poteries.
600-500 avant J.-C.	Kahn p. 6, Singh p. 42		Des scribes hébreux mettant par écrit le livre de Jérémie ont employé un simple chiffre de substitution connu sous le nom d' Atbash . C'était un des quelques chiffres hébreux de cette époque.
487 avant J.-C.	Kahn p. 9, Singh p. 24		Les grecs emploient un dispositif appelé la " scytale " - un bâton autour duquel une bande longue et mince de cuir était enveloppée et sur laquelle on écrivait le message. Le cuir était ensuite porté comme une ceinture par le messager. Le destinataire avait un bâton identique permettant d'enrouler le cuir afin de déchiffrer le message.
Environ 150 avant J.-C.	Kahn p. 10		L'historien grec Polybe (env. 200-125 av. J.-C.) invente le carré de Polybe , dont s'inspireront plus tard bien des cryptosystèmes.
60-50 avant J.-C.	Kahn p. 11, Singh pp. 25-26		Jules César (100-44 avant J.-C.) employait une substitution simple avec l'alphabet normal (il s'agissait simplement de décaler les lettres de l'alphabet d'une quantité fixe) dans les communications du gouvernement. Ce chiffre était moins robuste qu' Atbash , mais à une époque où très peu de personnes savaient lire, cela suffisait. César écrivait aussi parfois en remplaçant les lettres latines par les lettres grecques.

5e siècle ?	Singh, pp. 24-25		Le Kama-sutra est un texte écrit au 5e siècle par le brahmane Vatsayayana, mais fondé sur des manuscrits du 4e siècle avant J.-C. Le Kama-sutra recommande que les femmes apprennent 64 arts, entre autres cuisiner, s'habiller, masser et élaborer des parfums. La liste comprend aussi des domaines moins évidents, comme la prestidigitation, les échecs, la reliure et la tapisserie. Le numéro 45 de la liste est le mlecchita-vikalpa , l'art de l'écriture secrète , qui doit leur permettre de dissimuler leurs liaisons.
855	Kahn p. 15		Abu Bakr ben Wahshiyya publie plusieurs alphabets secrets utilisés à des fins de magie, dans son livre "Kitab shauk almustaham fi ma'arifat rumuz al aklam" (Le livre de la connaissance longuement désirée des alphabets occultes enfin dévoilée).
9e siècle	Singh, pp. 33-35		Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah Oòmran ibn Ismaïl al-Kindi rédige le plus ancien texte connu décrivant la technique de décryptement appelée analyse des fréquences .

L'éveil de l'occident (1000 - 1800)







Jusque-là largement devancé par la science arabe, l'Occident développe la cryptographie et la cryptanalyse.

DATES	SOURCES	IMAGES	COMMENTAIRES
1226	Kahn p.19		À partir de 1226, une timide cryptographie politique apparaît dans les archives de Venise, où des points ou des croix remplacent les voyelles dans quelques mots épars.
Environ 1250	Kahn p. 13, Singh p. 42		Roger Bacon a non seulement décrit plusieurs chiffres, mais il a aussi écrit : "Il est fou celui qui écrit un secret de toute autre manière que celle qui le soustrait à la connaissance du vulgaire".
1379	Kahn p. 19-20		Gabriel de Lavinde compose un recueil de clefs, dont plusieurs combinent code et substitution simple. En plus d'un alphabet de chiffrement, souvent avec des nulles , on trouve un petit répertoire d'une douzaine de noms communs et de noms propres avec leurs équivalents en bigrammes . C'est le premier exemple d'un procédé qui devait prévaloir pendant 450 ans en Europe et en Amérique: le nomenclateur .
1392	Singh p. 42		Dans un ouvrage intitulé "L'équatorial des Planètes", qui décrit le fonctionnement d'un instrument astronomique, Geoffrey Chaucer , a incorporé six courts cryptogrammes écrits de sa propre main.
1412	Kahn p. 16-18		La science arabe en matière de cryptologie est exposée dans la <i>subh al-a sha</i> , une énorme encyclopédie en 14 volumes, écrite pour fournir à la bureaucratie une connaissance exhaustive de toutes les principales branches du savoir. Son auteur, qui vivait en Egypte, était Abd Allah al-Qalqashandi . La section intitulée "De la dissimulation des informations secrètes dans les lettres" comporte deux parties, l'une traitant des représentations symboliques et du langage convenu, l'autre des encres invisibles et de la cryptologie.
1466-7	Kahn pp. 20-23, Singh pp. 61-62		Leon Battista Alberti invente et publie le premier chiffre polyalphabétique . Il conçoit un cadran chiffrant pour simplifier le processus. Cette classe de chiffre n'a pas été apparemment cassée jusqu'aux années 1800. Alberti a aussi écrit largement sur l'état de l'art dans des chiffres, en plus de sa propre invention. Ces chiffres polyalphabétiques étaient beaucoup plus robustes que le nomenclateur qu'utilisaient les diplomates de l'époque. Alberti inventa aussi le surchiffrement codique. Mais le génie d'Alberti était trop en avance sur son temps et ce n'est que 400 ans plus tard, vers la fin du 19e siècle, que les principales puissances mondiales commencèrent à surchiffrer leurs codes mais par des procédés bien plus simples.

1474	Wikipedia		Un contemporain d'Alberti, Sicco Simonetta , cryptanalyste au service du Duc de Milan, écrit <i>Liber Sifrorum</i> , un traité de cryptanalyse.
1506	Kahn pp. 23-24		Le premier grand cryptanalyste européen fut peut-être Giovanni Soro , nommé secrétaire chiffreur en 1506. Il devint secrétaire du chiffre de Venise. Le Vatican lui-même testa ses chiffres sur Soro, qui les perça à jour une première fois. Le Pape envoya d'autres textes chiffrés à Soro afin de savoir si le meilleur cryptanalyste pouvait battre son chiffre. Soro renvoya les textes en écrivant qu'il n'avait pas réussi à les déchiffrer mais on ne sut jamais s'il avait dit la vérité, ou s'il avait menti pour pouvoir décrypter sans difficultés tout message émanant des autorités pontificales...
1518	Kahn pp. 26-28, Singh p. 62		Jean Trithème a écrit le premier livre imprimé sur la cryptologie. Il a inventé un chiffre stéganographique dans lequel chaque lettre est représentée par un mot. La série résultante de mots ressemble à une prière. Il a aussi décrit des chiffres polyalphabétiques sous la forme désormais standard de tables de substitution rectangulaires .
1550 env.	Kahn pp. 37-38		Jérôme Cardan invente le premier procédé autoclave , mais ce système est imparfait et c'est finalement un autre procédé qui porte son nom. La grille de Cardan consiste en une feuille de matériau rigide dans laquelle ont été découpées, à des intervalles irréguliers, des fenêtres rectangulaires de la hauteur d'une ligne d'écriture et de longueur variable. Le chiffreur écrit le texte dans les fenêtres, puis retire le cache et comble les espaces vides avec un texte anodin. Le destinataire pose la même grille sur le texte crypté pour lire le message caché.
1553	Kahn pp. 34-35		Giovan Batista Belaso fait paraître un petit livre intitulé <i>La cifra del. Sig. Giovan Batista Belaso</i> . Il y proposait, pour le chiffrement en substitution polyalphabétique, l'emploi de clefs littérales, faciles à garder en mémoire et à changer. Il les appelait "mot de passe". Les clefs littérales furent immédiatement adoptées et l'innovation de Belaso est à l'origine de certains systèmes actuels très complexes où plusieurs clefs - et non pas une seule - sont utilisées et changées de façon irrégulière.
1563	Kahn pp. 35-36		Giovanni Battista Della Porta écrit <i>De Futivis Literarum Notis</i> . Ces quatre livres, traitant respectivement des chiffres anciens, des chiffres modernes, de la cryptanalyse, des caractéristiques linguistiques qui favorisent le déchiffrement, représentent la somme des connaissances cryptologiques de l'époque. Parmi les procédés modernes, dont beaucoup sont de son inventions, apparaît la première substitution bigrammatique: deux lettres sont représentées par un seul symbole. Il inventa aussi le premier chiffre polyalphabétique . Il fut le premier à classer les deux principes cryptographiques majeurs: la substitution et la transposition.
1578			Marins , un des décrypteurs de la république de Venise, fait paraître <i>Del mondo di extrazar le cifre</i> .
1585	Kahn pp. 39-42, Singh pp. 62-67		Blaise de Vigenère écrit son <i>Traicté des chiffres ou secrètes manières d'escrire</i> . Il présente entre autres un tableau du type Trithème , que l'on dénomme aujourd'hui à tort carré de Vigenère . On considéra longtemps ce chiffre comme indécryptable, légende si tenace que même en 1917, plus de cinquante après avoir été cassé, le Vigenère était donné pour "impossible à décrypter" par la très sérieuse revue <i>Scientific American</i> .
1623	Kahn pp. 359-364		Sir Francis Bacon (que l'on soupçonne fortement d'être William Shakespeare) est l'inventeur d'un système stéganographique qu'il exposa dans <i>De dignitate et augmentis scientiarum</i> . Il appelait son alphabet bilitère , car il utilisait un arrangement des deux lettres A et B en groupes de cinq.
1691	Kahn pp. 46-50, Singh p. 71		Antoine Rossignol et son fils Bonaventure élabore le Grand Chiffre de Louis XIV. Il tomba en désuétude après la mort de ses inventeurs et ses règles précises furent rapidement perdues. Le grand Chiffre était si robuste qu'on était encore incapable de la lire à la fin du 19e siècle, jusqu'à Bazeries .

L'essor des communications (1800 - 1970)

Les nouvelles techniques de communications (moyens de transports rapides, journaux, télégraphe, télégraphie sans fil) donne une nouvelle impulsion à la cryptologie. Les guerres modernes utilisent abondamment les télécommunications; l'interception devient simple et le décryptement des informations devient vital. La cryptologie entre dans son ère industrielle.

DATES	SOURCES	IMAGES	COMMENTAIRES
Les années 1790	Kahn pp. 154-156		Thomas Jefferson , invente son cylindre chiffant , si bien conçu qu'après plus d'un siècle et demi de rapide progrès technique, il était encore utilisé. C'était sûrement le moyen de chiffrement le plus sûr de l'époque, et pourtant il fut classé et oublié. Il fut réinventé en 1891 par Etienne Bazeries, qui ne parvint pas à le faire adopter par l'armée française. L'armée américaine mit en service un système presque identique en 1922.
1854	Kahn pp. 64-68, Singh pp. 401-402		Charles Wheatstone , un des pionniers du télégraphe électrique, invente le chiffre Playfair , du nom de son ami Lyon Playfair qui a popularisé ce chiffre.
1857			Après la mort de l'amiral Sir Francis Beaufort , son frère publie le chiffre de Beaufort (une variante du chiffre de Vigenère).
1854	Singh pp. 79-93		Charles Babbage casse le chiffre de Vigenère , mais sa découverte resta ignorée, car il ne la publia pas. Ce travail ne fut mis en lumière qu'au 20e siècle, lors de recherches effectuées sur l'ensemble des papiers de Babbage.
1861	Kahn pp. 69-70, Singh p. 93		Friedrich W. Kasiski publie <i>Die Geheimschriften und die Dechiffrierkunst</i> (les chiffres et l'art du déchiffrement), qui donne la première solution générale pour le déchiffrement d'un chiffre polyalphabétique à clefs périodique, marquant ainsi la fin de plusieurs siècles d'invulnérabilité du chiffre de Vigenère.
1891	Kahn pp. 71-76, Singh pp. 72-74		Le commandant Étienne Bazeries produit son cryptographe cylindrique. Il était composé de vingt disques portant chacun vingt-cinq lettres. Il ne sera jamais employé par l'armée française. Bazeries fut aussi le premier à déchiffrer le Grand chiffre de Louis XIV.
1917	Kahn pp. 374-377		Gilbert S. Vernam , travaillant pour AT&T, a inventé une machine de chiffre polyalphabétique pratique capable d'employer une clef qui est totalement aléatoire et ne se répète jamais - un masque jetable . C'est seul le chiffre, dans nos connaissances actuelles, dont on a prouvé qu'il était indécryptable en pratique et en théorie. Ce procédé ne fut cependant jamais utilisé par l'armée car il exigeait de devoir produire des millions de clefs différentes (une par message), ce qui est impraticable. Par contre, il fut utilisé par les diplomates allemands dès 1921.




1918	Kahn pp. 140-143, Singh pp. 117-119 & pp. 403-404		Le système ADFGVX a été mis dans le service par les Allemands à la fin de la première guerre mondiale. Il a été cassé par le lieutenant français Georges Painvin .
1918	Kahn p. 379, Singh pp. 142-157	 Scherbius	Arthur Scherbius fait breveter sa machine à chiffrer Enigma . Le prix d'un exemplaire s'élevait à 20'000 livres en valeur actuelle. Ce prix sembla décourager les acheteurs potentiels. Il est à noter que trois autres inventeurs, dans trois pays, avaient, chacun de son côté et presque simultanément, eu l'idée d'une machine basée sur des rotors: Hugo Alexandre Koch , Arvid Gerhard Damm et Edouard Hugh Hebern .
1925	Newton, pp. 129-130		Boris Caesar Wilhelm Hagelin (1892-1983) propose à l'armée suédoise la machine B-21, qui fut pendant une décennie la machine la plus compacte capable d'imprimer des messages chiffrés. Pendant la seconde guerre mondiale, les Alliés fabriquèrent une autre machine de Hagelin, la Hagelin C-36 (appelée M-209 aux États-Unis), à 140 000 exemplaires. Après la guerre, Boris Hagelin créa à Zoug, en Suisse, Crypto AG , qui est aujourd'hui encore l'un des principaux fabricants d'équipements cryptographiques.
1929			Lester S. Hill publie son article "Cryptography in an Algebraic Alphabet", dans <i>American Mathematical Monthly</i> , 36 , 1929, pp. 306-312. Il y décrit le chiffre qui porte son nom . C'est un chiffre polygraphique où l'on utilise des matrices et des vecteurs.
1931	Kahn pp. 167-175		Herbert O. Yardley publie <i>The American Black Chamber</i> , un des livres les plus célèbres sur la cryptologie. Il décrypta entre autres les codes japonais (avant leur machine PURPLE).
1933-45	Kahn pp. 257-265, Singh pp. 142-207	 Turing	La machine Enigma ne fut pas un succès commercial mais elle fut reprise et améliorée pour devenir la machine cryptographique de l'Allemagne nazie. Elle a été cassée par le mathématicien polonais Marian Rejewski , qui s'est basé seulement sur un texte chiffré et une liste des clefs quotidiennes obtenues par un espion. Pendant la guerre, les messages furent régulièrement décryptés par Alan Turing , Gordon Welchman et d'autres à Bletchley Parc, en Angleterre, à l'aide des premiers ordinateurs (les fameuses bombes).
1940	Kahn pp. 175-180		William Frederick Friedman , plus tard honoré comme le père de la cryptanalyse américaine, à la tête de son équipe du Signal Intelligence Service (S.I.S.), réussit le décryptement de la machine à chiffrer japonaise PURPLE. Avec sa femme, il s'intéressa beaucoup aux chiffres shakespeareiens , et, pendant la prohibition, ils déchiffrèrent les codes des trafiquants.

La cryptologie moderne (de 1970 à nos jours)

Les ordinateurs et le réseau Internet font entrer la cryptologie dans son ère moderne. La grande invention de ces dernières décennies fut la cryptographie à clefs publiques. Le futur sera peut-être la [cryptographie quantique](#), définitivement indécryptable.

DATES	SOURCES	IMAGES	COMMENTAIRES
-------	---------	--------	--------------

1970	Singh pp. 270-272		Au début des années 1970, Horst Feistel a mené un projet de recherche à l'IBM Watson Research Lab qui a développé le chiffre Lucifer , qui inspira plus tard le chiffre DES et d'autres chiffres.
1976	Diffie, Singh pp. 274-294	 Diffie  Hellman	<p>Whitfield Diffie et Martin Hellman publient <i>New Directions in Cryptography</i>, introduisant l'idée de cryptographie à clef publique. Ils donnent une solution entièrement nouvelle au problème de l'échange de clefs. Ils avancent aussi l'idée d'authentification à l'aide d'une fonction à sens unique.</p> <p>Ils terminent leur papier avec une observation pour laquelle cette page Web donne la preuve détaillée : "L'habileté dans la cryptanalyse a toujours été lourdement du côté des professionnels, mais l'innovation, en particulier dans la conception des nouveaux types de systèmes cryptographiques, est venue principalement d'amateurs."</p>
Novembre 1976	Singh pp. 272-273		<p>DES, pour Data Encryption Standard ("standard de cryptage de données"), est un algorithme très répandu à clef privée dérivé du chiffre Lucifer de Feistel (de chez IBM) dans sa version à 64 bits. Il sert à la cryptographie et l'authentification de données. Il a été jugé si difficile à percer par le gouvernement des Etats-Unis qu'il a été adopté par le ministère de la défense des Etats-Unis qui a contrôlé depuis lors son exportation. Cet algorithme a été étudié intensivement et est devenu l'algorithme le mieux connu et le plus utilisé dans le monde à ce jour.</p> <p>Bien que DES soit très sûr, certaines entreprises préfèrent utiliser le "triple-DES", qui n'est rien d'autre que l'algorithme DES appliqué trois fois, avec trois clés privées différentes.</p>
Avril 1977	Singh pp. 295-302	 Rivest  Shamir  Adleman	<p>RSA signifie Rivest-Shamir-Adleman, en l'honneur de ses trois inventeurs : Ron Rivest, Adi Shamir et Leonard Adleman qui l'ont inventé en 1977. Le brevet de cet algorithme appartient à la société américaine RSA Data Security, qui fait maintenant partie de Security Dynamics et aux Public Key Partners, (PKP à Sunnyvale, Californie, Etats-Unis) qui possèdent les droits en général sur les algorithmes à clé publique. RSA est un algorithme à clé publique qui sert aussi bien à la cryptographie de documents, qu'à l'authentification. Grâce au fait qu'il était à clé publique, et au fait qu'il était très sûr, l'algorithme RSA est devenu un standard de facto dans le monde.</p>
1978	RSA		L'algorithme RSA est publié dans les Communications de l'ACM.
1990	IACR90		<p>Xuejia Lai et James Massey publient <i>A Proposal for a New Block Encryption Standard</i>, un algorithme de cryptage des données International (IDEA: International Data Encryption Algorithm) - pour remplacer le DES. L'IDEA emploie une clef de 128 bits et utilise des opérations convenant bien à tout type d'ordinateurs, permettant donc une programmation plus efficace. Il s'agit d'un des meilleurs algorithmes de chiffrement, si ce n'est le meilleur. Personne n'a dévoilé à ce jour avoir cassé d'une manière ou d'une autre le moindre bloc de texte chiffré par IDEA. Il est actuellement exploité par la société Mediacrypt.</p>

1990	IACR90, Singh pp. 367-378	 Bennett	Charles H. Bennett et Gilles Brassard publient leurs résultats expérimentaux sur la Cryptographie Quantique, qui emploie des photons pour communiquer un flot de bits qui serviront de clefs pour un cryptage de type Vernam (ou d'autres utilisations). En supposant que les lois de la mécanique quantique se vérifient, la Cryptographie Quantique offre non seulement le secret, mais permet aussi de savoir si la ligne a été écoutée. Comme inconvénient, la QC exige actuellement un câble en fibres optiques entre les deux correspondants.
1991	Garfinkel, Singh pp. 319-343		Phil Zimmermann sort sa première version de PGP (Pretty Good Privacy) en réponse à la menace du FBI d'exiger l'accès au message clair des citoyens. PGP offre une haute sécurité au citoyen et cela gratuitement. PGP est en effet un freeware et est devenu rapidement une norme mondiale.
1995	Cerf		Nicolas Gisin et son équipe distribuent des clefs secrètes à l'aide d'un câble optique de 25 kilomètres sous le lac Léman en codant les q-bits par la polarisation de photons (cryptographie quantique). La distance est le prochain obstacle que devront franchir les chercheurs, car le dispositif ne peut excéder 50 à 60 km, selon leurs estimations.
Août 1999	LIX		11 sites répartis dans 6 pays factorisent le premier nombre ordinaire de 155 chiffres décimaux (512 bits). Un tel nombre aurait pu servir de clef dans un système de chiffrement moderne de type RSA, qui est utilisé dans le commerce électronique. Un tel record remet en question l'utilisation de clefs trop petites dans de tels systèmes.

Sources utilisées pour ce tableau

- **Diffie**: Whitfield Diffie and Martin Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Nov 1976.
- **Cerf**: Nicolas Cerf, Nicolas Gisin, "Les promesses de l'information quantique", La Recherche 327, Janvier 2000, pp. 46-53
- **Garfinkel**: Simson Garfinkel, "PGP: Pretty Good Privacy", O'Reilly & Associates, Inc., 1995.
- **IACR90**: Proceedings, EUROCRYPT '90; Springer Verlag.
- **Kahn**: David Kahn, "La guerre des codes secrets", InterEditions, 1980.
- **Newton**: David E. Newton, "Encyclopedia of Cryptology", ABC-CLIO, 1998
- **RSA**: Rivest, Shamir and Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, Feb. 1978, pp. 120-126.
- **Singh**: Simon Singh, "Histoire des codes secrets", LC Lattès, 1999.

Références

- [CME's Cryptography Timeline](#) (by Carl Ellison)
- [Wikipédia : Histoire de la cryptologie](#)

Aller vers :



Didier Müller, 10.5.02

