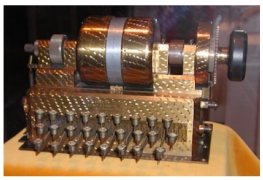
0 Cryptographie automatique

histoires d'informatique

Cryptographie automatique

la course au codage



hist-math.fr Bernard Ycart

Si je vous dis « histoire de l'informatique » et « cryptographie », vous pensez aussitôt Turing et Enigma. Oui, bien sûr, mais pas seulement.

Parmi les premiers codes secrets dont on ait gardé trace, il y a le code de César. Pas parce que Jules César l'a inventé, mais parce que Suetone dit qu'il l'utilisait.

1 Le code de César

« Il y employait, pour les choses tout à fait secrètes, une espèce de chiffre qui en rendait le sens inintelligible (les lettres étant disposées de manière à ne pouvoir jamais former un mot), et qui consistait, je le dis pour ceux qui voudront les déchiffrer, à changer le rang des lettres dans l'alphabet, en écrivant la quatrième pour la première, c'est-à-dire le D pour le A, et ainsi de suite. »

Le code de César
Suetone, La vie des douze Césars (ca. 100)

Il y employait, pour les choses tout à fait secrètes, une espèce de chiffre qui en rendait le sens inintelligible (les lettres étant disposées de manière à ne pouvoir jamais former un mot), et qui consistait, je le dis pour ceux qui voudront les déchiffrer, à changer le rang des lettres dans l'alphabet, en écrivant la quatrième pour la première, c'est-à-dire le D pour le A, et ainsi de suite.

Bon ; on peut choisir un autre nombre que quatre, ou tant qu'on y est définir une autre permutation des lettres. Ou pourquoi pas, faire correspondre chaque lettre avec un signe cabalistique quelconque. L'important est qu'on remplace une lettre donnée, toujours par le même signe. C'est une bijection : on parle de « substitution simple ». Il se trouve qu'un tel code est relativement facile à décoder, avec un minimum de statistique.

C'est al-Kindi qui le dit, au neuvième siècle, à Bagdad. Il a dirigé la maison de la sagesse, sous le calife al-Mamun. Il a écrit près de trois cents ouvrages, dont le premier traité de cryptologie, qui est aussi le premier ouvrage connu où il est question de statistique.

2 Analyse de fréquence

« La façon d'élucider un message crypté, si nous savons dans quelle langue il est écrit, est de nous procurer un autre texte en clair dans la même langue, de la longueur d'un feuillet environ, et de compter alors les apparitions de chaque lettre. Ensuite, nous nous reportons au texte chiffré que nous voulons éclaircir et relevons de même ses symboles. Nous remplaçons le symbole le plus fréquent par la lettre première (la plus fréquente du texte clair), le suivant par la deuxième, le suivant par la troisième, et ainsi de suite jusqu'à ce que nous soyons venus à bout de tous les symboles du cryptogramme à résoudre. »

Analyse de fréquence
Al-Kindī (ca. 800–880)

La façon d'élucider un message crypté, si nous savons dans quelle langue il est écrit, est de nous procurer un autre texte en clair dans la même langue, de la longueur d'un feuillet environ, et de compter alors les apparitions de chaque lettre. Ensuite, nous nous reportons au texte chiffré que nous voulons éclaircir et relevons de même ses symboles. Nous remplaçons le symbole le plus fréquent par la lettre première (la plus fréquente du texte clair), le suivant par la deuxième, le suivant par la troisième, et ainsi de suite jusqu'à ce que nous soyons venus à bout de tous les symboles du cryptogramme à résoudre.

Difficile de le dire plus clairement. L'analyse des fréquences de symboles est la première des choses à essayer quand on veut déchiffrer un message.

3 Sur le déchiffrement des messages cryptographiques

Évidemment, al-Kindi a réfléchi à la parade. Il y en a de multiples, et il les énumère longuement, ce qui donne la classification arborescente que vous voyez ici.

On ne va peut-être pas chercher à rentrer dans les détails de la classification d'al-Kindi. D'autant que la méthode qui nous intéresse surtout est la méthode de substitution multiple. Au lieu d'une seule bijection entre l'alphabet du texte en clair et le message chiffré, il y en aura plusieurs, qui se succèderont au fil du texte.

Sur le déchiffrement des messages cryptographiques
Al Kindī (ca. 800–880)

4 Blaise de Vigenère (1523–1596)

En Occident, le premier à décrire un tel code n'est pas Blaise de Vigenère. Mais comme souvent, on va prendre pour prétexte un livre en particulier pour donner son nom à ce qui était connu avant lui.

Blaise de Vigenère (1523–1596)

5 Traicté des chiffres ou secretes manieres d'escrire (1587)

Le livre, c'est celui-ci : le Traité des chiffres ou secrètes manières d'écrire. D'autres ont dit à peu près la même chose avant : Bellaso en Italie, Trithemius en Allemagne. Vigenère ne prétend pas être le premier. Mais tant pis : ce sera le « code de Vigenère ».

Traicté des chiffres ou secretes manieres d'escrire (1587)
Blaise de Vigenère (1523–1596)

TRAICTE'
DES CHIFFRES,
OV SECRETES
MANIERES
D'ESCRIRE.
PAR
BLAISE DE VIGENERE,
BOVRBONNOIS.

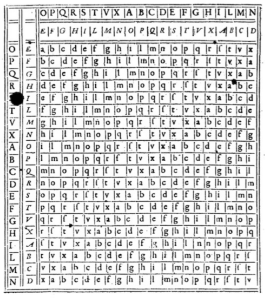
A PARIS,
Chez ABEL L'ANGELIER, au premier pilier de la grand'Salle du Palais.
M. D. LXXXVII.
AVEC PRIVILEGE DV ROY.

6 code de Vigenère

Voici de quoi il s'agit. Vigenère donne ce tableau. La première colonne à gauche est la colonne des clés. Chaque ligne contient une permutation de l'alphabet. Le chiffreur et le destinataire conviennent d'une phrase qui sert de clé. Cette phrase détermine quels alphabets utiliser. Disons que la clé est le mot Vigenère. Pour chiffrer la première lettre du message, on lit la ligne du V, puis la ligne du I pour la seconde lettre, puis la ligne du G pour la troisième, etc. Quand les lettres de la clé sont épuisées, on recommence.

On conçoit que ce soit plus difficile à déchiffrer qu'une substitution simple si on ne connaît pas la clé. Mais comment coder et décoder en un temps raisonnable ? Et comment éviter les erreurs de transcription ?

code de Vigenère
Vigenère, Traicté des chiffres ou secretes manieres d'escrire (1587)



7 Charles Wheatstone (1802–1875)

Charles Wheatstone est resté dans l'histoire des sciences pour un dispositif à mesurer les résistances électriques, le pont de Wheatstone. C'était un ami de Babbage et d'Ada Lovelace, et il est possible que ce soit lui qui ait engagé Ada Lovelace à traduire l'article de Menabrea. C'est vous dire le rôle clé qu'il a joué dans la naissance de l'informatique.

Bref. C'était un amateur de cryptogrammes, et comme beaucoup d'amateurs, il avait proposé son propre code. Mais il était également conscient du problème pratique.

Charles Wheatstone (1802–1875)

8 by means of an instrument

« On désire un chiffre qui soit à la fois parfaitement sûr et facile d'application. Et ces deux avantages combinés peuvent être obtenus seulement au moyen d'un instrument, dans lequel toute la complexité nécessaire pour assurer la sécurité s'effectue par la mécanique, tandis que sa manipulation est soumise aux règles les plus simples. Un tel instrument est maintenant offert au public. »

by means of an instrument
Charles Wheatstone (1802–1875)

A cipher which at the same time should be perfectly secure and easy in its application is a desideratum; and these combined advantages can only be obtained by means of an instrument in which all the complexity necessary to ensure security shall be effected by mechanical arrangements, whilst its manipulation shall be subjected to the simplest rules. Such an instrument is now offered to the public.

9 Wheatstone cryptograph (1848)

Cet instrument offert au public, le voici. Deux cercles concentriques, avec deux aiguilles comme les aiguilles d'une montre. Mais elles ont des mouvements décalés. L'une avance de 27 cases quand l'autre avance de 26. De sorte que les changements d'alphabet se font automatiquement à chaque nouvelle lettre codée.

Wheatstone cryptograph (1848)
Charles Wheatstone (1802–1875)

10 Charles Babbage (1791–1871)

Et le copain de Wheatstone, Babbage, qu'en pensait-il ? Lui aussi était un grand amateur de messages secrets, et il pratiquait depuis l'enfance. Voici ce qu'il raconte, dans ses mémoires.

Charles Babbage (1791–1871)

11 one the most fascinating of arts

« Déchiffrer est, selon moi une des activités les plus fascinantes, et je crains d'y avoir perdu beaucoup plus de temps qu'elle n'en mérite.

Il y a une maxime parmi les déchiffreurs, selon laquelle tous les chiffres peuvent être déchiffrés. »

Mais pourtant...

« Une des caractéristiques les plus singulières de l'art du déchiffrage est la forte conviction que chaque personne possède, même si elle n'est que modérément spécialiste, qu'elle est capable de construire un chiffre que personne ne peut déchiffrer. »

Il explique qu'il en était lui même persuadé étant jeune. Jusqu'à ce qu'il imagine un code, qui convainque tous ses amis. Pourtant, rien que d'expliquer son code, il avait déjà entrevu un angle d'attaque. Alors il demande à son ami, Fitton, de coder un message selon la règle qu'il avait inventée. Babbage raconte la suite.

one the most fascinating of arts
Babbage, Passages from the life of a philosopher (1864)

Deciphering is, in my opinion, one of the most fascinating of arts, and I fear I have wasted upon it more time than it deserves.

[...]

There is a kind of maxim amongst the craft of decipherers [...], that every cipher can be deciphered.

[...]

One of the most singular characteristics of the art of deciphering is the strong conviction possessed by every person, even moderately acquainted with it, that he is able to construct a cipher which nobody else can decipher.

12 it was not written according to the law

« Le soir suivant, de retour d'une réception, je trouvai le message de Fitton sur mon bureau. Je commençai immédiatement mes tentatives. Au bout de quelque temps, je trouvai qu'il ne cédait pas à mes attaques ; et en y regardant de plus près, je réussis à prouver qu'il n'avait pas été réalisé avec la méhode convenue. »

Babbage explique à Fitton ce qu'il a trouvé, Fitton vérifie, et effectivement, il y avait une erreur de transcription.

Voici quel était le chiffrage imaginé par Babbage.

it was not written according to the law
Babbage, Passages from the life of a philosopher (1864)

The next night, on my return from a party, I found Dr. Fitton's cipher on my table. I immediately commenced my attemps. After some time I found that it would not yield to my means of treating it ; and on further examination I succeeded in proving that it was not written according to the law agreed upon.

13 Two concentric circles of cardboard

« Le chiffre était arrangé selon le principe suivant. Deux cercles concentriques de carton étaient formés, chacun divisé en vingt-six cases ou plus.

Sur le cercle extérieur, les lettres dans l'ordre alphabétique. Sur le cercle intérieur, les mêmes 26 lettres, mais dans un ordre différent.

Chercher la première lettre à coder sur le cercle extérieur, puis lire la lettre correspondante sur le cercle intérieur. Maintenant, tourner le cercle intérieur jusqu'à ce que la lettre qui vient d'être écrite soit en face du A sur le cercle extérieur. Puis recommencer pour chaque lettre. »

Le code imaginé par Babbage, et qu'il avait lui-même craqué était donc une sorte de code de Vigenère, mais où la clé indiquant la substitution suivante était la lettre qui venait d'être écrite. Pourquoi pas !

L'utilisation de deux cercles de carton mobiles, était décidément plus pratique que le tableau carré de Vigenère. Mais l'idée était-elle nouvelle ?

Two concentric circles of cardboard
Babbage, Passages from the life of a philosopher (1864)

This cipher was arranged upon the following principle. Two concentric circles of cardboard were formed, each divided into twenty-six or more divisions.
On the outer were written in regular order the letters of the alphabet. On the inner circle were written the same twenty-six letters, but in any irregular manner.
In order to use this cipher, look for the first letter of the word to be ciphered on the outside circle. Opposite to it, on the inner circle, will be another letter, which is to be written as the cipher for the former.
Now turn the inner circle until the cipher just written is opposite the letter *a* on the *outer* circle. Proceed in the same manner for the next, and so on for all succeeding letters.

14 Leon Battista Alberti (1404–1472)

Eh bien non : elle remonte à cet homme, Leon Battista Alberti, qui a vécu plus d'un siècle avant Vigenère. C'est un de ces savants de la Renaissance italienne, d'une culture encyclopédique. Il a écrit sur beaucoup de sujets, des mathématiques à la poésie, en passant par la peinture et l'architecture.

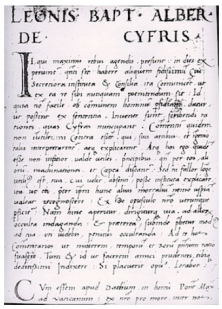
Leon Battista Alberti (1404–1472)

15 De cyfris (ca. 1467)

Il est aussi l'auteur de ce manuscrit, « De cyfris », Sur les chiffres. C'est le premier document occidental connu sur la cryptographie. Sept siècles après al-Kindi tout de même, mais il n'y a aucune indication qu'Alberti ait pu avoir conscience des nombreux traités arabes de cryptographie.

Il y explique, comme al-Kindi, que la méthode de substitution est vulnérable à l'analyse de fréquence, puis il propose sa solution.

De cyfris (ca. 1467)
Alberti (1404–1472)



16 Disque d'Alberti (ca. 1467)

Sa solution la voici. Comme Babbage, deux cercles concentriques. Sur le cercle extérieur, l'ordre alphabétique. Sur le cercle intérieur, un ordre différent. Mais il y a chez Alberti quatre cases particulières numérotées de 1 à 4, vous les voyez en haut à gauche. Elles servent de clé. Alberti explique qu'il faut convenir avec le destinataire d'une manière d'indiquer au fil du texte quelle est la lettre qui est en face de quel chiffre. Cela donne la position relative des deux cercles, et donc la substitution courante. On doit changer cette substitution assez souvent, en tournant les deux cercles l'un par rapport à l'autre.

Disque d'Alberti (ca. 1467)
Alberti (1404–1472)

17 Nicolas Bion (1652–1733)

Des cercles concentriques pour réaliser les codages par substitution, simple ou multiple, il y en a eu après Alberti dans tous les pays et sous tous les régimes. D'ailleurs, on peut encore en acheter de nos jours.

Voici l'appareil à chiffrer fabriqué par Nicolas Bion. Il est l'ingénieur du roi pour les instruments de mathématiques. Sauf que le roi, c'est Louis XIV, et que ses services de diplomatie n'utilisent pas les codes alphabétiques. Ils utilisent un code de substitution certes, mais sur un ensemble de syllabes et de mots, associés à des nombres jusqu'à 3 chiffres. En tout environ 600 codes différents.

Nicolas Bion (1652–1733)
Ingénieur du Roy pour les instruments de mathématiques

18 American civil war (1861–1865)

American civil war (1861–1865)
confederate army

Voici les cercles de chiffrage utilisés pendant la guerre de sécession par l'armée sudiste.

19 Première guerre mondiale (1914-1918)

Première guerre mondiale (1914-1918)
US army

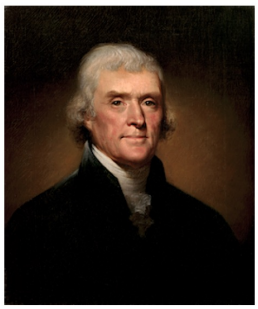
Et voici des cercles imprimés, à l'usage de l'armée américaine pendant la première guerre mondiale.

20 Thomas Jefferson (1743-1828)

Thomas Jefferson (1743-1828)

Il n'y avait donc pas mieux que les cercles concentriques et les codes de substitution ? Si, grâce à cet homme, Thomas Jefferson. L'un des sept pères fondateurs des États-Unis d'Amérique, avec Benjamin Franklin et Georges Washington. L'un des rédacteurs de la déclaration d'indépendance, et le troisième président des États-Unis. Bref pas un plaisantin.

Mais tout de même, quelqu'un qui savait vivre :



21 Le vin de Montrachet

« Je vous en prie de vouloir bien me procurer une douzaine de ceps des vignes dont on fait le vin de Monrachet, et autant de celles du vin de Vougeau, ou de Chambertin. Vous aurez bien le soin de les faire tirer de ces vignobles vous-même afin d'éviter toute possibilité de manquer des véritables espèces. »

C'est signé :

« Votre très humble et très obéissant serviteur, Thomas Jefferson. »

En français dans le texte : Thomas Jefferson a été ambassadeur des États-Unis en France de 1785 à 1789, et comme vous le voyez il n'y a pas perdu son temps. Il est aussi celui qui a acheté, sans trop l'avoir prévu, la Louisiane à Napoléon en 1803. Un territoire grand comme plusieurs fois la France pour une bouchée de pain. Euh en même temps, la France ne la possédait pas vraiment, la Louisiane. Elle venait d'en acheter la plus grande partie aux Espagnols, qui ne la possédaient pas plus avant. Mais bon, je m'égare.

Le vin de Montrachet
Thomas Jefferson (1787)

Je vous en prie de vouloir bien me procurer une douzaine de ceps des vignes dont on fait le vin de Montrachet, et autant de celles du vin de Vougeau, ou de Chambertin. Vous aurez bien le soin de les faire tirer de ces vignobles vous-même afin d'éviter toute possibilité de manquer des véritables espèces.

[...]

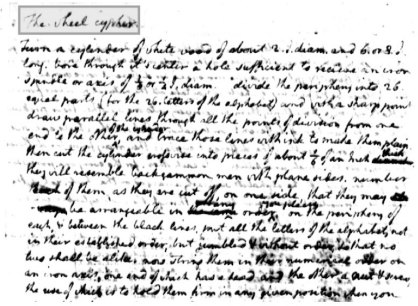
Votre très humble et très obéissant serviteur, Thomas Jefferson.

22 The wheel cypher (1793)

Jefferson donc. De retour de son ambassade en France, qui est en pleine Révolution, il devient le premier secrétaire d'état, sous Georges Washington, le premier président des États-Unis. Et il s'inquiète un peu de la confidentialité de ses dépêches.

Alors il a une idée, qu'il explique dans ce manuscrit, de manière tellement précise d'ailleurs qu'il suffit de suivre ses indications pour fabriquer ceci.

The wheel cypher (1793)
Thomas Jefferson (1743-1828)

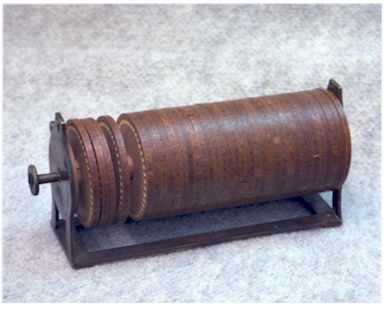

The wheel cypher

23 The wheel cypher (1793)

C'est un cylindre de bois, blanc précise-t-il, sur lequel on a marqué des lignes et inscrit des lettres, avant de le découper en rondelles. Si on a choisi un ordre dans lequel placer les rondelles, il suffit de les tourner de sorte à faire apparaître le message en clair, et on lit la traduction chiffrée sur une autre ligne.

C'est simple, mais il fallait y penser. Eh bien, ça n'a pas marché. Jefferson lui-même n'y a pas cru et n'a rien fait pour l'imposer.

The wheel cylinder (1793)
Thomas Jefferson (1743-1828)



24 M-94 (1917)

Dommage, parce que le système a été réinventé plusieurs fois, dont en 1917, plus d'un siècle après Jefferson, pour donner cet appareil, le M-94, en usage dans l'armée américaine à la fin de la première guerre mondiale.

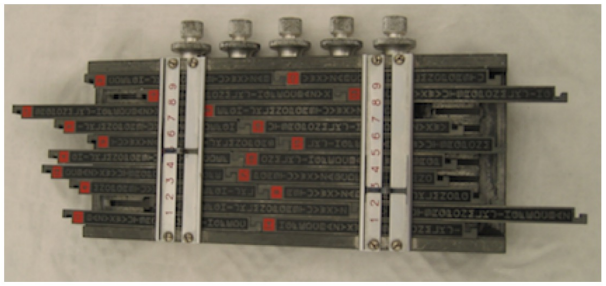
M-94 (1917)
US Army

25 Transpositeur à permutations secrètes (Sphinx, 1925)

Le même principe a aussi été mis sous forme d'un tableau de réglettes qui peuvent coulisser les unes par rapport aux autres ; La clé, c'est la permutation des réglettes, qui correspond à l'ordre des rondelles dans le cylindre de Jefferson.

La machine que vous voyez était fabriquée en France dans les années trente par la Société des Codes Télégraphiques Georges Lugagne.

Transpositeur à permutations secrètes (Sphinx, 1925)
Société des Codes Télégraphiques Georges Lugagne



26 Gottfried Wilhelm Leibniz (1646–1716)

Tous ces dispositifs de codages portatifs, c'est peut-être commode sur un champ de bataille, mais ça fait un peu bricolage. On ne pourrait pas trouver mieux ? Eh bien si, évidemment : quand il s'agit d'inventer une machine, il suffit de demander à Leibniz.

À force de réfléchir à sa machine arithmétique, il avait eu une idée géniale.

Gottfried Wilhelm Leibniz (1646–1716)

27 Machina Deciphratoria (1679)

« Cette machine arithmétique m'a amené à penser à une autre belle machine qui servirait à chiffrer et déchiffrer des missives, et à le faire d'une manière très rapide et indéchiffrable pour d'autres. Car j'ai observé que les codes utilisés communément sont aisés à déchiffrer, et ceux qui sont difficiles à déchiffrer sont généralement si difficiles à utiliser que les gens trop occupés les abandonnent. Mais avec cette machine une lettre entière est presque aussi facile à chiffrer et déchiffrer pour quelqu'un qui l'utilise, qu'elle le serait pour la recopier. »

Que nous a-t-il encore concocté ? L'idée est assez simple, le chiffrage ressemble aux cercles d'Alberti, puisqu'il s'agit de changer de substitution à chaque lettre, selon une clé convenue. Mais il a tout automatisé. Il suffit de taper les lettres sur un clavier et leur version chiffrée apparaît automatiquement.

Machina Deciphratoria (1679)
Gottfried Wilhelm Leibniz (1646–1716)

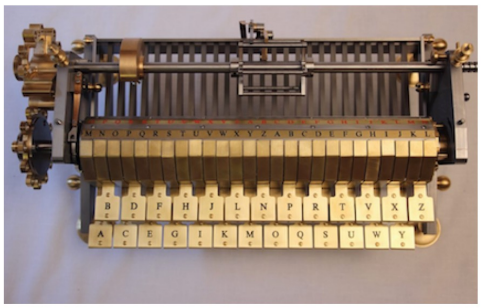
Cette machine arithmétique m'a amené à penser à une autre belle machine qui servirait à chiffrer et déchiffrer des missives, et à le faire d'une manière très rapide et indéchiffrable pour d'autres. Car j'ai observé que les codes utilisés communément sont aisés à déchiffrer, et ceux qui sont difficiles à déchiffrer sont généralement si difficiles à utiliser que les gens trop occupés les abandonnent. Mais avec cette machine une lettre entière est presque aussi facile à chiffrer et déchiffrer pour quelqu'un qui l'utilise, qu'elle le serait pour la recopier.

28 Machina Deciphratoria (reconstitution)

La machine de Leibniz a été reconstituée, mais seulement récemment. Elle n'avait jamais été construite auparavant.

Il était persuadé qu'avec cette invention géniale, le duc de Hanovre allait multiplier ses subventions et équiper tous les services diplomatiques. Eh bien non, pas du tout, c'est un flop. Alors, comme il ne voulait pas que son idée profite à l'ennemi, il a gardé ses plans secrets.

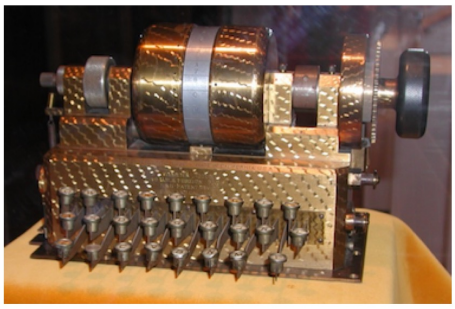
Machina Deciphratoria (reconstitution)
Gottfried Wilhelm Leibniz (1646–1716)



29 Machine de Hebern (1917)

L'idée d'automatiser un codage par substitution multiples va exploser à la fin de la première guerre mondiale. On ne compte plus les inventions, et aussi les piratages. Les premiers inventeurs pourraient bien avoir été hollandais, mais pour une raison inconnue leur dépôt de brevet n'a pas abouti. Le premier brevet est celui de Hebern, aux États-Unis, qui n'aura pas le succès commercial espéré.

Machine de Hebern (1917)
Edward Hugh Hebern 1869–1952



30 Machine Enigma (1919)

Machine Enigma (1919)
Artur Scherbius 1878–1929

Peu après arrive Scherbius en Allemagne, qui produit la première version d'Enigma.

Vous voyez trois roues dentées sur le dessus de celle-ci.

31 Rotor électro-mécanique

Ce sont trois rotors. Le principe de ces rotors est de réaliser une permutation cablée des lettres, et de tourner les uns par rapport aux autres pour composer ces permutations entre elles à chaque nouvelle lettre. Le codage de deux lettres consécutives est donc le résultat de deux substitutions différentes.

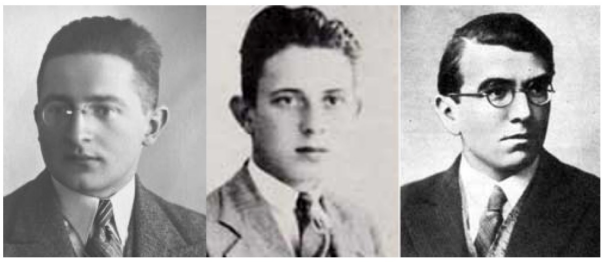
Rotor électro-mécanique

Évidemment, il faut une clé qui est la convention initiale de position des rotors. C'est comme pour les cercles d'Alberti, sauf que les permutations sont ici beaucoup plus compliquées, car le câblage des rotors est a priori inconnu.

Les machines de Scherbius sont en vente libre, et les services secrets des pays étrangers ne se sont pas privés d'en acheter. Sauf que les messages allemands que l'on intercepte à partir de 1927 changent d'aspect. Manifestement, ils ont été codés avec un appareil ressemblant à l'Enigma du commerce, mais en plus compliqué. Les Français et les Anglais ont bien intercepté des messages militaires allemands en quantité, ils ont bien leurs versions commerciales d'Enigma, mais ils ne savent rien en faire.

32 Biuro Szyfrów (1931–1939)

Biuro Szyfrów (1931–1939)
Marian Rejewski, Jerzy Różycki, Henrik Zygalski



Les Polonais, en 1930, en sont au même point. Mais ils prennent une initiative. Il y a en Pologne une école de mathématiciens de tout premier plan. Alors ils décident de donner des bases de cryptographie à quelques étudiants, puis de les recruter dans un « bureau du chiffre ». Parmi ces mathématiciens il y a ces trois hommes, Marian Rejewski, Jerzy Różycki et Henrik Zygalski.

Un officier français, le colonel Gustave Bertrand, leur avait fourni des renseignements venant d'un agent double allemand. En partie grâce à ces renseignements, ils réussissent à reconstituer le câblage des rotors de la version militaire d'Enigma. Et dès 1938, il sont capables de décoder les messages allemands.

33 Bomba kryptologiczna (1938)

L'avancée décisive est due à Marian Rejewski. Il a l'idée de fabriquer des rotors virtuels qu'il fait tourner en parallèle, de manière à explorer toutes les possibilités de câblage.

Comme sa machine fait tic, tic, tic, il l'appelle : la « bombe cryptologique ». Et ça marche ! Le bureau du chiffre polonais est capable de fabriquer des exemplaires reconstitués de la machine allemande, et d'en donner le mode d'emploi.

Comprenant parfaitement ce qui va arriver, les Polonais collaborent avec leurs alliés. Le 25 juillet 1939, soit à peine plus d'un mois avant l'invasion de la Pologne et le début de la guerre, une réunion a lieu à Varsovie, entre le bureau du chiffre polonais, et des membres des services secrets français et anglais. Les Polonais offrent à chacun un exemplaire de la machine Enigma reconstituée et son mode d'emploi. Les autres restent un peu secs : ils n'ont pas grand chose d'autre à dire que « merci ! ».

Bomba kryptologiczna (1938)
Marian Rejewski (1905–1980)

34 The Imitation Game (2015)

Le reste de l'histoire, vous le connaissez. Vous avez vu le film, The Imitation Game. Sinon, allez-y : c'est un très bon film, qui vaut vraiment la peine d'être vu.

Sauf qu'il n'y est aucunement question de Polonais.

The Imitation Game (2015)
Morten Tyldum

35 Alan Mathison Turing (1912–1954)

Le scénario est écrit pour glorifier l'action de Turing, qui le mérite amplement.

Après l'invasion de la Pologne, les mathématiciens du bureau du chiffre se sont réfugiés d'abord en France, où ils ont continué à travailler sur Enigma. Turing, qui n'était pas à la réunion de Varsovie, était venu discuter avec eux en France. Après novembre 42, Rejewski et Zygalski sont passés en Angleterre ; ils ont continué à travailler au service de cryptographie, mais pas directement avec Turing à Bletchley Park.

Alan Mathison Turing (1912–1954)

36 Alastair Denniston (1881–1961)

Le gradé administratif obtus et borné, qui met des bâtons dans les roues de Turing au début du film, c'est lui, Alastair Denniston. Il n'était ni obtus ni borné, et il a rendu d'immenses services.

Alastair Denniston (1881–1961)

37 Joan Murray (1917–1996)

Quant à la fille qui est embauchée bien qu'elle arrive en retard au test (mais comme elle est jolie on lui pardonne), c'est elle, Joan Murray. C'était une excellente mathématicienne, et sa contribution est allé beaucoup plus loin que mettre son héros en valeur.

Joan Murray (1917–1996)

38 Cambridge five

Ce qui n'apparaît pas non plus clairement dans le film, c'est le climat de paranoïa, en 1951, en pleine guerre froide, quand a éclaté l'affaire des « Cambridge five ». Ces cinq hommes étaient tous assez haut placés dans l'administration. Certains avaient même des postes de responsabilité dans les services secrets. Et ils transmettaient des informations aux Russes.

Le réseau d'espionnage avait démarré à Cambridge, où Turing avait étudié. Il y avait une relation homosexuelle entre deux des espions. Il n'en fallait pas plus pour que Turing soit assimilé aux « bad guys » dans l'hystérie collective.

Cambridge Five (1917–1996)
Philby, Burgess, Maclean, Blunt, Cairncross

39 Bombe rebuild project

Reste que l'essentiel du message de ce film est vrai : la victoire des alliés dans la seconde guerre mondiale doit beaucoup à tous ceux qui ont travaillé à Bletchley Park, et en premier lieu à Turing.

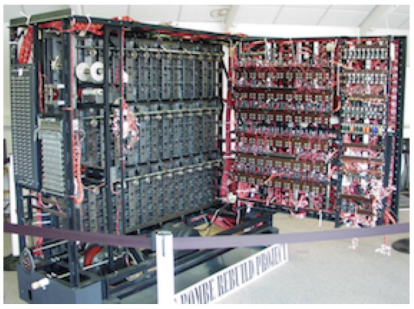
Les Polonais avaient montré la voie, et d'ailleurs Turing a continué à appeler « bombe » la machine à rotors qu'il a conçue et fait réaliser. Mais c'était sur une toute autre échelle.

Les Allemands, méfiants, avaient compliqué leur machine dans des versions successives qui devenaient beaucoup plus difficiles à décoder par l'approche polonaise. C'était vrai tout particulièrement pour les machines utilisées par la Kriegsmarine, dans les sous-marins. Elles avaient quatre rotors successifs au lieu de trois. Or décoder les messages des sous-marins était stratégiquement crucial.

Les sous-marins allemands patrouillaient en permanence dans l'Atlantique. Dès que l'un d'eux repérait un convoi, il prévenait les plus proches pour attaquer ensemble. Ils appelaient ça la tactique de la « meute de loups ». C'était terriblement efficace. Si les pertes de convois dans l'Atlantique avaient continué au niveau de 1942, l'approvisionnement de la Grande-Bretagne par les États-Unis aurait été compromis. L'apport de matériel et de troupes nécessaire au débarquement aurait été impossible, le débarquement lui-même n'aurait pas pu avoir lieu.

Dire que le décodage des messages de sous-marins à Bletchley Park a raccourci la guerre et épargné des centaines de milliers, peut-être des millions de vies, ce n'est pas une exagération.

Bombe rebuild project



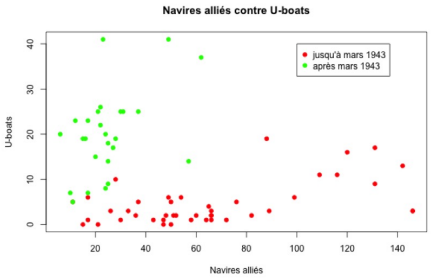
40 La victoire de Bletchley Park

Pour expliquer que la reconnaissance de l'action de Turing ait été aussi tardive, on a invoqué le fait que les archives de Bletchley Park avaient été classifiées : on ne pouvait pas savoir ce que Turing avait fait, parce que c'était « top secret ». Ce qu'il avait fait précisément, peut-être pas. Mais pour le résultat, il suffisait de compiler quelques chiffres.

Sur ce graphique, j'ai reporté un point pour chaque mois de la guerre. En abscisse, le nombre de navires alliés coulés dans l'Atlantique. En ordonnée, le nombre de sous-marins allemands coulés. Les mois jusqu'à mars 1943 sont les points rouges, les mois à partir d'avril 1943 sont en vert. Je crois que le graphique se passe de commentaires.

En décembre 1942, Turing est allé aux États-Unis. Il a expliqué ses besoins, la fabrication de bombes a été exécutée à grande échelle, la communication entre les bombes américaines et Bletchley Park a été mise en place. Turing est revenu en Angleterre pour coordonner le tout, et vous voyez le résultat.

La victoire de Bletchley Park
printemps 1943

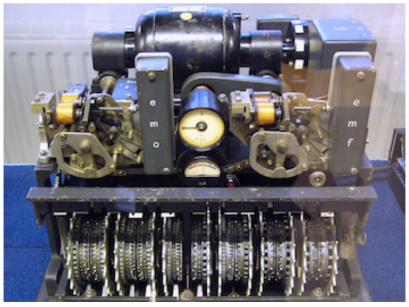


41 Lorenz SZ42

Au jour du débarquement en Normandie, le 6 juin 44, la guerre était loin d'être gagnée. Depuis plus de deux ans, les Allemands avaient commencé à coder leurs messages par radio-télégraphe entre les quartiers-généraux et les groupes d'armée, sur une machine encore plus compliquée qu'Enigma. Les Anglais, qui ne l'avaient jamais vue, l'avaient baptisé Tunny.

Cette fois-ci l'approche combinatoire des bombes ne suffisait plus. Une approche statistique avait été imaginée, mais elle demandait une masse de calculs qui n'était réalisable que par une machine. Cette machine, construite en quelques mois, a été le premier calculateur binaire électronique : Colossus de son petit nom.

Lorenz SZ42
Tunny and the Colossus



42 D-day, 6 juin 1944

En mars 1944, un ordre était arrivé à Bletchley Park : le décodage de Tunny devrait être opérationnel le premier juin. Ce jour-là, Colossus était prêt.

Le 5 juin, Eisenhower lisait un message secret de Hitler à Rommel confirmant qu'il ne croyait pas que le gros du débarquement aurait lieu en Normandie. Le premier message important décodé grâce à Colossus.

D-day 6 juin 1944
Dwight D. Eisenhower

43 références

Turing n'était pas seul à Bletchley Park. Des centaines de personnes, dont une majorité de femmes, y ont travaillé. Tous et toutes ont contribué au résultat.

Mais qu'on ne me dise pas qu'on ignorait ce qu'ils avaient fait : les nombres de vaisseaux coulés dans l'Atlantique, ils n'ont jamais été cryptés que je sache !

références

- J. Holden (2017) *The mathematics of secrets ; cryptography from Caesar ciphers to digital encryption*, Princeton University Press
- B. J. Copeland ed. (2006) *Colossus ; the secrets of Bletchley Park's codebreaking computers*, New York : Morton
- M. Rejewski (1981) How Polish mathematicians deciphered the Enigma, *IEEE Annals of the History of Computing*, 3(3), 213–234
- N. Rescher (2014) Leibniz's *Machina Deciphratoria* : a seventh-century proto-Enigma, *Cryptologia*, 38(2), 103–115
- C. Teuscher (ed.) (2004) *Alan Turing : life and legacy of a great thinker*, New York : Springer