4. Les machines à chiffrer

Les opérations de chiffrement et de déchiffrement sont considérées à juste titre comme particulièrement fastidieuses, ce qui a conduit à concevoir des machines à cryptographier pour rendre l'opération plus aisée et exempte d'erreur.

Les machines manuelles

Le cadran chiffrant est constitué d'un bouton moleté qui permet de faire tourner l'alphabet mobile autour d'un axe. La rotation régulière du cadran mobile permet de faire varier la correspondance des alphabets.

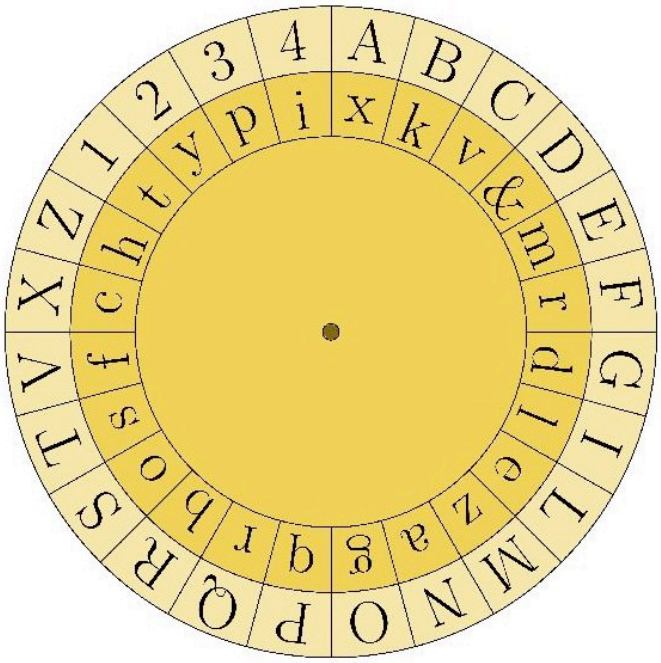
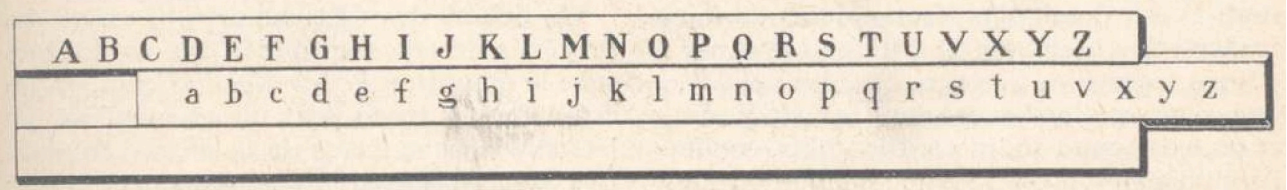


Fig. 1.7 Le cadran d'Alberti est constitué d'un cadran fixe et d'un cadran mobile. Les lettres du cadran fixe sont écrites en majuscule et représentent les lettres du texte clair. Les lettres du cadran mobile sont écrites en minuscule et représentent les lettres du cryptogramme.

La réglette coulissante de Saint-Cyr doit son nom à l'académie militaire française qui porte ce nom. Elle était en usage entre 1880 et le début du vingtième siècle.



RÉGLETTE DITE DE SAINT-CYR ET SON COULISSEAU (AU CENTRE)

En promenant, suivant une loi convenue, l'alphabet du coulisseau devant l'alphabet de la règle, on obtient des correspondances différentes entre les lettres du texte clair (majuscules) et celles qui les représentent dans le cryptogramme, ou message chiffré.

© http://www.cite-sciences.fr/csmedia/storage/PM_Document/sv1923,0.pdf

Le futur président des États-Unis d'Amérique Thomas Jefferson (1743-1826) a mis au point un dispositif appelé le *Wheel Cipher*, constitué de 26 disques sur la tranche desquels sont inscrits des alphabets désordonnés. Pour chiffrer un message, on fait tourner les roues de manière à faire apparaître le message. Le cryptogramme est constitué de l'une quelconque des séquences des autres lettres. Pour déchiffrer, il suffit de disposer du même cylindre constitué des mêmes 26 disques, d'aligner le cryptogramme et de lire ailleurs le seul texte qui semble avoir un sens. On peut changer de clé en changeant l'ordre des cylindres.

http://ciphermachines.com/photos/index.php/M-94/M-94-Cipher-Device/P1020375-1653469878

Les machines électromécaniques

Le chiffrement polyalphabétique ne sera vraiment utilisé qu'au début du vingtième siècle avec l'apparition des machines électromécaniques à rotor. Elles ont été présentées presque simultanément par quatre inventeurs de pays différents: l'américain Edward Hugh Hebern, le hollandais Hugo Alexander Koch, le suédois Arvid Damm et l'allemand Arthur Scherbius. Ce dernier est l'inventeur de la fameuse machine ENIGMA qui sera adoptée et améliorée par l'armée allemande à partir de 1928.

Le mode d'emploi de la machine ENIGMA est particulièrement simple : l'opérateur actionne une

touche sur un clavier alphabétique et une lampe indique quelle est la lettre à substituer dans le cryptogramme. L'utilisation pour le déchiffrement est similaire.

Illustration 1: Soldats allemands utilisant une machine Enigma pendant la seconde guerre mondiale (http://www.franceculture.fr/emission-concordance-des-temps-sesame-ouvre-toi-des-codes-depuis-toujours-2013-02-09)

Fig. 1.11 La machine Enigma : cette vue ouverte de la machine Enigma fait apparaître les trois rotors ainsi que les lampes qui indiquent la lettre qui se substitue à celle qui est actionnée sur le clavier.

Le cœur de ces machines est constitué d'une série de rotors qui sont des cylindres rotatifs sur la tranche desquels sont placés 26 contacts représentant chacun une lettre de l'alphabet. Un rotor réalise une permutation entre les contacts de chaque bord. Plusieurs rotors sont mis en série pour multiplier les permutations ainsi composées. Chaque lettre provoque la rotation des rotors, ce qui change la permutation opérée.

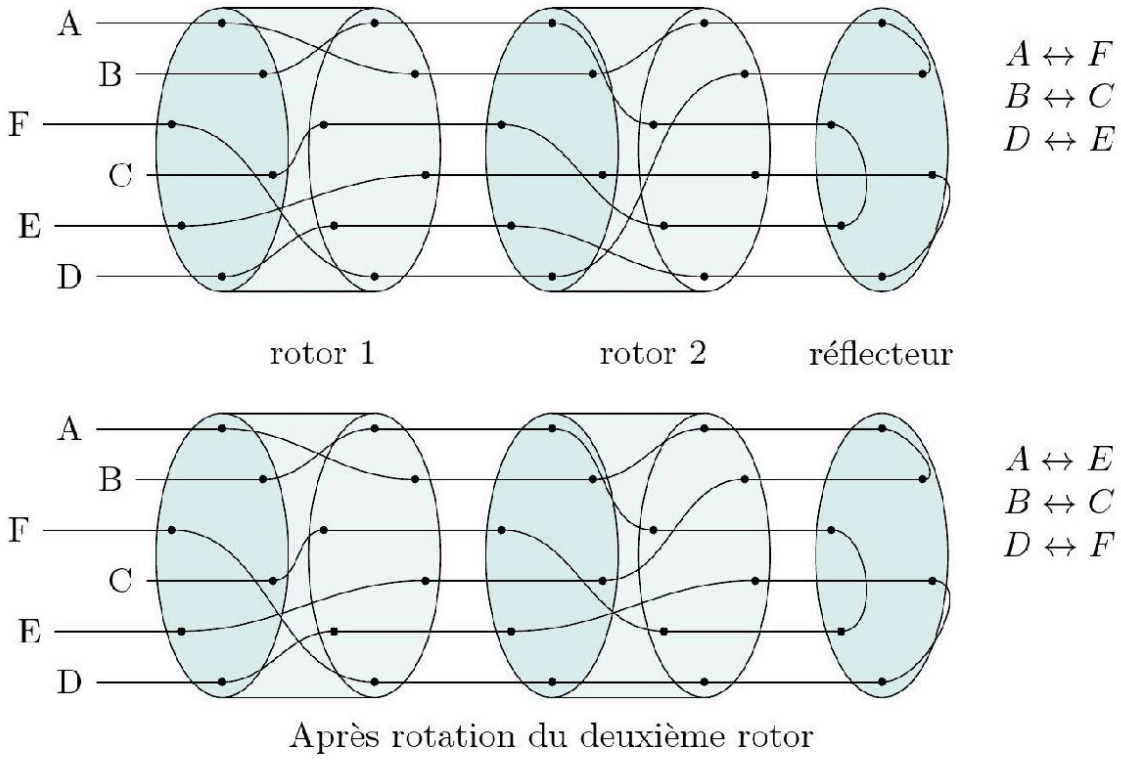


Fig. 1.12 Principe de fonctionnement des machines à rotor illustré sur une machine à deux rotors sur l'alphabet ABCDEF. Chaque lettre de texte provoque la rotation des rotors, ce qui change à chaque fois la permutation opérée.

La carte à puce

Une étape technologique importante pour la cryptologie va être franchie avec le dépôt en 1974 par Roland Moreno d'un « objet portable à mémoire revendiquant des moyens inhibiteurs, un comparateur avec compteur d'erreurs et des moyens de couplage avec le monde extérieur ». Ce dispositif deviendra la carte à puce avec l'adjonction d'un processeur de calcul par l'ingénieur en télécommunication Michel Ugon.

http://support.gateway.com/s/Mobile/SHARED/FAQs/1014330Rfaq21.shtml

L'apparition de ce dispositif va avoir un impact considérable sur le développement de la cryptologie dans le grand public et de multiples applications cryptologiques grand public l'utilisent à grande échelle : carte bancaire, carte vitale, cartes d'abonnement à la TV à péage, cartes SIM des téléphones portables.

Une carte à puce contient des clés secrètes qui permettent d'authentifier les données fournies et ainsi d'ouvrir l'accès à des services de façon confiante et sécurisée.