Cryptographie - Enigma

Septembre 2015

"N'accordez jamais une confiance aveugle à un système de cryptographie " - Gilles Dubertret

L'histoire de Enigma

C'est à la fin de la première guerre mondiale qu'est apparue la nécessité de crypter les messages (bien que les techniques de chiffrement existaient déjàdepuis fort longtemps).

C'est un Hollandais résidant en Allemagne, le ***Dr Arthur Scherbius*** qui mit au point à des fin commerciales la machine Enigma, servant à encoder des messages.

Le modèle A de la machine (*Chieffrienmaschinen Aktien Gesellschaft*) fût présentée en 1923 au *Congrès Postal International* de Bern. Le prix de cette machine à l'époque (équivalent à 30000 euros aujourd'hui) en fit un échec cuisant. Mais l'idée fit son chemin et la marine de guerre allemande reprit le projet en 1925 et en confia son évolution au service de chiffrement (*Chiffrierstelle*) du ministère de la guerre allemand. Le modèle *Enigma M3* fût finalement adopté par la *Wehrmacht* (armée Allemande) le 12 janvier 1937.

Ce que les Allemands ignoraient, c'est que les services de contre-espionnage français et Polonais travaillaient également depuis 1930 sur une méthode de déchiffrement. Le ***Commandant Gustave Bertrand*** des services secrets français, recruta pour cela ***Hans Thilo Schmidt*** (dont le nom de code était ***Asche***), qui travaillait à l'époque pour le *Chiffrierstelle*.

Lorsque la seconde guerre mondiale éclata en 1939, les alliés savaient décrypter les messages d'Enigma. Le 24 juillet 1939, ***Marian Rejewski*** (responsable du *Biuro Szyfrow* - service européen le plus avancé dans les recherches sur le chiffrement allemand) remit un modèle de la machine Enigma au ***Commandant Bertrand*** et à ***Alistair Denniston***, chef du service de déchiffrement de l'*Intelligence Service* (IS) britannique.

La guerre s'est ensuite intensifiée et la cadence de déchiffrement augmenta. Ainsi, entre les mois d'octobre et juin 1939, plus de 4000 messages chiffrés furent décodés par les services secrets français. Ces opérations portaient désormais un nom : *Opération Z* pour les français et *Code Ultra* (pour *Ultra Secret*) pour les Anglais.

En Août 1939 les Anglais installèrent à Bletchley Park (80 km de Londres) les services du Code et du Chiffre. Ce n'étaient pas moins de 12000 scientifiques et mathématiciens Anglais, Polonais et français qui travaillaient à casser le code d'Enigma. Parmi ces mathématiciens, on retrouve l'un des inventeurs de l'informatique moderne : ***Alan Turing***, qui dirigeait tous ces travaux.

Les messages décryptés à Bletchley Park arrivaient par tapis roulant à la *Huts 6*, puis, au poste pour être traduits (2 postes par équipe) :

- un pour les messages en retard
- un pour le matériel urgent

Les messages traduits de la *Luftwaffe* étaient transmis aux 3A et ceux de l'armée aux 3M (A= aviation; M= militaire). On attribuait ensuite des *Z* en fonction de l'importance des messages (*1Z*: peu important; *5Z*: extrêmement urgent). Les renseignements étaient résumés et envoyés en 3 exemplaires :

- un au SIS de Broadway ;
- un au service de ministère approprié ou à Withehall ;
- un au général concerné sur le terrain.

Les Anglais réussirent ainsi à déchiffrer ces messages codés. Seulement, la *Kriegsmarine* (Marine de guerre Allemande), utilisant des mesures de cryptage différentes, le déchiffrement s'avèra plus difficile. La capture sur le *U-110* d'une Enigma et surtout de ses instructions permit une avancée importante. Ceci permettant de connaître les positions de sous-marins et de réduire le tonnage coulé par les *U-Boot* (Cf : Le film *U-571*).

Le 1er février 1942, le modèle *Enigma M4* fut mis en service. Pendant onze mois, les alliés ne réussirent pas à décrypter ces messages.

Durant toute la guerre, plus de 18 000 messages par jours furent décryptés, et permirent aux forces de l'alliance de connaître les intentions de l'Allemagne. Le dernier message chiffré fut trouvé en Norvège, signé par l'***Amiral Doenitz*** : « Le Führer est mort. Le combat continue ». Les Allemands ne se sont jamais doutés que leur précieuse machine pouvait être décryptée.

Source :

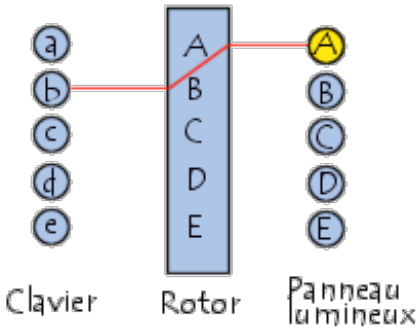
- Mémorial de Caen : http://www.memorial-caen.fr/

Le fonctionnement de Enigma

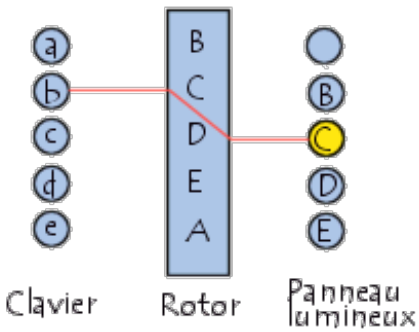
Enigma possédait un fonctionnement particulièrement simple : l'objet était équipé d'un clavier pour la saisie du message, de différentes roues pour le codage, et enfin d'un tableau lumineux pour le résultat.

A chaque pression d'une touche du clavier, une lettre du panneau lumineux s'illuminait. Il y avait ainsi 3 roues de codage, appelées « Brouilleur Rotor », qui reliaient le clavier au panneau lumineux.

Par exemple, avec un seul rotor, lorsque l'on appuie sur *B* le courant passe par le rotor et allume *A* sur le panneau lumineux :



Pour complexifier la machine, à chaque pression sur une touche, le rotor tourne d'un cran. Après la première pression on obtient donc :



Suivant les modèles (M3 ou M4), le système était muni de 3 ou 4 rotors. Les deuxième et troisième rotors avançaient d'un cran quand le précédent faisait un tour complet. Il y avait aussi un tableau de connexion qui mélangeait les lettres de l'alphabet et un réflecteur qui faisait repasser le courant dans les rotors avant l'affichage.

Au final, pour des machines Enigma équipées pour 26 lettres, il y avait 17 576 combinaisons (26 x 26 x 26)

liées à l'orientation de chacun des trois rotors, 6 combinaisons possibles liées à l'ordre dans lequel sont disposés les rotors, soient 100 391 791 500 branchements possibles quand on relie les six paires de lettres dans le tableau de connexions : 12 lettres choisies parmi 26 (*26! /(12!14!)*), puis 6 lettres parmi 12 (12!/6!), et puisque certaines paires sont équivalents (A/D et D/A), il s'agit de diviser par 2^6.

Les machines Enigma peuvent donc chiffrer un texte selon 10^{16} (17 576 * 6 * 100 391 791 500) combinaisons différentes !

Cassage du code d'Enigma

Les Polonais inventèrent « *la Bombe* » (rebaptisée plus tard « Ultra ») qui permettait de connaître les réglages Enigma. Seulement, à partir de 1938, c'est l'opérateur lui-même qui établissait le réglage. Pour remédier à ce problème, les polonais trouvèrent la solution: chaque message contenait soit une répétition de mots soit des mots récurrents (appelés « femelles »).

Ceci était un indice quant au noyau (réglage de base des rotors). Pour découvrir ce réglage, les Polonais utilisaient ensuite la « Grille » (cartes perforées correspondant à toutes les permutations du noyau). Ces cartes étaient empilées les unes sur les autres par rapport à la position des « femelles ».

Ensuite, il s'agissait de chercher le point où une série de perforations se recouvrait du haut en bas de la pile.

Article écrit par Jean-François PILLOU et Sébastien DELSIRIE

‹ Précédent

- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14

Suivant ›

Réalisé sous la direction de Jean-François PILLOU,
fondateur de CommentCaMarche.net.