LYU Shuyuan
OMNES Nathanaël

Rapport - Enigma

Info 910 : Cryptologie

Introduction

Enigma est une machine qui permet de chiffrer des textes. Elle fut créée en 1918 et était surtout utilisée pour un usage civil à la base, comme des banques et des grandes entreprises. Mais Enigma est principalement connue pour son utilisation par les Nazis pour chiffrer leurs messages durant la seconde guerre mondiale.

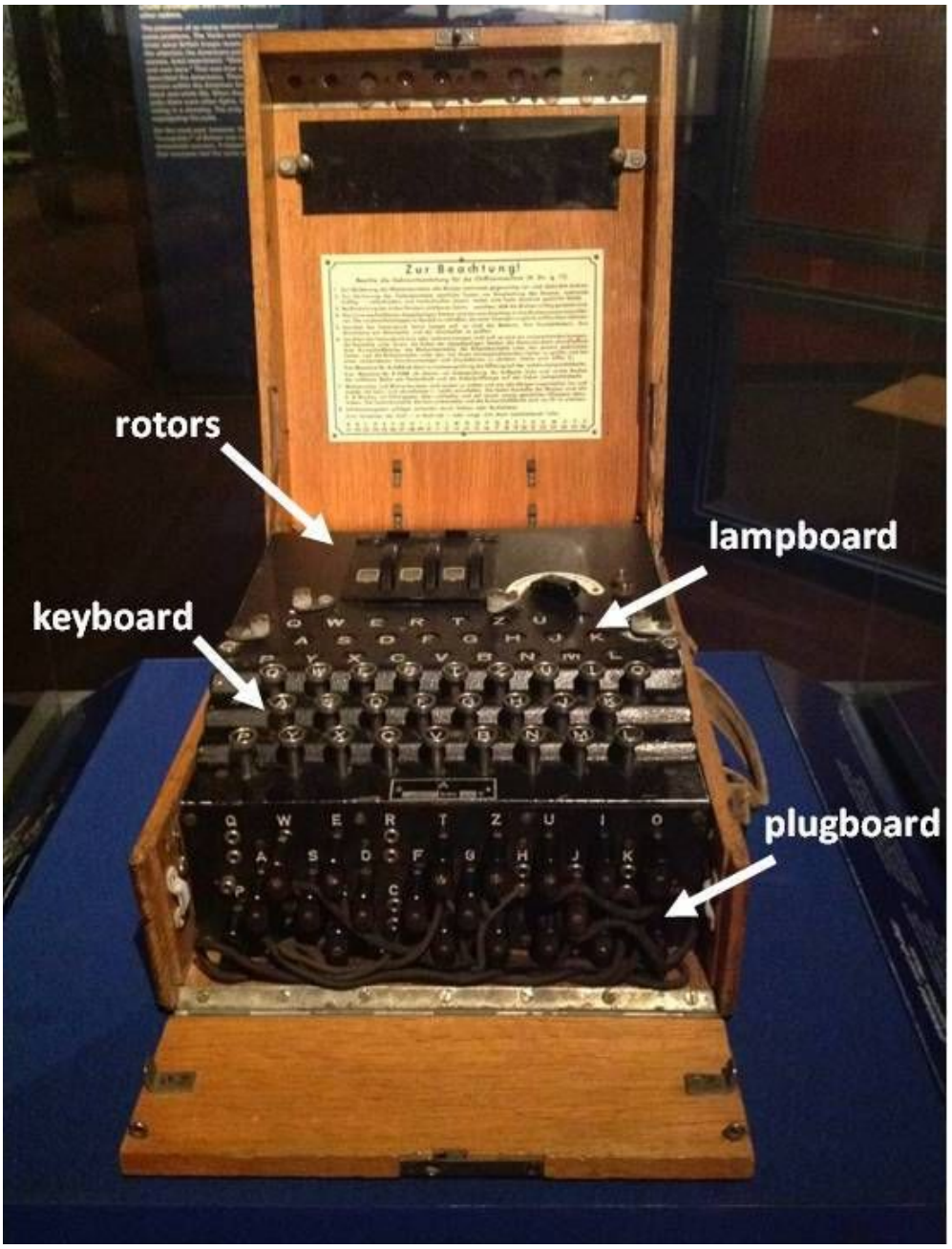
Grâce à son fonctionnement, elle était considérée comme incassable, c'est-à-dire que sans avoir les bons paramètres de la machine, personne ne pouvait trouver le message car trouver la combinaison de paramètres était trop impossible.

Mais les services secrets des forces alliées ont tout de même engagé des gens pour essayer de trouver un moyen de déchiffrer les messages encryptés par Enigma de manière systématique pour pouvoir avoir un avantage certain sur leurs ennemis. Une solution fut trouvée et il a été estimé que cela a permis de finir la guerre 2 ans plus tôt et empêché la mort de 14 millions de personnes.

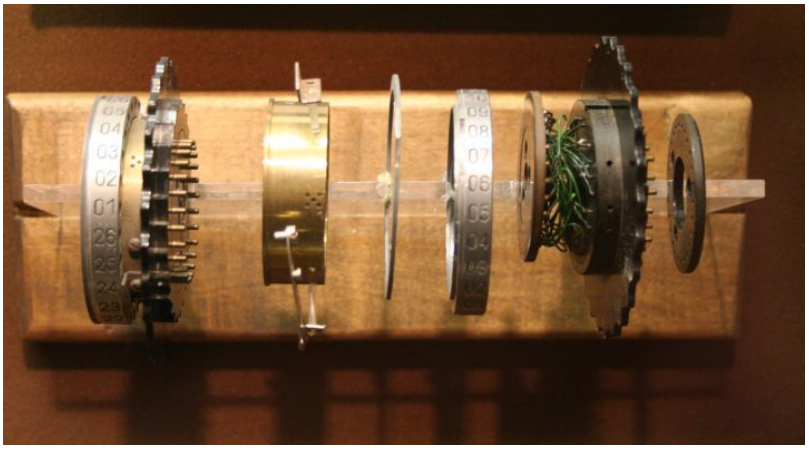
Son fonctionnement

À partir d'un message clair écrit avec les lettre de l'alphabet [A, B, C, …, Z], Enigma chiffre le message avec une méthode par substitution, cela signifie qu'une lettre de l'alphabet sera chiffrée par une autre lettre de l'alphabet dans le message crypté.

Cette méthode de chiffrement fonctionne de la manière suivante :

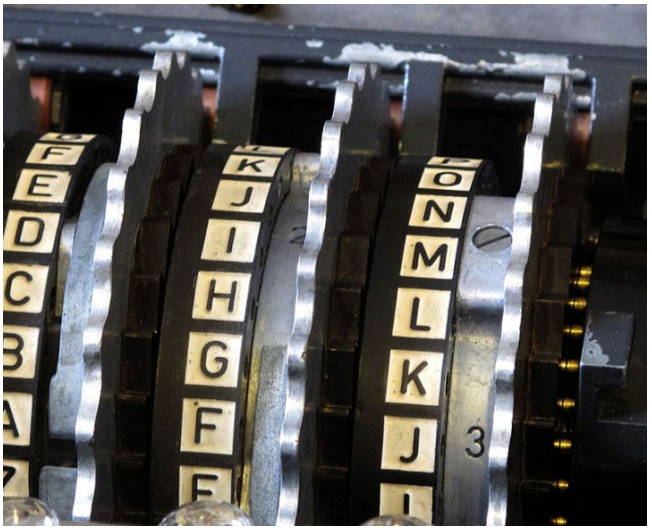


Il y a trois rotors reliés entre eux, chaque rotor dispose de 26 positions différentes, la construction interne est comme l'image ci-dessous :



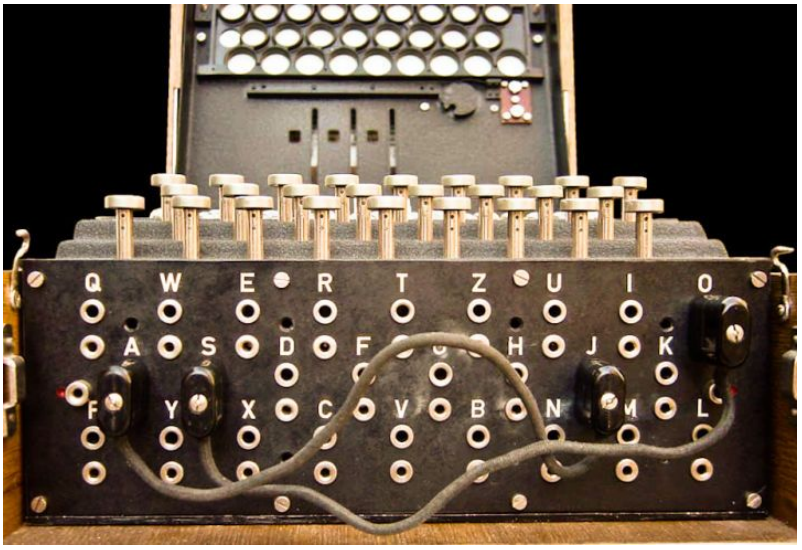
le fonctionnement d’un rotors est simple :

Sur l’une des deux faces sont disposés 26 connecteurs électroniques. Sur l'autre face, le même nombre de connecteurs sont disposés. Les 26 positions représentent les 26 lettres de l’alphabet. Le signal entre depuis la partie gauche, et sort par l’autre partie, les connecteurs du rotor sont reliés entre eux par des câbles croisés (câbles en vert sur l’image ci-dessus). Grâce à cela, une lettre entrée sera chiffrée par une autre lettre avec une substitution classique, par exemple, pour la lettre ‘A’ entrée, ‘E’ sera la sortie.



Une fois que les trois rotors sont assemblés, nous avons trois chiffrements différents imbriqués. Et à chaque fois nous appuyons une lettre sur le clavier, le troisième rotor se décale d’un cran. Quand le 3ème rotor aura fait un tour complet, le 2ème rotor se décalera d’un cran, de même pour le fonctionnement entre le 2ème et le 1er rotor. Ce qui entraîne un changement du circuit interne, à chaque fois qu’une lettre est saisie, le signal électrique ne fera pas le même chemin qu’à la saisie de la lettre précédente. Donc pour une même lettre, la lettre en sortie sera différente.

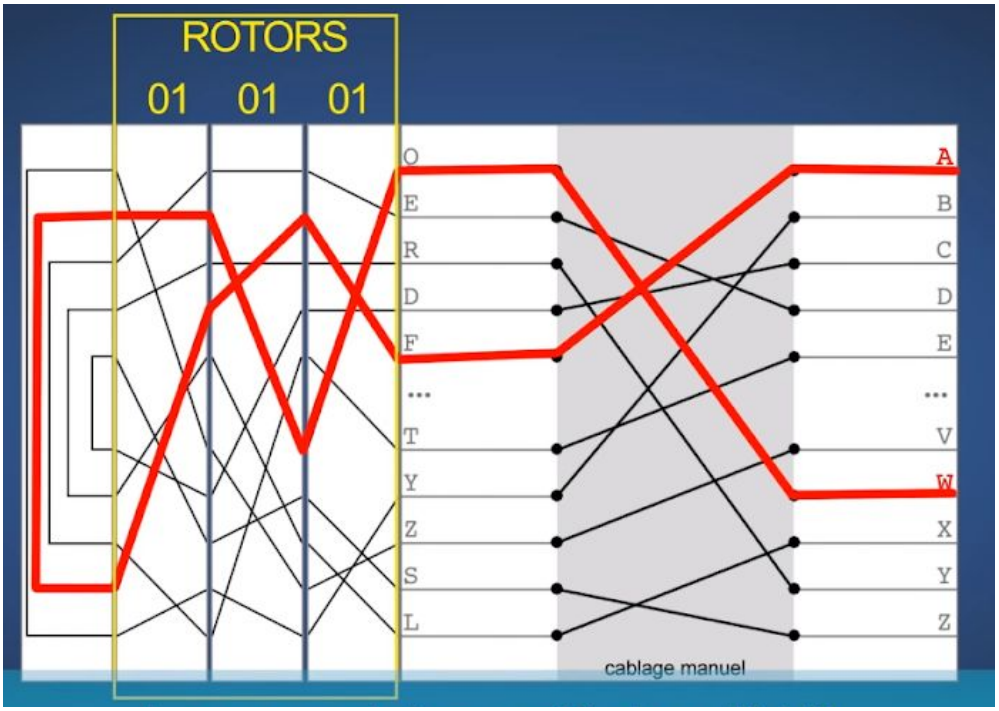
$26^3 = 17\,576$ positions de rotos sont possibles. 5 rotors différents existent, leur différence est qu’en fonction du rotor choisi, la lettre de sortie ne sera pas la même. $5 * 4 * 3 = 60$ possibilités différentes de rotors existent donc : rotors 1-2-3, rotors 2-5-4, rotors 5-1-2, ... Ce nombre combiné aux positions des rotors possibles amène le nombre de possibilités à $17\,576 * 60 = 1\,054\,560$. Bien que déjà un important, avec suffisamment de personnes ou le bon algorithme, la bonne combinaison de rotors et de positions peut être trouvée relativement rapidement par des humains. C’est une méthode par substitution plus évoluée que le chiffre de César mais pas suffisamment complexe pour bien crypter les messages pendant la seconde guerre mondiale.



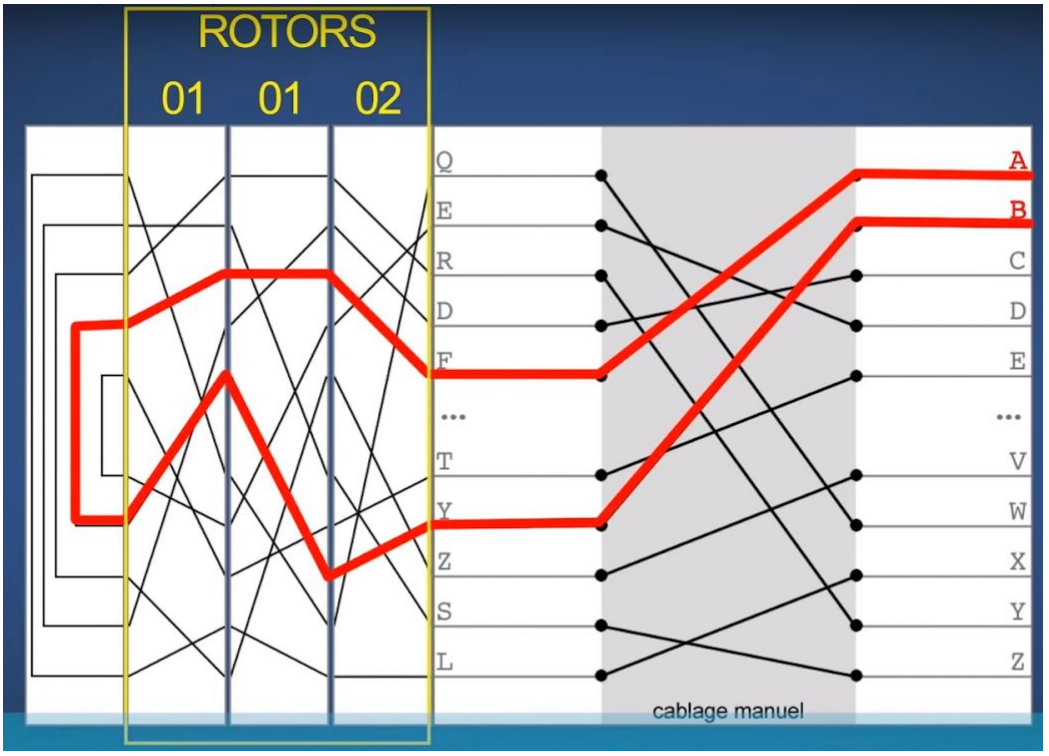
Un câblage manuel a été rajouté à Enigma par l'armée allemande en 1930 pour renforcer la force cryptographique de la machine. Le câblage permet d'échanger jusqu'à 13 paires de lettres entre elles. Généralement, 10 paires de lettres étaient échangées donc 6 lettres restaient identiques. Le câblage manuel permet d'avoir $26! / (6! * 10! * 2^{10}) = 151 * 10^{12}$ possibilités différentes (résultat arrondi).

Le câblage manuel ajouté aux rotors permet donc d'avoir au total $151 * 10^{12} * 1\,054\,560 = 159 * 10^{18}$ possibilités de combinaisons différentes.

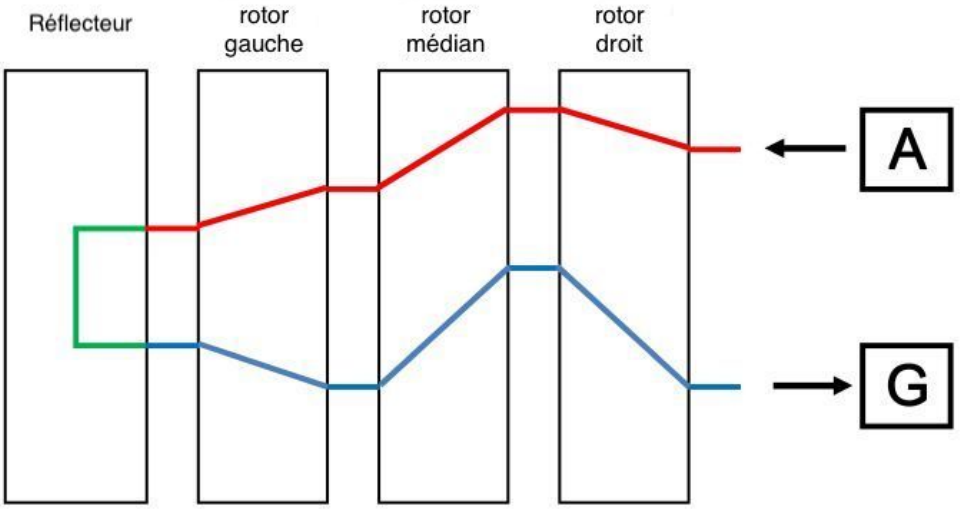
Exemple :



Avec les positions de rotos 1-1-1 et le câblage manuel fait, la lettre A en entrée devient W et inversement.



Avec cette position, la lettre A en entrée devient B et inversement car même si le câblage manuel reste le même, le dernier rotor s'est décalé de 1.



Comme l'image ci-dessus le montre, la lettre 'A' est saisie, le signal d'entrée est le chemin rouge, qui passe par les trois rotors, puis arrive à un réflecteur. Dans ce réflecteur, la lettre est remplacé par une autre lettre (chemin vert), puis le signal sort part le chemin bleu.

Cela donne deux caractéristique à Enigma :

- Ce cryptage est symétrique. Si nous obtenons ‘G’ depuis ‘A’, avec la même paramètre de la machine, nous pouvons forcément obtenir ‘A’ depuis ‘G’.
- La lettre chiffrée ne sera jamais identique, cela est dû au réflecteur, le chemin d’entrée (en rouge) ne peut pas être le même que celui de sortie (en bleu).

De plus, les allemands, changeaient les combinaisons de chiffrement de leurs messages tous les jours. Il est donc complètement impossible de trouver la bonne combinaison d’Enigma en un temps faisable par recherche exhaustive effectuée par des humains.

Enigma possède non seulement une façon de chiffrement difficile à décrypter, mais elle possède aussi une façon d’utilisation simple. Pour obtenir une texte chiffré, il suffit de saisir le texte clair sur le clavier de la machine et noter les lettres chiffrées éclairée par une lumière sur le lamp board, et inversement pour déchiffrer le message. Grâce à cela, des soldats qui n’avaient aucune connaissance en cryptographie pouvaient utiliser cette machine juste en connaissant ses paramètres initiaux et le texte à chiffrer/déchiffrer.

Méthode utilisée pour déchiffrer Enigma

Les messages chiffrés par les allemands étaient envoyés par ondes radios. N’importe qui disposant des bons outils pouvaient intercepter ces messages. Mais seuls ceux qui disposaient d’une machine Enigma avec la bonne combinaison pouvait décrypter le message.

À cause de la menace des Nazis sur l’invasion de la Pologne, c’est le bureau de chiffrement polonais qui a commencé à effectuer des travaux sur le décryptage de la machine Enigma telle qu’elle était utilisée par les allemands. Marian Rejewski a détecté une faille dans la méthode d’envoi les messages par les allemands. Un message envoyé a comme entête une combinaison de trois lettres chiffrée deux fois, cette entête est la clé utilisée le jour même. Elle est suivie d’une clé arbitraire qui indique la position initiale des rotors.

Lors de l’invasion de la Pologne par les allemands, les polonais ont partagé leurs recherches ainsi que deux répliques de la machine Enigma aux français et britanniques.

Malgré la réputation d'Enigma, une solution fût trouvée par l'équipe d'Alan Turing pour déchiffrer la machine. En effet, il existe deux autres défauts qui ont permis aux forces alliées de la déchiffrer.

Le premier défaut vient directement d'Enigma : il est impossible qu'une lettre soit du texte clair soit encryptée par elle-même. Par exemple, la lettre "k" dans le message clair ne pourra jamais être "k" dans le message chiffré.

Le second défaut provient directement des messages des allemands. Certains messages ont réussi à être décryptés avant la création de la machine qui a permis de déchiffrer Enigma appelée "Bombe". Il a été remarqué que les forces allemandes envoyaient chaque jour à 6h00 le bulletin météo, qui était composé du mot "wetterbericht" ainsi que "heil Hitler".

À partir de ces deux défauts, une machine qui pouvait chercher la bonne combinaison des paramètres d'Enigma fût inventée par Alan Turing. Cette machine testait les combinaisons possibles et dès qu'une contradiction dans la combinaison était trouvée, la machine passait à la combinaison suivante.

Exemple de contradiction :

Exemple de combinaison possible :

Tous les câblages et rotors possibles étaient par la suite essayés. Un des points positifs de cette machine est qu'à partir d'une contradiction trouvée, toutes les étapes intermédiaires qui ont mené à cette contradiction peuvent être rejetées ce qui réduit le temps de traitement nécessaire pour trouver la bonne combinaison.

Finalement, la bonne combinaison quotidienne utilisée pour crypter un message pouvait être trouvée en 20 minutes grâce à cette machine. "Bombe" fût inventée en 1940, elle connut des amélioration jusqu'à la fin de la guerre.

Sources

https://en.wikipedia.org/wiki/Enigma_machine
Imitation Game - Morten Tyldum
http://www.bibmath.net/crypto/index.php?action=affiche&quoi=debvingt/enigmaguerre
https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma
http://www.nww2m.com/2012/10/sci-tech-tuesday-70th-anniversary-of-enigma-capture-from-u-559/
http://users.telenet.be/d.rijmenants/en/enigmasim.htm
https://en.wikipedia.org/wiki/Bombe
En chinois :
https://zhuanlan.zhihu.com/p/20336621
https://www.zhihu.com/question/28397034