Favre-Teylaz Sacha
Favre-Teylaz Baptiste
Quentin Blin

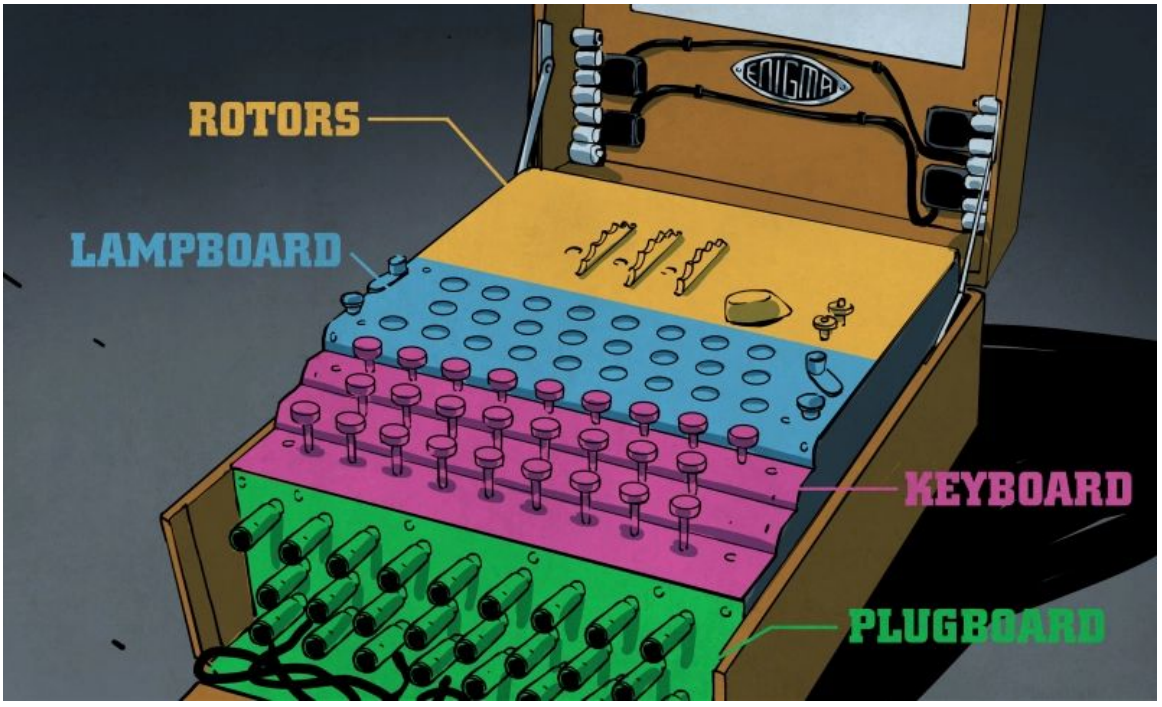
Rapport - Enigma

Info 910 : Cryptologie

Introduction

Enigma est une machine électromécanique portable servant au chiffrement et au déchiffrement de l'information. Elle fut inventée par l'Allemand Arthur Scherbius en reprenant un brevet de 1919 de Hugo Koch.
Le terme Enigma désigne en fait toute une famille de machines, car il en a existé de nombreuses et subtiles variantes, commercialisées en Europe et dans le reste du monde à partir de 1923. Elle fut aussi adoptée par les services militaires et diplomatiques de nombreuses nations.
Son utilisation la plus célèbre fut celle faite par l'Allemagne nazi et ses alliés, avant et pendant la Seconde Guerre Mondiale.

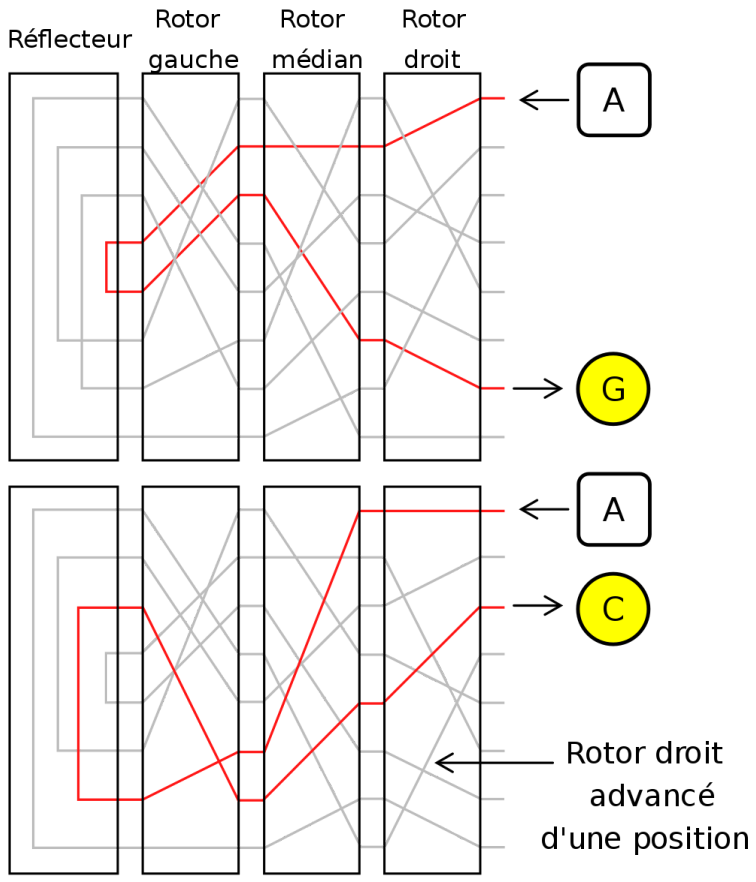
Description



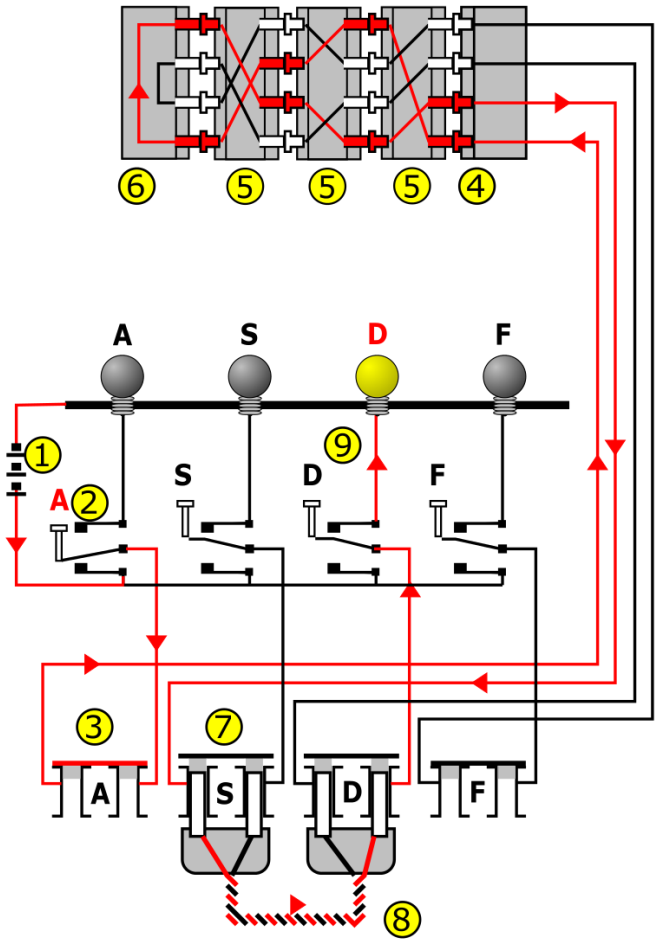
Enigma chiffre les informations en faisant passer un courant électrique à travers une série de composants. Ce courant est transmis en pressant une lettre sur le **clavier**, il traverse un réseau complexe de fils puis allume une **lampe** qui indique la lettre chiffrée. Le premier composant du réseau est une série de roues adjacentes, appelées **rotors** , qui contiennent les fils électriques utilisés pour chiffrer le message. Les rotors tournent, modifiant la configuration complexe du réseau chaque fois qu'une lettre est tapée. Enigma utilise habituellement une autre roue, nommée **réflecteur**, et un composant appelé **tableau de connexion**, ce qui permet de complexifier encore plus le processus de chiffrement.

Fonctionnement

Enigma est une machine électromécanique, ce qui signifie qu'elle utilise une combinaison de parties mécaniques et électriques. La partie mécanique est composée du clavier, des différents « rotors » arrangés le long d'un axe et d'un mécanisme entraînant en rotation un ou plusieurs des rotors chaque fois qu'une touche est pressée. Le mouvement continu des rotors permet l'obtention de transformations cryptographiques différentes à chaque pression sur une touche. La partie électrique de l'appareil est constitué par une pile reliant les touches du clavier à des lampes. Lorsque l'on appuie sur l'une des touches, l'une des lampes s'allume.



Pour déchiffrer un message, il faut soit disposer d'une machine Enigma absolument identique à celle qui a été utilisée par l'expéditeur pour le chiffrement de ce message et que cette machine soit réglée de la même façon, soit avoir une connaissance approfondie du fonctionnement extraordinairement complexe de cette machine, ce dont peu de gens étaient capables. Par contre, une fois la clef quotidienne d'encodage découverte, tous les messages échangés ce jour-là par le réseau concerné peuvent enfin être très rapidement décryptés.



Les rotors forment le cœur de la machine Enigma. Sur une face sont disposés en cercle des contacts électriques à aiguilles, donc équipés de ressorts. Sur l'autre face, le même nombre de contacts plats sont disposés. Les contacts plats et à aiguilles représentent l'alphabet. Une fois les rotors assemblés, les contacts à aiguilles d'un rotor se positionnent en face des contacts plats du rotor voisin, formant ainsi la connexion électrique. À l'intérieur du rotor, un ensemble de 26 câbles électriques assurent les connexions entre les contacts à aiguilles et les contacts plats suivant un schéma compliqué, qui permet le chiffrement des lettres. D'un rotor à l'autre, les connexions internes ne sont pas les mêmes.

Le rotor utilisé tout seul ne réalise en fait qu'un chiffrement très simple, le chiffrement par substitution. Par exemple, le contact à aiguille correspondant à la lettre E peut

être connecté sur la face opposée au contact plat de la lettre T. La complexité de la machine Enigma provient de l'utilisation de plusieurs rotors en série généralement trois ou quatre, ainsi que le mouvement régulier de ces rotors. Lorsque 26 lettres ont été pressées, une came entraîne le rotor de la fente suivante et le fait tourner. L'alphabet de substitution est ainsi modifié à chaque pression de touche. Ces deux mécanismes forment un type de chiffrement beaucoup plus performant.

À l'exception des machines Enigma modèles A et B, le dernier rotor était suivi d'un **réflecteur**. Le réflecteur connecte les sorties du dernier rotor par paire, redirigeant le courant dans les rotors selon un chemin différent. C'est ce réflecteur qui garantit le caractère involutif de l'Enigma : chiffrer est identique à déchiffrer, comme pour le chiffrement par masque jetable. Cependant, le réflecteur empêche également l'Enigma de substituer une lettre à elle-même dans le texte chiffré.

Les machines des armées, et non les machines commerciales, avaient un **tableau de connexion** à l'avant de la machine, composé de l'alphabet. Quand une touche est pressée, le courant électrique passe d'abord par le câble de la lettre échangée, avant de traverser les rotors, qui fonctionnent normalement. Dix paires de lettres sont ainsi permutées chaque jour. C'est la partie de la machine qui possédait les possibilités de connexions les plus élevées, bien plus que les rotors.

Sécurité et combinaisons

Dans le premier emplacement, il y a 5 rotors à choisir, dans le deuxième, 4 rotors à choisir et dans le troisième, 3 rotors à choisir. Il y a donc 5×4×3 = 60 façons de configurer les cinq rotors.

Il y a 26 positions de départ pour chaque rotor, donc il y a 26×26×26=17,576 choix pour les configurations initiales des numéros/lettres des rotors.

Comme il y a 26 lettres dans l'alphabet, il y a 26! façons de disposer les lettres, on faisait en général 10 paires avec le tableau de connexion, donc il y a 20 lettres impliquées dans les paires, et 6 restantes qui doivent être divisées. De plus, il y a 10 paires de lettres, et l'ordre des paires n'a pas d'importance, donc il faut aussi diviser par 10! et l'ordre des lettres dans la paire n'a pas d'importance, donc il faut aussi diviser par 2^10. Le nombre de combinaisons obtenu par le tableau de connexion est le suivant :

$$\frac{26!}{6!\times 10!\times 2^{10}} = 150,738,274,937,250$$

au total on a : 60×17576×150,738,274,937,250= 158,962,555,217,826,360,000 façons de configurer la machine.

Mise en oeuvre d’Enigma

La mise en œuvre est effectuée par deux chiffreurs. La procédure est entièrement manuelle. Dans l'Armée de terre et la Luftwaffe les choses se passent comme suit. Chaque mois de l'année, dans chaque réseau, de nouvelles instructions de mise en œuvre spécifient des modifications (quotidiennes ou plus fréquentes) de plusieurs réglages.

Réglage interne :

1- Ordre des rotors : choix et positionnement des trois rotors prescrits par les instructions (ex : I-V-III).

2-Disposition de la bague des rotors gauche, milieu et droit prescrite par les instructions.

3- Permutations des fiches du tableau de connexions prescrites par les instructions. Un des chiffreurs dispose la machine en conséquence.

Réglage externe :

4- Le premier chiffreur dispose les trois rotors sur la position initiale définie par les instructions quotidiennes, le premier chiffreur choisit au hasard un réglage initial de rotors et le frappe deux fois, c'est la clef brute du message

5- Le second chiffreur note le résultat affiché par les voyants ; c'est l'indicateur ou clef chiffrée

6- Le premier chiffreur dispose ses rotors sur la position indiquée par la clef brute puis entre au clavier le texte du message en clair, lettre par lettre ; le second chiffreur note les lettres signalées par l'allumage des voyants.

Le message clair est bien sûr formaté par l’état major allemand pour brouiller encore plus les pistes, le message chiffré et formaté est alors émis en morse au moyen d'un poste radio.

Contexte Historique

Enigma permis au allemands de chiffrer des messages avant et pendant la seconde guerre mondiale en effet, 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 pouvaient décrypter le message.

Les polonais furent les premiers à effectuer des travaux sur le decryptage des messages d'enigma. Marian Rejewski et ses collègues du bureau du chiffre polonais sont les premiers à réussir à déchiffrer des messages sans avoir jamais eu d'Enigma entre les mains puis plus tard à mettre des "bomby" au point pour déchiffrer les messages.

En janvier 1939, les Alliés décidèrent d'envoyer et de centraliser tous les éléments connus sur les déchiffrages d'Enigma à Bletchley Park,les cryptanalystes britanniques, dont Alan Turing, purent continuer les travaux de Marian Rejewski. Ils furent par la suite, dans des circonstances favorables et pendant des intervalles de temps plus ou moins longs, capables de déchiffrer les messages Enigma en perfectionnant les « bombes électromécaniques» inventées et mises au point par Rejewski.

Les informations obtenues grâce au déchiffrement des messages d'Enigma donnèrent au camp des Alliés un avantage certain dans la poursuite de la guerre.

Cryptanalyse d'Enigma

Propriété technique d'Enigma :
Certaines propriétés d'Enigma ont aidé à son décryptage, on peut ainsi prendre en compte la règle qui fait qu'une lettre ne peut pas rester identique après le processus de cryptage.
Il faut également considérer que le cryptage est symétrique, il utilise la même clé de cryptage que de décryptage.
Pour finir le mécanisme qui permet de faire bouger les rotors et donc de changer la clé de cryptage affecte moins les rotors situés dans les dernières positions, un texte court peut donc être identique sur une machine à trois ou quatre rotors.

Défaillances humaines :
Des défaillances humaines liées à la fatigue et au surmenage des agents de transmission leur ont fait commettre des erreurs.
Parmi ces dernières il y a par exemple les "cillies" qui tirent leur nom d'un allemand qui utilisait toujours C.I.L comme clé, alors qu'ils avaient pour règles de changer régulièrement de clé de cryptage.

Dans le même type il y a également les “Herivel tips”, le fait de ne pas changer la position initiale des rotors dont le nom provient du mathématicien qui avait prévu cette faille.
En dernière place dans cette catégorie il y a les messages de test, rempli par exemple de T (dont la version crypté ne contient donc aucun T), ces messages ont permis de mieux comprendre le fonctionnement des rotors.

Stratégie de communications :
La stratégie de communications des allemands à également laisser paraître des failles qui ont permis d’aider au décryptage d’Enigma.
Le meilleur exemple sont les “Cribs”, ce sont la diffusion de messages identiques cryptés et non cryptés, qui permettent de comparer et de valider une traduction.
Également le formalisme imposé pour la rédaction de document a permis de faire gagner un temps précieux en termes de vérification et de validation.

Méthode de protections :
Pour ralentir le décryptage, les Allemands ont mis en place des parades, avec la modification du nombre de rotors, ou des branchements internes de rotors.
Ils ont également mis en place des codages avant chiffrement, ainsi les messages de la Kriegs Marine même en cas de décryptage restait complètement illisible pour les décrypteurs.

Décryptage avant Turing :
Des méthodes de décryptage basées sur des grilles symbolisant la position des rotors étaient initialement utilisées.
Avant turing les polonais avait déja réussi à casser Enigma dans sa version commerciale, grâce a une bombe électro mécannique.
Cependant avec l’invasion de la Pologne et les modifications appliquées à Enigma par l’armée allemande, ces méthodes étaient devenues obsolètes.

Bombes électromécaniques :
Les bombes en cryptologie ne sont pas des engins explosifs et elles permettent au contraire de "bruteforcer" un code en essayant un nombre très grands de possibilités.
Dans le cas d’Enigma elles permettent d’essayer toutes les positions possibles de rotors.
Le problème est qu’elle nécessite de connaître la structure de la machine à décrypter.
La bombe construit en 1938 par les polonais en se basant sur une version commerciale d’Enigma n’était donc inneficace sur les versions de l’armée, mais en utilisant des version capturé pendant la guerre Turing est parvenue a mettre au point une bombe capable de percer Enigma.

Ce haut fait a paradoxalement été possible grâce au allemands qui en structurant leur message de manière ultra prévisible et en laissant des phrases très récurrentes ont permis de faire facilement valider des hypothèses de combinaisons.

Principes des bombes électromécaniques :
Les bombes se contentent de simuler une position aléatoire des rotors et de tester si un texte clair devient le texte codé.
Cependant si on connaît le texte initial par analyse de récurrence on peut faire valider beaucoup plus rapidement une hypothèse et de manière beaucoup plus sûr que par compte d'indice de récurrence des lettres.
C'est ainsi que l'armée allemande a été trahie par son utilisation abusive de "heil hitler" dans tous ses messages.

Conclusion

Les historiens estiment que Turing et son équipe ont sauvé 14 millions de vies tout en écourtant la guerre d'au moins 2 ans grâce aux travaux de cryptanalyse d'Enigma. Les travaux de Turing ont permis le développement de machines de Turing, les premiers ordinateurs.

Sources

https://fr.wikipedia.org/wiki/Enigma_(machine)

https://fr.wikipedia.org/wiki/Alan_Turing

https://fr.wikipedia.org/wiki/Cryptanalyse_d'Enigma

https://www.youtube.com/watch?v=V4V2bpZlqx8

https://hackaday.com/2017/08/22/the-enigma-enigma-how-the-enigma-machine-worked/

https://brilliant.org/wiki/enigma-machine/