BAJT Arthur
JUBARD Théo

INFO002
Lundi 20 Mars 2023

INFO002 : Cryptologie

Enigma et chiffrement pendant la 2ème Guerre Mondiale

2022-2023

Table des matières

Introduction

Depuis l'Antiquité, la guerre a été un catalyseur pour les avancées technologiques dans de nombreux domaines, y compris la cryptologie et la stéganographie.
La cryptologie est l'étude de la sécurité des communications et la stéganographie est l'art de la dissimulation de messages. Ces deux techniques ont été largement utilisées dans les conflits armés pour protéger les messages et les secrets des ennemis.
L'histoire montre que les gouvernements et les armées ont développé des méthodes sophistiquées de cryptage et de dissimulation de messages, souvent considérées comme des éléments essentiels de la stratégie militaire.
Nous vous proposons avec ce document de nous intéresser au fonctionnement d'Enigma, la façon dont cette machine cache et chiffre des messages. Ainsi qu'à différentes machines.

Poste de travail d'un opérateur recevant et envoyant les messages

La machine à chiffrement : Enigma

Histoire

La machine à chiffrer Enigma a été inventée dans les années 1920 par l'ingénieur allemand Arthur Scherbius. Elle a été utilisée par les forces armées allemandes pendant la Seconde Guerre mondiale pour protéger leurs communications militaires.

L'objectif de l'utilisation de la machine Enigma était de crypter les messages pour que seuls les destinataires autorisés puissent les comprendre, tout en empêchant les ennemis de décoder ces messages interceptés. En utilisant des réglages différents pour la machine régulièrement, les Allemands pensaient qu'ils avaient créé un système inviolable, ce qui leur a donné un avantage dans la guerre.

Cependant, les Alliés ont finalement réussi à casser le code Enigma en utilisant des techniques de cryptanalyse avancées. Cela leur a permis de comprendre les plans et les intentions des Allemands, donnant ainsi un avantage considérable aux Alliés. La cassure du code Enigma est considérée comme un tournant décisif dans la guerre et a contribué à la victoire finale des Alliés.

Fonctionnement mécanique de Enigma

Enigma est de façon simple, est un simple système permettant de remplacer une lettre saisie par une autre, comme le chiffrement de César. Toutefois, là où le chiffrement de César est une technique de substitution simple qui utilise un décalage fixe pour remplacer chaque lettre du message original. Le chiffrement d'Enigma est une technique de substitution beaucoup plus complexe qui utilise plusieurs rotors pour permuter les lettres du message original. La configuration initiale de la machine influe sur le résultat obtenu.

Étant donné que Enigma encode un message depuis une configuration initiale, il est aussi possible de l'utiliser pour décoder un message. Si bien sûr, le receveur partage la même configuration initiale sur sa machine.

Voyons maintenant ce qui compose Enigma :

Rotors

Les rotors sont une superposition de petit point de contact enchantant le signal d'une lettre pour une autre.
Leur position change à chaque appui de touche.

Tableau Lumineux (Sortie)

Un fois le signal d'une touche permuté par le reste des composants, il illumine l'une des lettres correspondantes sur le tableau lumineux.
Ces lettres composent le message encodé.

Clavier (Entrée)

C'est ici que nous rentrons le message en clair.
A l'appui d'une touche, un signal électrique parcourt la machine et est encodée avant d'être affiché sur le tableau lumineux.

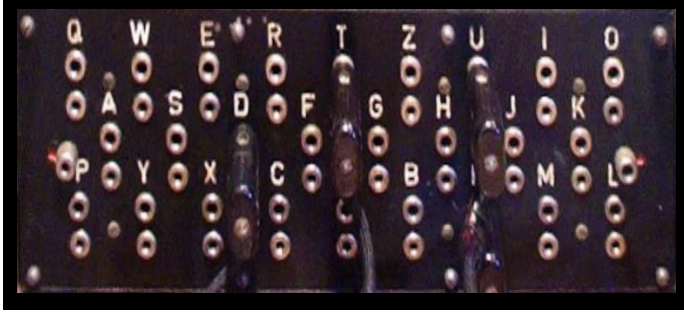
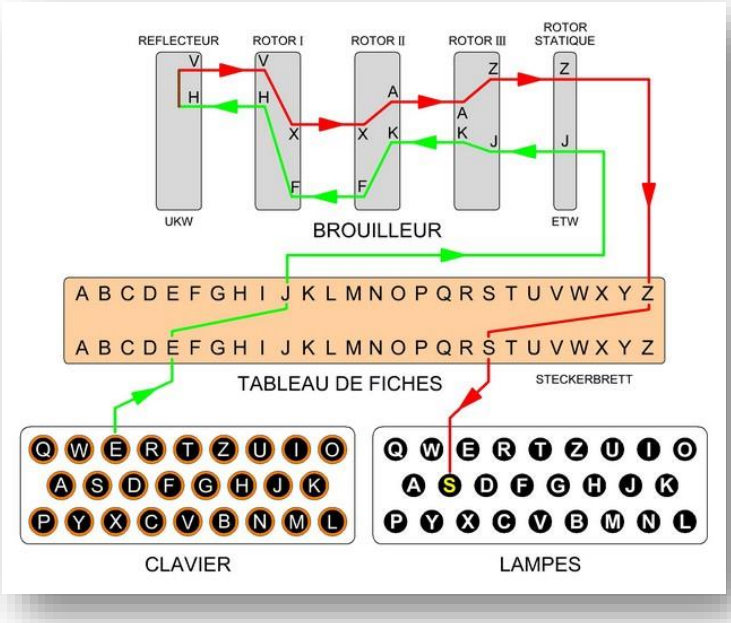


Tableau de fiches

Ici chaque lettre peut être permutée manuellement avec une autre. Si aucune fiche n'est branchée à une lettre, le signal reste inchangé avant de rentrer ou de sortir des rotors.

Voyons maintenant le parcours d'un signal à la saisie d'une lettre, jusqu'à l'affichage de la lettre encodée :

Clavier	Tableau de fiches	Rotors					Tableau de fiches	Tableau Lumineux
Appuie sur une Touche	1er passage dans le tableau de fiches	1er rotor	N-ème rotor	Réflecteur	N-ème rotor	1 er rotor	2ème passage dans le tableau de fiches	Affichage
Création du signal Et incrémentation des rotors	La lettre est échangée ou non avec une autre	La lettre est échangée	La lettre est échangée	Le signal repart des Rotors.	La lettre est échangée	La lettre est échangée	La lettre est échangée ou non avec une autre	La lettre est affichée
Début →	→ → → sens du signal → → →							→ Fin



Exemple de passage par Enigma

Représentation Mathématique

Cette présentation du fonctionnement mécaniques de Enigma peut être accompagnée d'une représentation algorithmique des actions faites par la machine. Enigma repose sur plusieurs produits de permutations.
On utilisera la notation suivante dans la suite de cette partie :

- P pour la transformation réalisée par le clavier
- U pour l'action du réflecteur
- G, M, D les actions des différents rotors (gauche, milieu, droite)
- C le codage ou la suite d'action effectués après chaque appuie sur une touche
-

On obtient alors la représentation suivante :

$$C = PDMGUG^{-1}M^{-1}D^{-1}P^{-1}$$

Cette représentation représente les actions suivantes : A chaque appuie sur le clavier (**P**), le rotor droit tourne (**D**), puis celui du milieu (**M**), puis celui de gauche (**G**). On retrouve ensuite l'action du réflecteur (**U**) permettant d'inclure un caractère involutif à la machine (déchiffrer et chiffrer sont la même action). Bien sûr, ces différentes actions dépendent des actions effectuées lors du dernier appuie sur le clavier.

En allant plus loin, chaque action sur une lettre du clavier entraîne une rotation du rotor ainsi qu'une transformation cryptographique. Ainsi pour une rotation de i positions du rotor droit, le chiffrement est représenté sous la forme $\boldsymbol{\rho^{i}D\rho^{-i}}$ où désigne une permutation circulaire (Passage de A à B, de B à C …). En appliquant cette logique pour les rotors du milieu (j rotations) et de gauche (k rotations), on obtient alors la formule suivante :

$$C = P\,(\rho^{i}D\rho^{-i})(\rho^{j}M\rho^{-j})(\rho^{k}G\rho^{-k})\,U\,(\rho^{i}D^{-1}\rho^{-i})(\rho^{j}M^{-1}\rho^{-j})(\rho^{k}G^{-1}\rho^{-k})\,P^{-1}$$

Eléments de Enigma présents dans la formule

Nombre de Possibilités

Malgré son principe connu de tous, Enigma reste une machine très pertinente pour son nombre très important de combinaisons entre les réglages initiaux de la machine et la clé brute du message. Ce nombre important de combinaisons s'explique via le fonctionnement même de Enigma.
Le calcul se fait en plusieurs étapes : l'arrangement des rotors, l'alphabet des rotors et le tableau de connexions.

Cette machine compte 3 rotors à arranger parmi les 5 présents. Pour leur positionnement, on compte donc :

$$A_3^5 = \frac{5!}{2!} = 5 * 4 * 3 = 60\ Possibilités$$

En dehors de l'arrangement des rotors, il faut prendre en compte le fait que chacun d'eux possède les 26 lettres de l'alphabet. On se retrouve donc avec :

$$26^3 = 17576\ Possibilités$$

Ces possibilités concernent les arrangements pour les 3 lettres initiales.

Pour finir, il faut prendre en compte l'état du tableau de connexions : celui-ci compte 10 câbles qui permettent de relier 20 lettres 2 à 2. 20 lettres pourront donc être permutées tandis que les 6 dernières resteront inchangées.
Le nombre de possibilité suivante est donc présenté :

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

Ce résultat s'explique de la manière suivante : en comptant les combinaisons totales de connexions, on trouve 26! possibilités. Cependant, 6 lettres ne sont pas connectés en enlevant donc 6! possibilités. De plus, l'ordre des paires étant interchangeable et sans ordre ni classification unique, on se retrouve avec 10! possibilités en moins. Pour finir, on peut remarquer le fait que les paires de lettres marchant dans les 2 sens, sans cheminement à sens unique soit 210possibilités.

Une fois ces 3 calculs effectués, on peut donner le nombre total de combinaisons possibles :

$$60 * 17576 * 150738274937250 = 158962555217826360000 \simeq 1.59 * 10^{20}$$

Exemple d'implémentation de la logique d'Enigma

Bien que la méthode de chiffrement d'Enigma ne soit plus utilisée depuis longtemps, de nombreuses applications et librairies permettent de prendre en main Enigma mais aussi de

Enigma Java: Librairie Java, celle-ci permet de prendre en main sous forme textuelle la machine en chiffrant et déchiffrant des messages et en jouant sur certains paramètres. La librairie donne aussi accès aux méthodes de craquages de la machine permettant ainsi de mieux comprendre comment ceux-ci ont été trouvés.

pyEnigma: Tout comme pour la librairie Java, elle permet de prendre en main Enigma. Celle-ci possède malgré un paramétrage beaucoup plus poussé, donnant l'accès aux différentes versions de la machine mais aussi aux paramètres en fonction des années de fabrications. Il est aussi possible de modifier les tables de permutations, la position des rotors et ainsi que les 3 premières lettres.

```
>>> print("Affichage du rotor\n",rotor.ROTOR_GR_III,"\n")
Affichage du rotor

        Name: III
        Model: German Railway (Rocket)
        Date: 7 February 1941
        Wiring: JVIUBHTCDYAKEQZPOSGXNRMWFL
        State: A
>>> engine = enigma.Enigma(rotor.ROTOR_Reflector_A, rotor.ROTOR_I,rotor.ROTOR_II, rotor.ROTOR_III,
key="ABC", plugs="AV BS CG DL FU HZ IN KM OW RX")
>>> print("Affichage de la machine \n",engine,"\n")
Affichage de la machine

        Reflector:
        Name: Reflector A
        Model: None
        Date: None
        Wiring: EJMZALYXVBWFCRQUONTSPIKHGD

        Rotor 1:
        Name: I
        Model: Enigma 1
        Date: 1930
        Wiring: EKMFLGDQVZNTOWYHXUSPAIBRCJ
        State: A
```

Virtual Enigma: publié le 23 juin 2021, le site permet l'accès à Enigma dans un environnement en 3d. Ludique, cette simulation accompagne l'utilisateur dans le paramétrage et l'utilisation de Enigma tout en apportant du contexte historique. Le site donne aussi accès à des simulations d'autres machines de chiffrement créées durant la seconde guerre mondiale.

Autres machines de chiffrement similaires

Machine à chiffres C-38

Aussi connus sous le nom : C-35 et C-37. La machine à chiffres C-38 est l'équivalent français à Enigma. Elle a été développée avant la Seconde Guerre mondiale par la société A.B. Cryptoteknik du Suédois Boris Hagelin.
En 1934, l'armée française demande à Hagelin de plancher sur une machine à chiffrer/déchiffrer pouvant se transporter facilement sur le front.

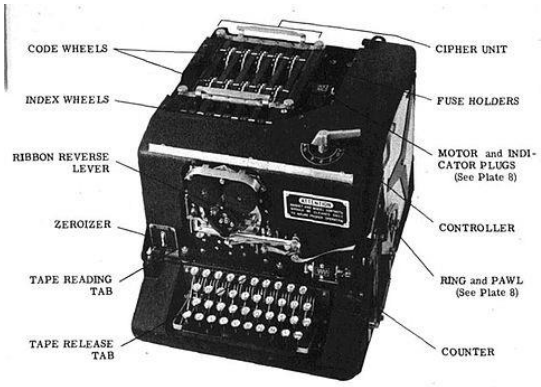
La machine C-38 a été considérée comme étant plus sûre que la machine Enigma, car elle avait un plus grand nombre de configurations possibles pour les rotors et d'autres paramètres, la rendant plus difficile à décrypter. Cependant, malgré la relative sécurité de la machine C-38, les forces allemandes ont finalement réussi à la casser, ce qui a permis de déchiffrer les messages confidentiels français pendant la guerre.

La machine M-209

La machine M-209 a été utilisée par l'armée américaine pendant la Seconde Guerre mondiale, la machine M-209 était une machine portable à roue de chiffrement qui utilisait plusieurs roues pour chiffrer les messages. Elle était plus simple que la machine Enigma mais offrait tout de même un niveau de sécurité suffisant pour les communications militaires.

SIGABA

La machine SIGABA (ou Converter M-134, CSP-889, CSP-2900) : Également utilisée par l'armée américaine pendant la Seconde Guerre mondiale, la machine SIGABA était considérée comme l'une des machines de chiffrement les plus sûres de son époque. Comme beaucoup de machines de cette époque, elle utilisait un système électromécanique de rotors pour chiffrer les messages. Aucune cryptanalyse efficace contre elle pendant sa période de mise en service n'a été révélée à ce jour.



La machine Purple

Utilisée par les forces militaires japonaises pendant la Seconde Guerre mondiale, la machine Purple était une machine électromécanique complexe qui utilisait des roues pour chiffrer les messages. Elle était considérée comme étant plus sûre que la machine Enigma mais a finalement été cassée par les cryptanalystes américains.

Conclusion

Malgré la complexité de Enigma, cette machine à pu être cassé par de nombreuses personnes :

- Décembre 1932 : Des mathématiciens polonais réussissent à décrypter des messages chiffrés avec Enigma
- Octobre 1938 : L'un de ces mathématiciens crée un système de décryptage électromécanique (2 heures étaient nécessaires pour déchiffrer la clé)
- 25 Juillet 1939 : Des exemplaires d'Enigma avec la documentation de décryptage ont été envoyé aux représentants de renseignement français et britannique.
- Pour finir, Alan Turing accompagné d'autres mathématiciens britanniques furent à l'origine de la bombes électromécaniques la plus efficace pour décrypter Enigma en se basant sur les travaux de Marian Rejewski, mathématicien à l'origine de ce type de méthode.

Les conflits du 21ème siècle et plus particulièrement la seconde Guerre Mondiale ont permis de faire passer la cryptographie d'un domaine artistique à un domaine mathématique. Les avancées faites durant ce conflit ont permis de poser les bases de la cryptologie moderne ainsi que de marquer les premiers pas de l'informatique.