Comment Alan Turing a cassé Enigma

Introduction

Le chiffrement de messages a toujours été une pratique importante pour protéger les informations sensibles et confidentielles dans le monde de la communication.

Cependant, pendant la Seconde Guerre mondiale, la machine de chiffrement allemande Enigma a posé un défi presque insurmontable aux Alliés pour décoder les messages interceptés.
C'est dans ce contexte que le mathématicien et cryptographe britannique Alan Turing a travaillé sur le projet secret d'interception et de décodage des messages allemands, connu sous le nom d'Opération Ultra.
Nous allons explorer les différentes parties de la méthode utilisée pour casser Enigma, en se concentrant particulièrement sur le rôle crucial d'Alan Turing dans cette réussite historique. Nous examinerons tout d'abord comment fonctionnait Enigma, puis nous nous pencherons sur les contributions des cryptologues Marian Rejewski et Henryk Zygalski, qui ont notamment créé le Cyclometer et la Bomba pour aider à décrypter les messages allemands.
Enfin, nous expliquerons comment Alan Turing a utilisé ses connaissances en mathématiques et en informatique pour concevoir une machine électromécanique appelée la "Bombe" qui a permis de casser Enigma. Cette étude de l'histoire de la cryptographie révèle le travail brillant et innovant de Turing et de ses congénères, qui a contribué à la victoire des Alliés dans la guerre contre l'Allemagne nazie.

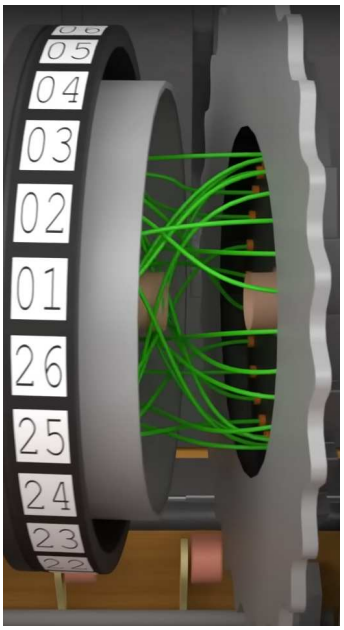
Le craquage d'Enigma a eu un impact majeur sur l'issue de la Seconde Guerre mondiale, car cela a permis aux Alliés d'intercepter et de décoder les messages allemands. Cela a donné aux Alliés des informations précieuses sur les plans et les intentions des forces ennemies, qui ont été utilisées pour prendre des décisions stratégiques cruciales sur le champ de bataille.
Grâce au décryptage des messages d'Enigma, les Alliés ont été en mesure de déjouer de nombreux plans d'attaque allemands, notamment la bataille de l'Atlantique, où les U-boats allemands tentaient de couler des convois de navires alliés transportant des fournitures essentielles. Les Alliés ont également utilisé les informations obtenues par le décryptage pour planifier le débarquement en Normandie en 1944, qui a été l'une des opérations les plus importantes et les plus réussies de la guerre.
En fin de compte, le craquage d'Enigma a permis de sauver des milliers de vies en aidant les Alliés à gagner la guerre. En plus de cela, cela a jeté les bases de la cryptographie moderne et des technologies de l'information qui sont maintenant utilisées dans le monde entier pour protéger les informations et garantir la sécurité des communications.

I Comment fonctionne Enigma

a) Design d’Enigma

Enigma se présentait sous la forme d'une boîte rectangulaire d'environ 30 cm de long sur 15 cm de large et 10 cm de haut, avec un couvercle amovible. Elle avait un clavier avec les 26 lettres de l'alphabet, une série de rotors fixés sur un axe, un tableau de connexions et un plugboard à l'avant de la machine.
Le nombre de rotors utilisés variait selon les modèles, mais la plupart des versions d'Enigma en utilisaient trois.
Le plugboard se trouvait à l'avant de la machine et permettait de connecter des paires de lettres pour échanger leur position.
En plus de ces composants principaux, Enigma avait également des voyants lumineux pour indiquer les lettres de sortie et un réflecteur, qui permettait aux lettres de revenir à travers les rotors avant d'être transmises à nouveau pour une deuxième phase de chiffrement.

b) Les rotors



Les rotors étaient des disques de métal, chacun comportant un anneau de 26 lettres de l'alphabet. Les lettres étaient disposées dans un ordre aléatoire et différent pour chaque rotor. Les rotors étaient fixés sur un axe et pouvaient être tournés pour changer l'ordre des lettres.
Lorsque l'opérateur saisit une lettre sur le clavier, le courant électrique passe à travers les rotors. Les rotors étaient reliés les uns aux autres et à un tableau de connexions, ce qui signifiait que chaque lettre saisie passait par plusieurs rotors avant d'être envoyée au tableau de connexions.
Les rotors tournent à chaque pression de touche, changeant la disposition des lettres pour chaque caractère saisi. Cette rotation a également été programmée pour que le rotor le plus à droite tourne d'un cran à chaque pression de touche.
Ensuite lorsque le rotor avait fait un tour complet il entraîne le rotor suivant d’un cran.

c) Plugboard

Il s'agit d'un panneau situé à l'avant de la machine, sur lequel l'opérateur pouvait brancher des câbles pour connecter des paires de lettres.
En branchant des câbles sur le plugboard, l'opérateur pouvait échanger la place de certaines lettres avant qu'elles ne passent à travers les rotors, augmentant ainsi encore la complexité du chiffrement.

Par exemple, en branchant les câbles pour échanger les lettres "A" et "D", chaque fois que "A" était tapé sur le clavier, le courant électrique passait par le plugboard et la lettre "D" était envoyée à la première rangée de rotors à la place de "A".
Lors du retour du courant, si les lettres “K” et “B” sont échangées, si le “K” est renvoyé par les rotors c’est la lettre “B” qui s'illumine.

Le nombre de connexions possibles sur le plugboard était de 10, ce qui signifiait que 10 paires de lettres pouvaient être échangées avant le chiffrement. Bien que cela puisse sembler peu, cela a considérablement augmenté la complexité du chiffrement et a rendu la machine Enigma encore plus difficile à décrypter.

d) Comment fonctionne Enigma

Le chiffrement d'Enigma est basé sur une série de transformations mathématiques simples mais répétées qui sont effectuées sur chaque lettre du message d'origine avant qu'elle ne soit envoyée à un destinataire. Voici les étapes principales :

1. L'opérateur saisit une lettre sur le clavier. Cette lettre est appelée la lettre claire.

2. La lettre claire est envoyée au plugboard. Si une paire de lettres est connectée par le plugboard, les lettres sont échangées
   .

3. La lettre claire entre ensuite dans le premier rotor. Le rotor est essentiellement une substitution alphabétique, qui échange chaque lettre en entrée avec une autre lettre en sortie. Le rotor tourne d'une position après chaque lettre.

4. Après être passée à travers le premier rotor, la lettre est transmise à travers un deuxième rotor, puis un troisième rotor. Chaque rotor effectue une substitution alphabétique différente et tourne à chaque lettre. Les trois rotors ensemble créent un chiffrement beaucoup plus complexe que tout rotor seul.

5. La lettre chiffre sort du dernier rotor et passe à travers un réflecteur, qui échange la lettre avec une autre lettre.

6. La lettre réfléchie passe ensuite de nouveau à travers les rotors, mais cette fois-ci dans l'ordre inverse. Les lettres sont substituées dans l'ordre inverse, c'est-à-dire qu'elles traversent les rotors de droite à gauche.

7. La lettre finale est envoyée au tableau de connexions, où elle peut être échangée avec une autre lettre. Si une paire de lettres est connectée par le tableau de connexions, les lettres sont échangées.

8. La lettre finale, qui est le résultat du chiffrement de la lettre claire, est envoyée au destinataire.

En résumé, Enigma utilise une série de substitutions alphabétiques et d'échanges de lettres pour transformer les lettres claires en lettres chiffrées. Les rotors tournent après chaque lettre, ce qui ajoute une complexité supplémentaire et rend le chiffrement encore plus difficile à décrypter.

e) Nombre de configuration possible

1. Nombre de rotor, il ya 5 rotors en tout dont 3 dans la machine : 5*4*3. Nous pouvons choisir un des 5 rotors puis il en reste 4, puis 3.

2. Le nombre de positions de départ des rotors : chaque rotor pouvait être réglé sur 26 positions différentes, ce qui signifie qu'il y avait 26x26x26 = 17 576 façons de les disposer.
3. Le nombre de configurations du plugboard : il y avait 10 paires de lettres qui pouvaient être connectées sur le plugboard, ce qui signifie qu'il y avait environ 150 millions de façons de les disposer.

Nous avons donc 60 * 17 576 * 150 738 274 937 250 possibilités, ce qui nous donne $2^{67.1}$.
Si les analystes de Bletchley Park arrivait à tester 1 combinaison par seconde il leur faudrait 290 milliard d'années pour trouver une combinaison, qui est changée tous les jours.

II) Contributions de Marian Rejewski et Henryk Zygalski.

a) Cyclometer

Le cyclomètre était une machine électromécanique utilisée par les cryptanalystes polonais pour casser Enigma. Il a été inventé par Marian Rejewski en 1932.
Le cyclomètre était un appareil circulaire équipé de plusieurs connecteurs électriques autour de sa circonférence. Chaque connecteur correspondait à une lettre de l'alphabet. Il y avait également des contacts électriques sur la face intérieure de l'appareil.
Le fonctionnement du cyclomètre était le suivant : le cryptanalyste saisissait une lettre du message chiffré, puis tournait le disque jusqu'à ce que la lettre soit alignée avec un des connecteurs électriques. Les contacts électriques étaient ensuite utilisés pour connecter le cyclomètre aux rotors de la machine Enigma.
En tournant le cyclomètre, le cryptanalyste pouvait générer une série de combinaisons de lettres. Pour chaque combinaison, le cyclomètre envoyait un courant électrique à travers les

connexions du rotor correspondant sur Enigma. Les courants électriques générés par le cyclomètre étaient enregistrés et utilisés pour tenter de déterminer la configuration de substitution alphabétique utilisée par les rotors.
Le cyclomètre a permis aux cryptanalystes polonais de découvrir la structure interne d'Enigma, y compris le fait que les lettres ne pouvaient pas être cryptées en elles-mêmes, et de trouver des méthodes pour casser Enigma.

b) Feuilles de Zygalski

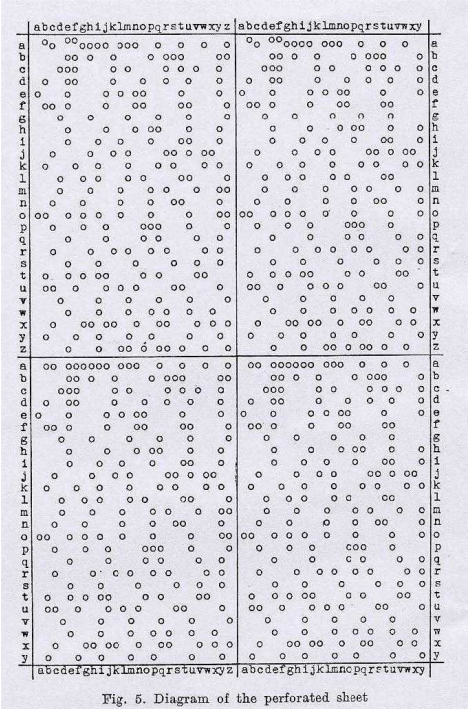


Fig. 5. Diagram of the perforated sheet

Les feuilles de Zygalski étaient un dispositif utilisé par les cryptanalystes polonais pour casser Enigma pendant la Seconde Guerre mondiale. Il a été inventé par Henryk Zygalski en 1938.
Les fiches de Zygalski étaient des feuilles de papier perforées avec des trous disposés en grille. Chaque feuille avait une grille différente, ce qui signifiait que chaque feuille ne pouvait être utilisée qu'une seule fois pour une configuration donnée d'Enigma.
Le fonctionnement des feuilles de Zygalski était le suivant : une fois qu'un message chiffré avait été intercepté, les cryptanalystes plaçaient une fiche de Zygalski sur la machine Enigma pour aligner les trous de la fiche avec les lettres de la machine. Ensuite, ils pouvaient commencer à tester différentes positions de départ pour les rotors jusqu'à ce qu'ils trouvent une configuration qui corresponde au message chiffré.
Les feuilles de Zygalski étaient utilisées en conjonction avec le cyclomètre et d'autres méthodes de cryptanalyse pour casser Enigma. Les feuilles de Zygalski étaient particulièrement utiles pour tester rapidement des configurations de rotors possibles, car elles permettaient aux cryptanalystes de limiter le nombre de configurations qu'ils devaient tester manuellement.
Bien que les fiches de Zygalski aient été utilisées avec succès pour casser Enigma pendant un certain temps, leur utilité a diminué à mesure que les Allemands ont commencé à utiliser des techniques plus avancées pour crypter leurs messages.
Le but est de superposer des feuilles afin de découvrir avec la superposition de trous, une femelle qui permet de découvrir le cycle des rotors.

Dès l’automne 38 l’ajout de plus de permutations de lettres a enterré ces inventions.

c) Bomba

Pour déchiffrer les messages codés, la "Bomba" utilisait une méthode appelée "attaque par force brute". Cela impliquait d'essayer toutes les combinaisons possibles de réglages de la machine Enigma jusqu'à ce que le bon réglage soit trouvé.
La machine "Bomba" était capable de tester environ 17 000 combinaisons par seconde, ce qui était suffisamment rapide pour être efficace dans la découverte des réglages de la machine Enigma.
En utilisant la "Bomba" et d'autres techniques de cryptanalyse, les cryptologues polonais ont réussi à décrypter de nombreux messages de l'armée allemande.
Cette technique fut abandonnée lorsque Enigma fut équipée des deux rotors supplémentaires en Décembre 39.
La disposition des rotors est passée de 3*2*1 possibilités à 5*4*3 devenant impossible à casser par force brute malgré la vitesse apparente de cette technique.

III) Comment Alan Turing a cassé Enigma

a) Les différentes erreurs Allemandes

Repérer les indicateurs : Les "trucs" d'Herivel commencent par l'observation que la machine Enigma a un dispositif appelé "indicateur" qui était utilisé pour initialiser les réglages de la machine. Herivel a remarqué que les opérateurs allemands utilisaient souvent des combinaisons de lettres spécifiques pour réinitialiser l'indicateur.

Utiliser la connaissance des réglages : Une fois que l'indicateur a été identifié, Herivel a utilisé sa connaissance des réglages de la machine Enigma pour déterminer les combinaisons de lettres qui étaient les plus probables d'être utilisées. Par exemple, il a su que certaines lettres étaient rarement utilisées dans certaines positions, et il a utilisé cette connaissance pour réduire le nombre de combinaisons possibles.

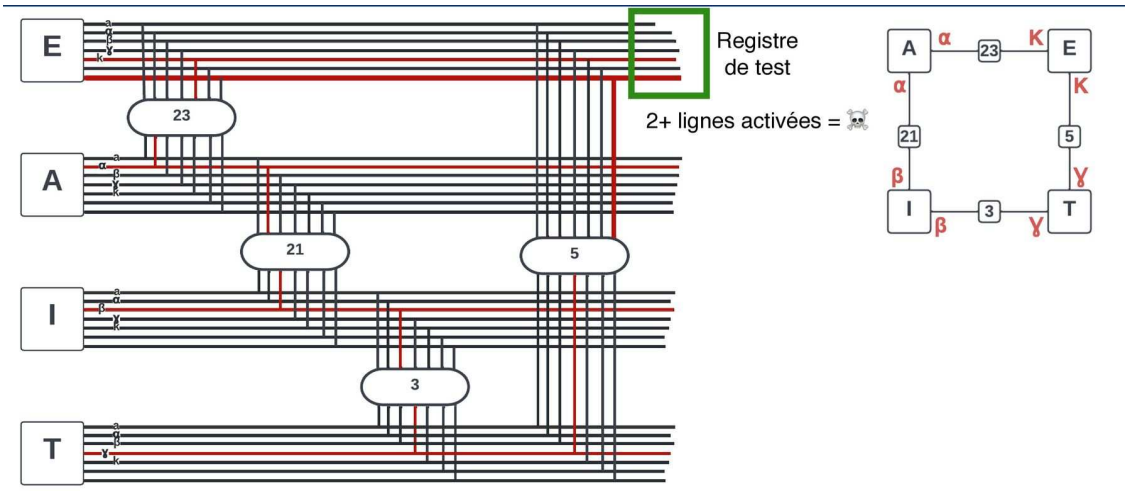
Les cillies : Certains chiffreurs d’ Enigma utilisent toujours plus ou moins la même clef, par exemple les initiales d'un proche. Les Britanniques utilisent le terme « cillies » pour qualifier ces imprudences (à cause d'un chiffreur qui utilisait systématiquement les initiales C.I.L.).

Les CRIBS, traduit par antisèches, sont des : “mots probables”. La rigueur allemande a posé problème car des messages étaient composés de la même manière : la marine allemande envoyait tous les matins un bulletin météo qui contenait un “Heil Hitler” à la fin et “WETTERBERICHT” (TR : bulletin météo).

La machine Enigma possédait une erreur importante : un “A” ne peut pas devenir un “A” etc… Oui une lettre ne peut pas être codé par elle même.

b) La bombe de Turing

La bombe de Turing était une machine électromécanique utilisée pendant la Seconde Guerre mondiale pour casser les codes allemands chiffrés avec la machine Enigma. Elle a été inventée par Alan Turing en 1940.
La bombe de Turing fonctionnait en testant toutes les configurations possibles des rotors de la machine Enigma pour une série de messages chiffrés donnés. Elle utilisait des circuits électriques pour simuler les rotors de la machine Enigma, ainsi que des dispositifs mécaniques pour reproduire les mouvements des rotors.
La bombe de Turing utilisait également les techniques de cryptanalyse et erreurs définies plus haut pour réduire le nombre de configurations de rotors qu'elle devait tester. Elle exploite la faiblesse de la machine Enigma qui garantissait qu'une lettre ne pouvait jamais être chiffrée en elle-même par exemple.
Une fois qu'une configuration de rotor était trouvée, la bombe de Turing utilisait cette configuration pour déchiffrer les messages chiffrés correspondants. Elle enregistrait ensuite les résultats et continuait à tester d'autres configurations de rotor jusqu'à ce que toutes les configurations possibles aient été testées.
La bombe de Turing était une avancée majeure dans la cryptanalyse de l'Enigma, car elle était capable de tester des millions de configurations de rotors en quelques heures seulement. De plus, la configuration d’Enigma permettait de tester des implications à partir d'hypothèses, ce qui accélère le temps de calcul en abandonnant des hypothèses fausses.
La recherche de cycle (créé par les rotors) a été un atout majeur dans la cryptanalyse d’Enigma.



c) Court exemple pratique

Dans cet exemple, nous recherchons le CRIBS “HEIL HITLER” dans la suite codée par Enigma ci-dessus. (L’espace est remplacé par un “X”.)
Nous pouvons déduire le placement du mot en regardant simplement si des lettres se retrouvent doublées et rendent impossible la position actuelle du mot.
Nous allons donc décaler le mot et si son placement semble logique, nous commençons à chercher.

d) Obsolescence

La machine de Turing est devenue obsolète pour plusieurs raisons.
Tout d'abord, les Allemands ont commencé à utiliser des versions plus avancées de la machine Enigma qui étaient plus difficiles à casser. Par exemple, ils ont introduit des réglages de rotor supplémentaires et ont augmenté la longueur des clés de chiffrement, ce qui a considérablement augmenté le nombre de configurations possibles. Cela a rendu la tâche de cassage des codes beaucoup plus difficile et a nécessité des méthodes de cryptanalyse plus avancées.
De plus, l'usage de la bombe de Turing nécessitait beaucoup de temps et de ressources. Les premières versions de la bombe de Turing étaient des machines électromécaniques qui nécessitent des opérateurs humains pour les programmer et les faire fonctionner. Cela rendait le processus de cassage des codes lent et coûteux en termes de temps et d'argent.
Enfin, après la guerre, les méthodes de cryptanalyse ont continué à évoluer rapidement, en particulier avec l'avènement de l'informatique électronique. Les nouvelles machines de cryptanalyse électroniques, telles que les ordinateurs, étaient beaucoup plus rapides et plus efficaces que les machines électromécaniques, comme la bombe de Turing. Cela a rendu la bombe de Turing obsolète dans la cryptanalyse moderne.
En résumé, la bombe de Turing a été un outil important pour casser les codes allemands pendant la guerre, mais elle est devenue obsolète en raison de l'évolution de la technologie et des méthodes de cryptanalyse.

CONCLUSION

En conclusion, Alan Turing était un mathématicien et cryptologue brillant dont les contributions ont été essentielles pour le succès des Alliés pendant la Seconde Guerre mondiale. En utilisant des méthodes novatrices comme les machines "bombes" et la cryptanalyse, Turing a développé une méthode efficace pour briser les codes Enigma utilisés par l'armée allemande. Son travail a permis aux Alliés de décrypter des milliers de messages de l'ennemi, ce qui a eu un impact majeur sur l'issue de la guerre. En raison de ses réalisations, Turing est considéré comme l'un des pionniers de la cryptologie et un héros de la guerre. Cependant, il est important de souligner que la contribution de nombreux autres cryptologues et mathématiciens britanniques et polonais a également été essentielle pour casser les codes Enigma.

Ressources et pour aller plus loin

https://fr.wikipedia.org/wiki/Cryptanalyse_d%27Enigma
How did the Enigma Machine work?
https://fr.wikipedia.org/wiki/Enigma_(machine)
https://www.cryptomuseum.com/crypto/cyclometer/index.htm

Mon code pour recréer Enigma

https://github.com/ElRoulioKFC/testEnigma
https://test-enigma.vercel.app/

Si mon site n’est plus en ligne, il suffit très simplement d’aller sur https://vercel.com/, et de lancer en quelques clics mon répertoire git.
Le site est réalisé en Typescript et utilise le framework REACT.
Si des améliorations sur mon travail sur Enigma voient le jour, notamment une création d’un code recréant le décryptage d’Enigma, il apparaîtra sur mon répertoire.