

2020-2021

BOMBE

Un peu de contexte...

Alain Turing a vécu de 1912 à 1954, ce fut un grand mathématicien et cytoglogue jouant un rôle décisif durant la seconde guerre mondiale, notamment grâce à la réussite du décryptage d'Enigma une machine de cryptage Allemande qui ont permit au allié de lire les messages codés de l'Allemagne Nazi et de raccourcir la guerre de 2ans en sauvant probablement 14 Millions de vies.

Il imagina aussi une machine en 1936 permettant de suivre une liste d'instruction donné grâce à un algorithme et qui serait capable d'écrire ou d'effacer sur un ruban des caractères formels, ce qui donna lieu de nos jours aux ordinateurs

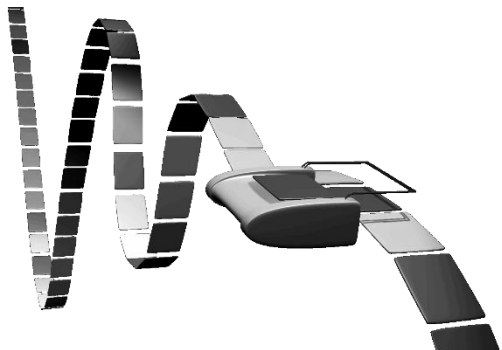


Illustration de la Machine de Turing

Possibilité d'Enigma :

$$\begin{aligned} 5 \times 4 \times 3 &= 60 \\ 26 \times 26 \times 26 &= 17\,576 \\ 60 \times 17\,576 &= 1\,054\,560 \\ \frac{26!}{6! \times 10! \times 2^{10}} \times 1\,054\,560 &= \end{aligned}$$

158 962 555 217 826 360 000

...De Enigma à BOMBE

Enigma est une machine Allemande de chiffrement à la particularité d'être indéchiffrable par un humain, Mais pas par une machine.

Le principe d'Enigma se base sur le principe de substitution qui est de changer une lettre en une autre. Elle est constituée de 3 rotors parfaitement Connectés par un circuit électrique, chaque rotor Vont changer une lettre en une autre puis l'un des Rotors va changer sa position en tournant une fois sur 26 positions différentes.

Les rotors sont choisis parmi 5 rotors rendant les possibilités de déchiffrement gigantesque

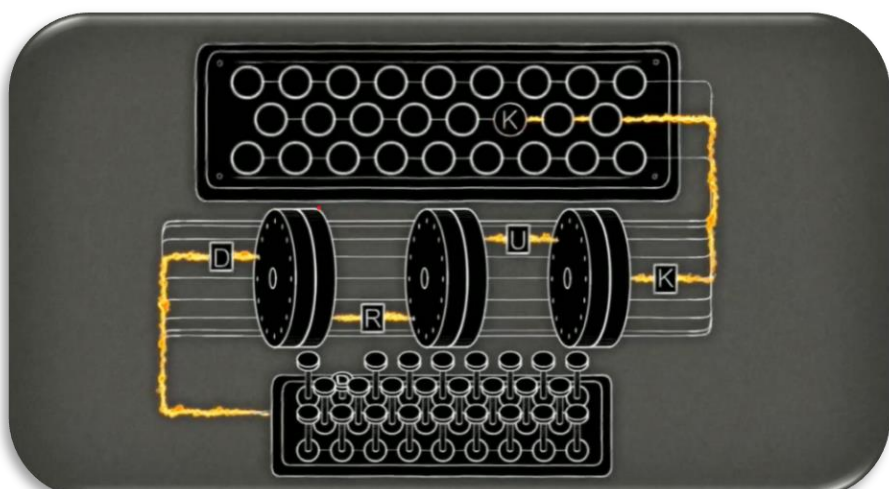


Illustration fonctionnement d'Enigma

Turing la Machine

Turing pris d'admiration par Enigma et eut l'idée d'utiliser une machine contre une autre pour la décrypter.

Il inventa enfin la machine Bombe composée de 36 rotors qui teste toutes les positions possibles des rotors par rapports à un message.

Les rotors sont en colonnes de 3 qui tournent continuellement pour trouver la position initiale des rotors, la machine s'arrête quand elle arrive à coïncider le message codé avec la position des rotors

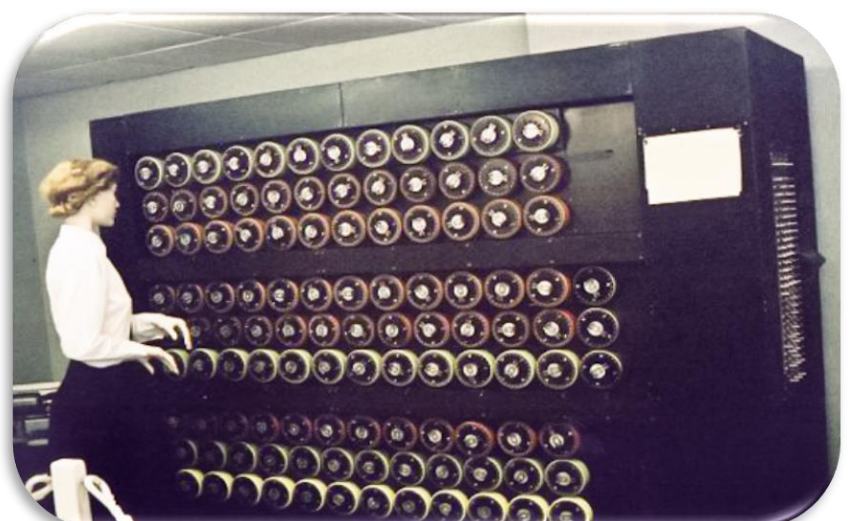


Photo machine Bombe Musée