

LA MACHINE ENIGMA

Histoire d'Enigma

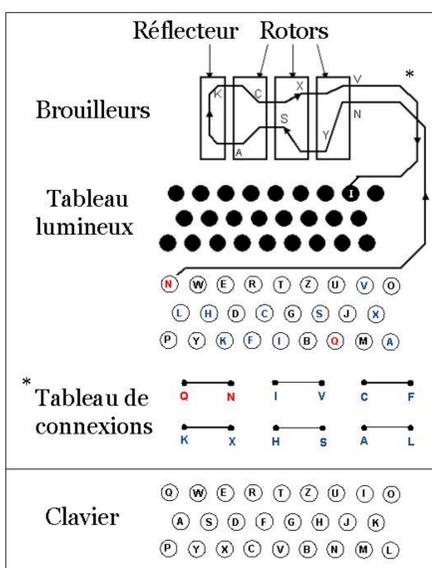


Arthur Scherbius, un Hollandais, et Richard Ritter, un Allemand, inventent la machine Enigma dans les années 1920.

La machine est utilisée par les Allemands dès 1930 et durant toute la deuxième guerre mondiale.



Le fonctionnement d'Enigma



Enigma a plusieurs composants :

- clavier* : pour la saisie du message
- rotor* : trois roues de codage formant le brouilleur
- connections* : un tableau qui échange 6 paires de lettres
- réflecteur* : fait en sorte que pour chiffrer on utilise les mêmes réglages que pour déchiffrer
- panneau* : panneau lumineux qui affiche le message après l'avoir codé.

$$\text{Nombre de clefs: } (26 \cdot 26 \cdot 26) \cdot (3!) \cdot \binom{26}{12} = 169\ 743\ 735\ 200$$

A l'attaque d'Enigma

- D'abord les Polonais s'attaquent à Enigma (Marian Rejewski).
- Les cryptanalystes anglais, environ 3500, se retrouvent à Bletchley Parc, où chaque jour ils essayent de déchiffrer les messages allemands (Alan Turing).
- Après la 2^{ème} guerre mondiale, Bletchley Parc reste secrètement en activité, puis devient un musée.

