— “Enigma et la seconde guerre mondiale”

7 février 2016

Betty Fabre

3. Fonctionnement d’Enigma

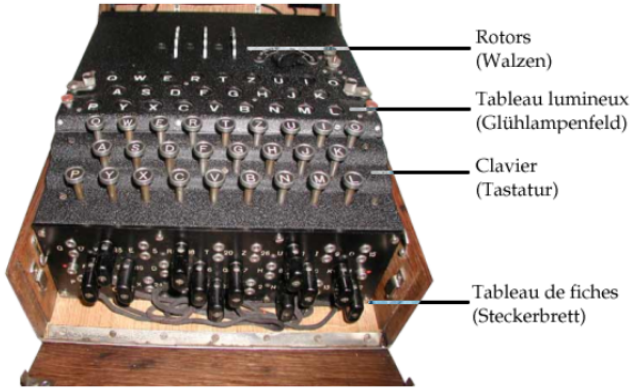
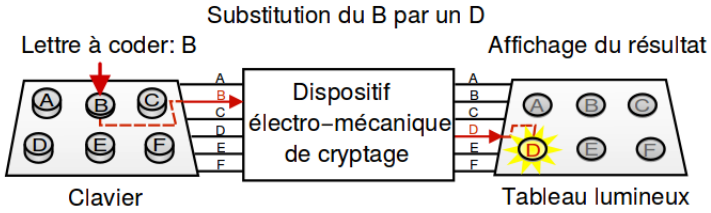


FIG. 3.1.: Les composants d’une machine Enigma standard.



Brouilleur

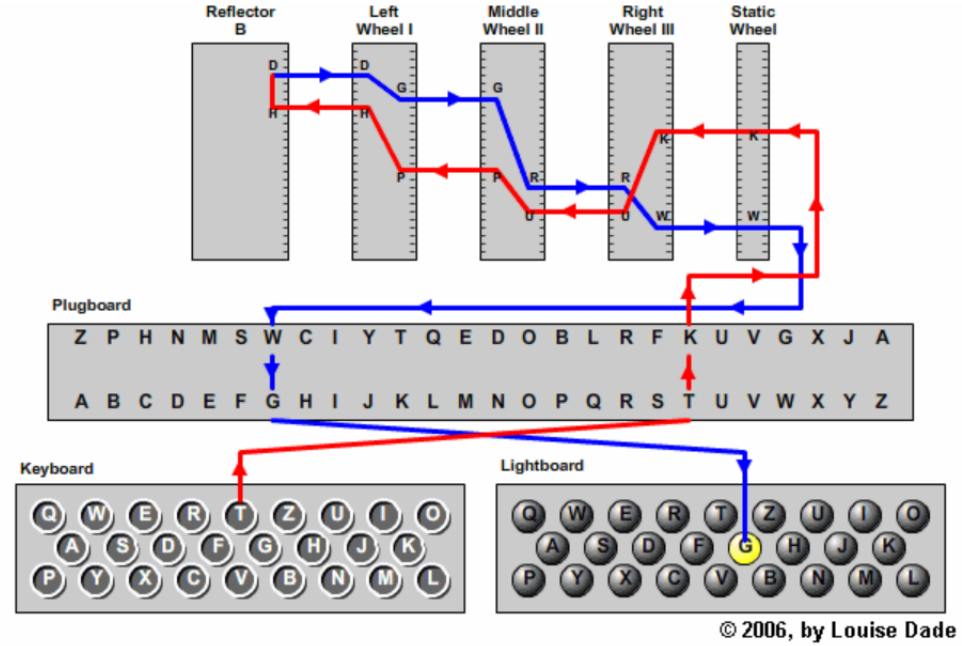
→ 3 rotors → 26 alphabets chacun

→ 1 réflecteur

Rotor Un rotor "rapide" tourne à chaque lettre, le second tourne une fois que le premier a fait un tour complet, et le troisième une fois que le deuxième a fait un tour complet.

Chaque rotors a un câblage donné.La machine possède 5 rotors mais n’en utilise que 3.

Réflecteur Le réflecteur assure la symétrie des alphabets à une position donnée. Attention, le réflecteur entraîne qu’une lettre ne peut pas se coder elle-même.



La clé du jour

La clé possède plusieurs infos:

→ les 3 rotors et leur ordre

→ le placement de la bague , elle introduit un décalage dans la position des rotors, mais n'est pas très importante pour décrypter.

→ les couples de lettres inchangées et donc les fiches à positionner sur le tableau des fiches. 10 fiches sont branchées.

→ la composante propre au message → l'orientation des rotors

6. Le décryptage d'Enigma

L'indice de coïncidence

→ permise par la puissance des *ordinateurs*
outil linguistique : *indice de coïncidence*

Indice de coïncidence: proba que 2 lettres dans un texte soient identiques. → on compte toutes les apparitions pour toutes les lettres de l'alphabet + loi binomiale.

Décryptement pas à pas d'un message

Cryptanalyse d'un message :

→ quels rotors sont utilisés ?

→ orientation initiale ?

→ quelles fiches sont reliées sur le tableau de fiches?

On teste les 60 façons possibles de placer les rotors. On garde celui pour lequel l'indice de coïncidence est le plus grand comme réglage initial des rotors.

Quelles fiches branchées ? → Cryptogramme partiellement décrypté grâce à l'odre et la position des rotors. On y cherche des morceaux de texte clair.

On branche des lettres par intuition.

On continue jusqu'à avoir un texte décrypté.