La machine Enigma

sv

March 24, 2026

Pourquoi chiffrer des messages ?

Pendant une guerre, les armées doivent transmettre des messages secrets.

- messages militaires
- informations stratégiques
- communications radio interceptables

Pendant la Seconde Guerre mondiale, l'Allemagne utilise une machine appelée **Enigma**.

La machine Enigma

Enigma est une machine électromécanique utilisée pour chiffrer des messages.
Elle possède :

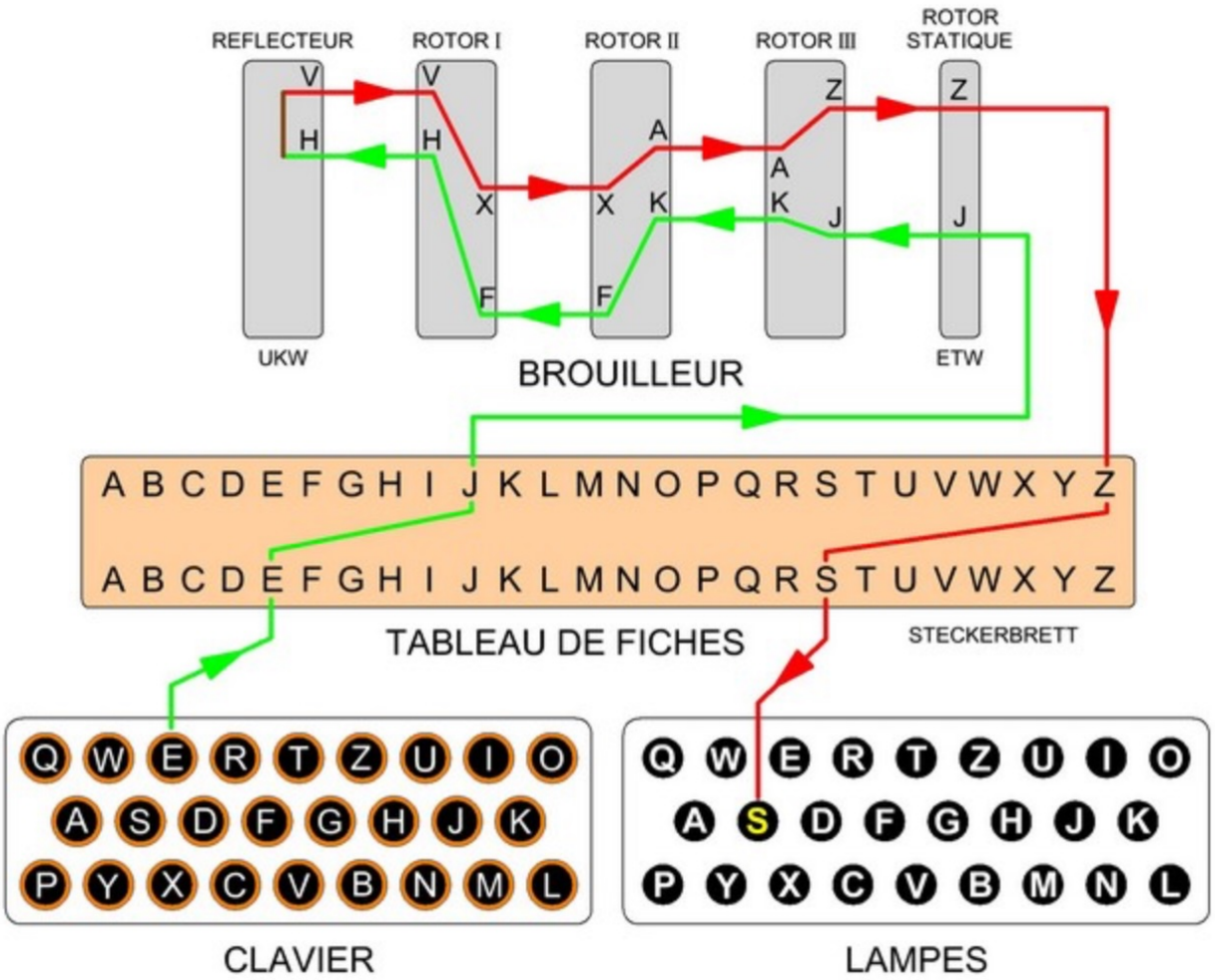
- un clavier
- des lampes pour afficher les lettres
- plusieurs rotors
- un système de connexions appelé *plugboard*

Quand on appuie sur une lettre, une autre lettre s'allume.

La machine Enigma

Vikidia Enigma

Le principe de l'Enigma



apprendre-en-ligne.net

Principe du chiffrement

Enigma réalise une **substitution**.
Exemple simple :

$$\begin{aligned} A &\rightarrow D \\ B &\rightarrow M \\ C &\rightarrow Q \end{aligned}$$

Mais avec Enigma, la substitution change **à chaque lettre**.

Pourquoi est-ce compliqué ?

Chaque fois qu'une lettre est tapée :

- les rotors tournent
- le chiffrement change

Donc :

A peut devenir G, puis T, puis L.

Le même message chiffré deux fois donnera un résultat différent.

Les rotors

Les rotors sont le cœur de la machine.
Chaque rotor réalise une permutation de l'alphabet.
Caractéristiques :

- plusieurs rotors
- ordre configurable
- position initiale
- rotation après chaque lettre

Cela produit un très grand nombre de clés possibles.

Le plugboard

Avant et après les rotors, il existe un système appelé **plugboard**.
Il permet d'échanger des lettres.
Exemple :

$$A \leftrightarrow M$$
$$G \leftrightarrow T$$

Cela ajoute encore plus de complexité au chiffrement.

Une propriété étonnante

Dans Enigma :

> Une lettre ne peut jamais être chiffrée en elle-même.

Par exemple :

- A ne peut jamais devenir A

Cette propriété aidera plus tard les cryptanalystes.

Casser Enigma

Les Alliés ont réussi à casser le code Enigma.
Ils utilisent :

- des mathématiques
- des machines de calcul
- des erreurs humaines

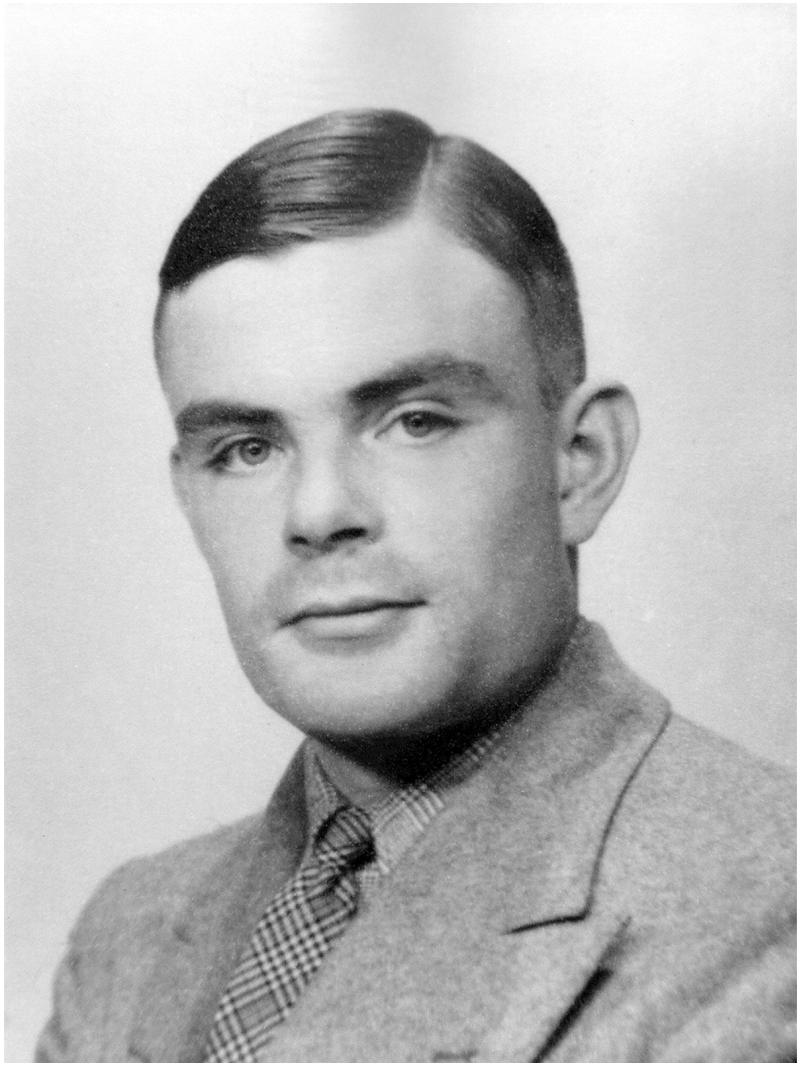
Les cryptanalystes

Des mathématiciens ont joué un rôle important :

- Alan Turing
- Marian Rejewski

Ils travaillent dans un centre secret appelé Bletchley Park.

Alan Turing



La machine Bombe

Pour aider à casser Enigma, les Alliés construisent une machine appelée **Bombe**.
Son objectif :

- tester rapidement de nombreuses clés
- trouver les réglages de la machine Enigma

Impact historique

Le décryptage d'Enigma permet :

- de lire les messages allemands
- de connaître certaines stratégies militaires

Les historiens pensent que cela a raccourci la guerre de plusieurs années.

Conclusion

La machine Enigma montre que :

- un système peut sembler très sécurisé
- les mathématiques jouent un rôle crucial
- la cryptanalyse est essentielle

Aujourd'hui, la cryptographie est utilisée partout :

- internet
- paiements
- messageries sécurisées