ARBORESCENCE

CRYPTOGRAPHIE

La machine Enigma

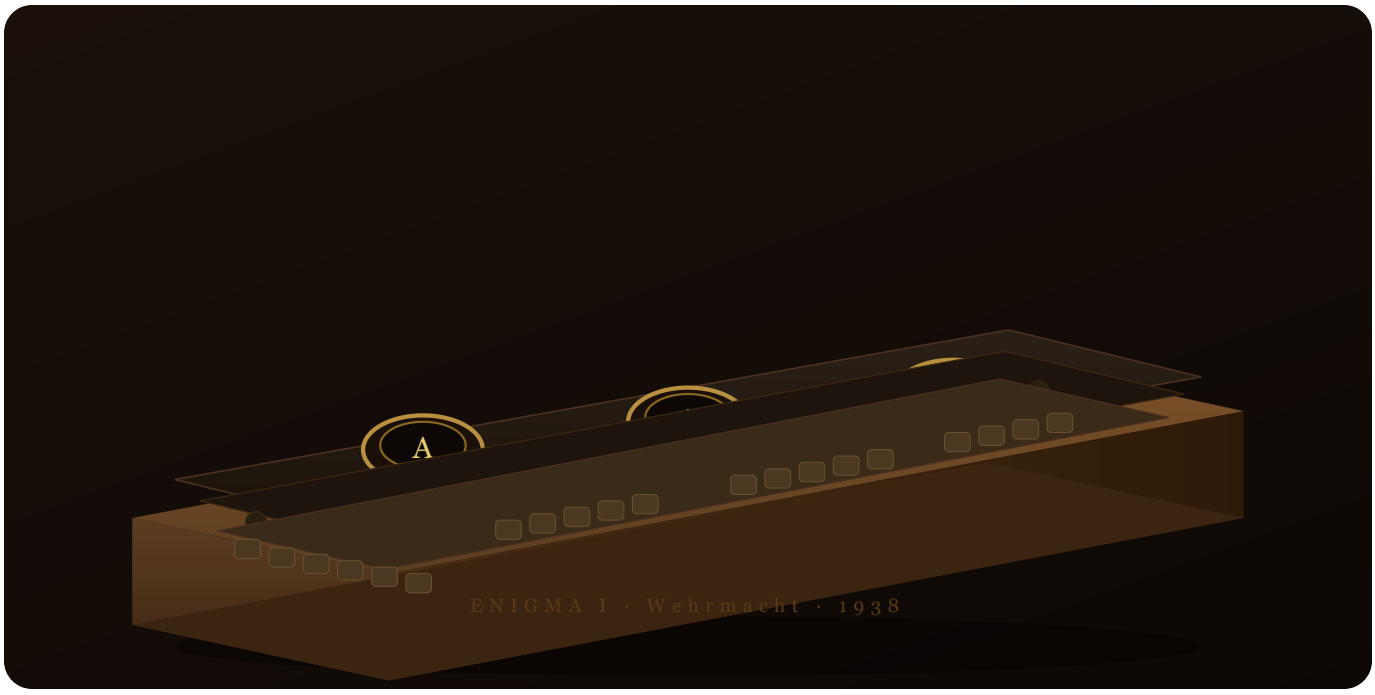
Comment les nazis chiffraient leurs messages — et comment Alan Turing les a cassés. Avec un simulateur interactif fidèle à la machine originale.

5 min · interactif | Dès 10 ans | Fiche C1

01 Objectif

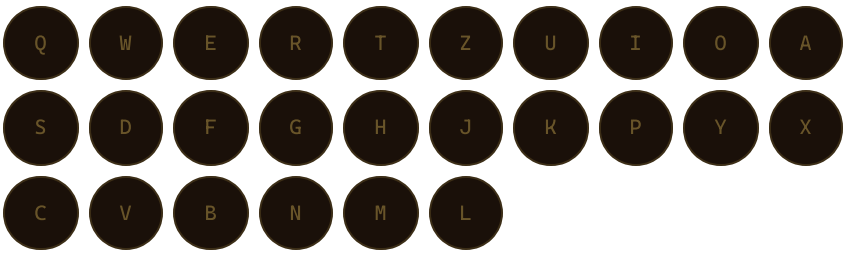
À la fin de cette séquence : expliquer le principe d'un chiffrement à rotors, comprendre pourquoi Enigma était considérée incassable, et simuler le chiffrement d'un message.

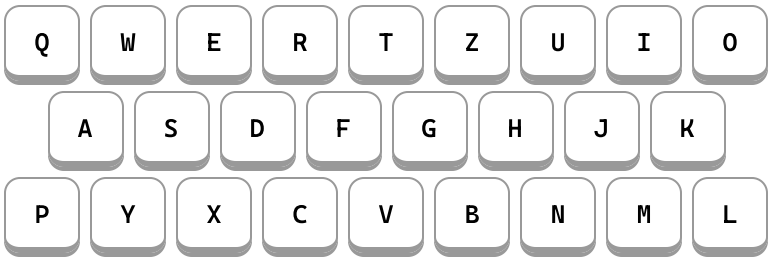
02 La machine — jouez avec



ROTOR I ROTOR II ROTOR III

Frappez une touche ou tapez au clavier





TEXTE EN CLAIR (OU CHIFFRÉ)

TAPEZ ICI

SORTIE CHIFFRÉE

LA SORTIE APPARAÎT ICI

ROTOR I I

ROTOR II II

ROTOR III III

↺ Réinitialiser

✕ Tout effacer

03 L'essentiel

Un chiffrement qui se transforme à chaque lettre

Les anciens chiffrements (César, Vigenère) remplacent toujours A par la même lettre. Enigma tourne ses rotors à chaque frappe : la première lettre et la deuxième ne subissent pas le même codage. C'est ce qui le rendait, a priori, indéchiffrable sans la machine.

Trois rotors qui avancent comme un compteur kilométrique

Le rotor de droite tourne à chaque touche. Quand il a fait un tour complet, il entraîne le rotor du milieu, qui entraîne à son tour le rotor de gauche. Plus de 150 000 positions distinctes possibles avant de se répéter.

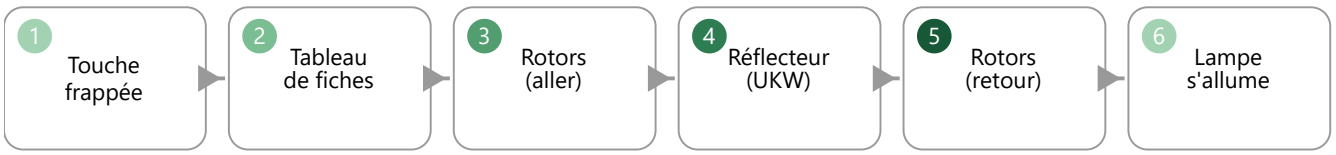
Le réflecteur — la faille fatale

Le signal repart en sens inverse via un réflecteur fixe. Conséquence : A ne peut *jamais* s'encoder en A. Les équipes de Bletchley Park ont exploité cette propriété pour réduire l'espace de recherche de 10^{23} à des milliers de cas testables par machine.

Alan Turing et la Bombe

En 1940, Turing conçoit une machine électromécanique — la Bombe — qui exploite les répétitions prévisibles des messages (météo, formules rituelles) pour tester des milliers de réglages par minute. Enigma est cassé en 1941. La guerre est raccourcie d'au moins deux ans selon les historiens.

04 Le schéma — chemin du signal



Le signal traverse deux fois les rotors — aller et retour — via le réflecteur. Chaque frappe avance au moins un rotor : la même touche frappée deux fois de suite produit deux lettres différentes.

05 Alan Turing & Bletchley Park

1918

Invention par Arthur Scherbius

La machine est d'abord commerciale — banques et diplomatie. L'armée allemande l'adopte et la modifie profondément.

1932

Marian Rejewski casse la version commerciale

Le mathématicien polonais analyse des messages et retrouve le câblage interne des rotors grâce à une répétition d'indicateur introduite par erreur de procédure. Première grande victoire.

1939

Les Polonais transmettent leur savoir aux Alliés

Trois semaines avant l'invasion, les services polonais partagent leurs méthodes avec la France et le Royaume-Uni. Sans ce geste, Bletchley Park partirait de zéro.

1940

La Bombe de Turing entre en service

Basée sur les Bombes polonaises de Rejewski, la version de Turing et Gordon Welchman teste 17 000 réglages par heure. Elle exploite la propriété qu'Enigma ne code jamais une lettre en elle-même.

1941–45

Ultra — le secret le mieux gardé de la guerre

Les messages allemands sont lus en quasi-temps-réel, mais Churchill impose de ne jamais révéler la source. Des convois sont parfois sacrifiés pour ne pas alerter l'ennemi que le code est cassé.

1974

Le secret est enfin levé

Trente ans après la fin de la guerre, le gouvernement britannique déclassifie l'opération Ultra. Le monde découvre l'ampleur du travail accompli à Bletchley Park.

06 Jeu — Opération Ultra

🎯 MISSION DE DÉCHIFFREMENT

Un message ennemi vient d'être intercepté

Les renseignements confirment que les réglages de la machine étaient : **Rotors I–II–III, position de départ A–A–A**, sans tableau de fiches.

Réinitialisez la machine avec ces réglages (c'est le réglage par défaut), **tapez le message chiffré ci-dessous** dans le simulateur, et lisez la sortie.

```
FUVBY CQMHZ WJTKL
```

Indice : c'est une phrase de trois mots en anglais, la langue des communications militaires alliées interceptées pour l'exercice.

✓ Valider mon déchiffrement

07 À retenir

- **Jamais la même lettre que soi-même** : A ne s'encode jamais en A. Bletchley en a fait la première faille à exploiter.
- **Le réglage change chaque jour** à minuit selon un livre de codes mensuel. Capturer ce livre était une priorité militaire absolue.
- **La Bombe de Turing** n'est pas un ordinateur : c'est une machine dédiée à parcourir les réglages possibles, exploitant les fautes d'inattention des opérateurs.

08 Exercice

Sur le simulateur, chiffrez le mot ENIGMA (position de départ A–A–A). Notez le résultat. Réinitialisez, puis rechiffrez ce résultat avec exactement les mêmes réglages. Que se passe-t-il ? Expliquez pourquoi.

Indice — La machine est symétrique : chiffrer la sortie avec les mêmes réglages redonne l'entrée. C'est à la fois sa force (pas besoin d'un déchiffreur séparé) et l'une de ses faiblesses structurelles.

09 Vérification des acquis

▶ **Pourquoi Enigma était-elle considérée incassable ?**

▶ **Qu'est-ce que la faiblesse du message prévisible ?**

▶ **Vrai ou faux : Enigma pouvait chiffrer A en A.**

Chaque fiche est autonome et conçue pour être imprimée (mise en page papier optimisée).