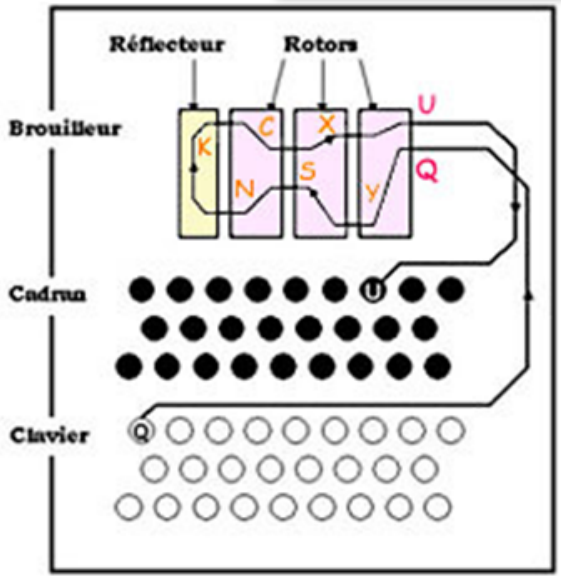
ENIGMA

10 millions de milliards de clés



ENIGMA

La première version d'ENIGMA était utilisée comme suit.

Agencement des 3 rotors.
123, 132, 213, 231, 312, 321
6 possibilités.

Position des trois rotors, 3 lettres.
26x26x26=17 576 possibilités.

Connexions des fiches (6 connexions).
100 391 791 500 possibilités.

Exemple de clef: (231,DFT,AD,BE,CM,FY,UI,LP)

Nombre total de clefs:
6 * 17 576 * 100 391 791 500=10 586 916 764 424 000
10 million de milliard de possibilités…

Briser ENIGMA

Sur une période de 10 ans, les Allemands se dotèrent de plus de 30 000 machines ENIGMA.

ENIGMA est un véritable cauchemar pour les cryptanalystes.

Toute attaque statistique est inutile puisque chaque lettre du message est chiffré de façon différente.

Inutile d'essayer de deviner la clef. Il y en a trop.

La plupart des cryptanalystes abandonnèrent rapidement espoir de briser ENIGMA. Il y avait une exception. Les Polonais avaient peur d'une invasion Allemande. Pour eux, briser ENIGMA était vitale.

Briser ENIGMA

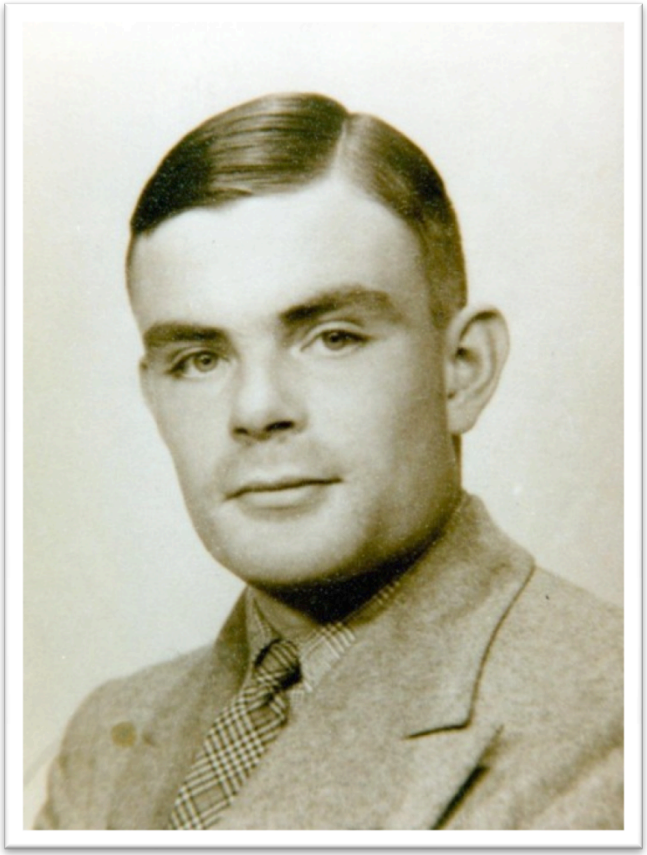
Les services de renseignement polonais ont obtenu par l'intermédiaire d'un informateur une description de la machine, ainsi que son mode d'utilisation.

Un livre de code donnait pour chaque jour la clef utilisée. Pour éviter que tous les utilisateurs d'ENIGMA utilisent la même clef, l'opérateur choisissait trois lettres au hasard qu'il chiffrait avec la clef du jour, deux fois. Ensuite la position des rotors était modifiée en fonction de ces trois lettres.

Chaque message était donc chiffré avec une clef différente.

Briser ENIGMA
1932-1944

Marian Rejewski
Polonais



Alan Turing
Britannique

Briser ENIGMA

Marian Rejewski

Le code ENIGMA fut brisé en décembre 1932 par Marian Rejewski, travaillant pour les services de renseignement polonais. A partir de 1933, les Polonais ont réussi a déchiffrer des milliers de messages allemands.

Les Polonais on réussi là ou les autres services de renseignement ont échoué.

Briser ENIGMA

La clef du succès de Marian Rejewski fut de se concentrer sur le fait que chaque message commençait par une répétition de 3 lettres.

Par exemple, pour quatre messages interceptés, on pouvait obtenir les données suivantes:

LOKRGM
MVTXZE
JKTMPE
DVYPZX

Chacun de ces chiffres dépend de l'agencement des rotors, du positionnement des fiches et bien sûr, des trois caractères choisis. Examinons la première et la quatrième lettre.

ABCDEFGHIJKLMNOPQRSTUVWXYZ
P M RX

Briser ENIGMA

Avec l'interception de plusieurs messages, on peut compléter le tableau.

ABCDEFGHIJKLMNOPQRSTUVWXYZ
FQHPLWOGBMVRXUYCZITNJEASDK

Ce tableau dépend de la clef du jour. Marian eu une intuition remarquable.

A-F-W-A	3 LIENS
B-Q-Z-K-V-E-L-R-I-B	9 LIENS
C-H-G-O-Y-D-P-C	7 LIENS
J-M-X-S-T-N-U-J	7 LIENS

Le même exercice peut être réalisé avec les lettres numéro 2 et 5, ainsi que 3 et 6. Marian remarqua que la longueur des chaînes changeait à chaque jour. Si on change la position des fiches, les lettres des chaînes vont changer mais pas leurs longueurs. La longueur des chaînes ne dépend que de la position des rotors.

Briser ENIGMA

Il existe 6 x 26^3= 105 456 positionnements des rotors. Chacun donne lieu a une liste de chaînes avec des tailles caractéristiques. En une année, Marian réussit a construire une table de toutes les possibilités. Pour identifier la position des rotors, il suffisait d'intercepter quelques messages, calculer la longueur des chaînes, et regarder dans la table.

Il restait maintenant à trouver la position des fiches. Une fois les rotors bien positionnés, si on laisse le tableau des fiches vierge, l'opération de déchiffrement donnera un message illisible mais facile à briser. Les lettres sont simplement permutées suivant la position des fiches. Une attaque statistique trouve facilement les branchements.

ENIGMA et Turing

Alan Turing
Britannique

Un peu avant l'invasion allemande, les Polonais on dévoilé leurs techniques pour briser ENIGMA aux Britanniques. La partie n'était pas complètement gagnée. ENIGMA fut modifié durant la guerre. Des rotors furent ajoutés et à un certain moment, les Allemands ont cessé de répéter les trois lettres de la clef. Il y eut donc de courtes périodes pendant lesquelles les Alliés furent incapables de déchiffrer les messages allemands, mais des techniques de plus en plus sophistiquées et un appareillage électrique de plus en plus imposant leur permirent de déjouer les cryptographes allemands.