

## La machine Enigma

La machine cryptographique Enigma est une des illustrations du rôle majeur de la science et de la technologie dans les guerres du XX<sup>e</sup> siècle.

### L'objet lui-même...

La cryptographie est l'activité qui consiste à rendre un message inintelligible afin de protéger des données. Les procédés généralement utilisés sont la modification de l'ordre des signes et le remplacement de ceux-ci par d'autres signes. Le cryptage réalisé par les Enigma allemandes repose sur ces principes.

Enigma a l'apparence d'une machine à écrire : comme cette dernière, elle est munie d'un clavier dont chaque touche est surmontée d'une lettre. Sur la partie supérieure de l'appareil, on distingue en outre d'autres lettres incluses chacune au sein d'un médaillon. Celui-ci est en réalité un voyant qui peut devenir lumineux.



1 Machine Enigma.  
Inv. : DEP 4509  
© Paris, musée de l'Armée  
/ RMN-GP.

Le fonctionnement d'Enigma nécessite la présence de deux opérateurs. Le premier opérateur tape le message à transmettre à l'aide du clavier. À chaque pression sur une touche, plusieurs cylindres situés à l'intérieur de la machine effectuent une rotation à l'issue de laquelle une lettre de substitution apparaît sur le voyant éclairé ; cette lettre de remplacement est prise en note par le deuxième opérateur. La lettre de substitution varie à chaque fois : un N devient par exemple un P la première fois, un D la fois suivante, un R au bout de la troisième fois. Pour un mot de trois lettres, des millions de combinaisons sont donc possibles. Transmis en morse, le message reçu est décodé par une deuxième machine Enigma, associant elle aussi deux opérateurs.

### L'objet nous raconte...

Enigma est la copie allemande d'une machine d'origine hollandaise. Destiné initialement à un usage commercial, cet appareil d'un genre entièrement nouveau intéresse les militaires et Hitler le fait développer à partir de 1934. L'armée de terre, la marine et l'aviation du III<sup>e</sup> Reich en font rapidement leur instrument privilégié de transmission de messages secrets car il est jugé inviolable. Peu avant le déclenchement de la seconde guerre mondiale, les services secrets polonais, français et britanniques parviennent cependant à mettre au point des méthodes de décryptage efficaces. Ces dernières doivent beaucoup aux recherches d'un mathématicien juif polonais, connu sous le nom d'emprunt de Lewinski.

En janvier 1939, afin de coordonner les efforts des différents services alliés, un centre spécialisé dans le décodage des Enigma est installé en janvier 1939 à Bletchley Park, au nord de Londres.

Le décryptage des Enigma montre son efficacité tout au long de la guerre et constitue un avantage certain en faveur des Alliés ; il les aide à anticiper certaines actions de l'ennemi. Pendant la bataille d'Angleterre de l'été 1940 par exemple, les Britanniques, qui disposent également du radar, sont ainsi remarquablement informés sur les raids aériens de la Luftwaffe.

Sur le plan technologique surtout, la machine Enigma est à l'origine des premiers pas de l'intelligence artificielle. Depuis la fin de l'année 1938, les Britanniques travaillent à la construction d'un appareil de décodage automatique baptisé « la Bombe ». Cet instrument est mis au point à partir des concepts développés par un jeune mathématicien, Alan Turing (1912-1954). Une machine de décodage plus puissante est cependant nécessaire car les Allemands transmettent, au cours de la guerre, près de 10 000 messages Enigma par jour. Ce nouvel outil découle lui aussi des travaux de Turing, élève d'Einstein à Princeton. Il s'agit d'un calculateur électronique de grande taille, appelé pour cette raison Colossus. Alimenté par câbles, Colossus effectue les opérations de déchiffrement en suivant une logique abstraite et universelle ; il est également capable de programmer d'autres machines et de s'arrêter lui-même après avoir inscrit ses résultats sur un ruban de papier. L'ordinateur est né.

L'existence de Colossus et des autres machines similaires n'est connue que depuis le début des années 1970. Détruit en 1945 sur ordre de Churchill, Colossus a été reconstruit en 1999. Quant à la plupart des scientifiques ayant travaillé sur ce projet, ils furent victimes de la raison d'État britannique. Turing, que l'on tenta de faire passer pour un déséquilibré, est ainsi condamné pour homosexualité et se suicide en 1954.

