

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^e siècle.



Machine cryptographique allemande de type Enigma, © Musée de l'Armée / RMN-GP 08-509639

CHRONOLOGIE



1-3 SEPTEMBRE

1939

L'armée allemande envahit la Pologne. Français et Britanniques se mobilisent et déclarent la guerre à l'Allemagne.

17 JUIN

1940

Pétain demande l'armistice. Le lendemain, depuis Londres, le général de Gaulle lance un appel à poursuivre les combats.

22 JUIN

1941

Après 2 années d'entente, Hitler s'en prend à l'Union soviétique (opération *Barbarossa*).

7 DÉCEMBRE

1941

Attaque aéronavale japonaise contre la flotte américaine de Pearl Harbor. Les États-Unis entrent en guerre contre le Japon (8/12) et l'Allemagne (11/12).

20 JANVIER

1942

Conférence de Wannsee, programme nazi d'extermination des juifs d'Europe, la « solution finale ».

2 FÉVRIER

1943

Capitulation allemande à Stalingrad sur la Volga.

6 JUIN

1944

Débarquement allié en Normandie (opération *Overlord*). Le front de l'Ouest est ouvert.

8 MAI

1945

Capitulation sans condition du III^e Reich à Berlin quelques jours après la prise de la ville.

6-9 AOÛT

1945

Explosion d'une bombe atomique sur la ville japonaise d'Hiroshima, suivie d'une seconde sur Nagasaki.

2 SEPTEMBRE

1945

Signature de la capitulation sans condition de l'Empire Nippon: la Seconde Guerre mondiale est terminée.

L'objet en 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 machines *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. 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^e Reich en font rapidement leur instrument privilégié de transmission de messages codés 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 colonel français Bertrand, actif dans le renseignement dès le début des années 1930, comprend l'importance de la cryptanalyse dans le contexte des futures hostilités. Avec l'avènement de la guerre et l'occupation allemande de la France, Bertrand continue ses efforts de renseignement, travaillant dans l'ombre pour collecter des informations sur les opérations ennemies. Une partie cruciale de son travail est la collecte d'informations sur la machine *Enigma* et ses codes. Les forces françaises réussissent à obtenir des exemplaires d'*Enigma* et des documents connexes grâce à des opérations de renseignement et à des actes de résistance. 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 10000 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.

Notice

→ **Numéro d'inventaire**
4509 DEP

→ **Création**
Berlin, Allemagne

→ **Période**
XX^{ème} siècle, Europe - période
contemporaine de 1914 à nos jours

→ **Dimensions**
Hauteur : 15 cm, Largeur : 25 cm,
Profondeur : 35 cm

→ **Mots-clés**
Armée allemande, cryptographie,
époque de la Seconde Guerre
mondiale, espionnage

→ **Localisation**
Département des deux guerres
mondiales – Salle Leclerc

Bibliographie

Enigma, D. TURING, Nouveau Monde
Ed., 2019, 406p

Alan Turing ou l'énigme de l'intelligence,
A. HODGES, Payot, 2004, 437p