Enigma: La machine à crypter de la seconde guerre mondiale

Notre curiosité du jour est une Enigma, une machine utilisée par les Allemands pendant la seconde guerre mondiale pour envoyer des messages codés puis les décrypter. Arthur Scherbius (1878-1929), le fondateur de l'entreprise Scherbius & Ritter et l'inventeur du rotor (une roue de code câblée), enregistre un premier brevet à Berlin, le 23 février 1918 (numéro Sch 52638 IX/42n).

Il n'est pas le seul à travailler sur ce type de mécanisme et un second brevet est déposé le 7 octobre 1919, par l'ingénieur hollandais Hugo Alexander Koch (1870-1928).
Au début, la machine n'est pas destinée à un usage militaire, mais aux grandes entreprises qui souhaitent protéger leur correspondance. La Securitas-Werke A-G se porte acquéreuse des licences commerciales de la machine et en confie l'exploitation, à une société par actions, la Chiffriermaschinen A-G. Le premier modèle, l'Enigma-A, est produit à partir de 1923. Elle se présente comme une machine à écrire portative composée d'un clavier, où chaque touche illumine un voyant portant une lettre, et d'un jeu de disques rotatifs appelés « rotors » pour le codage. Le mouvement des rotors permet de permuter les lettres plusieurs fois et d'obtenir des transformations cryptographiques différentes à chaque pression sur une touche. Pour des machines Enigma équipées de 26 lettres, il existe 17 576 combinaisons et, pour déchiffrer les messages, il faut connaître la séquence d'encodage choisie par l'opérateur. Néanmoins son prix est plutôt élevé (30000 euros aujourd'hui) et le succès commercial se fait attendre.

Dans les années qui suivent plusieurs versions de la machine sont mises au point, dont le fameux modèle D, qui s'exporte en Hollande, en Suède, en Pologne, en Angleterre, en Italie, en Espagne, au Japon et aux Etats-Unis. La Reichsmarine, la marine allemande, l'adopte dès 1926. En juin 1930, le modèle I, une machine à vocation militaire, entre en service. Dès lors, l'usage de l'Enigma est étendue à toute l'armée allemande (la Reichswehr, la Reichsbahn, la Luftwaffe, la Wehrmacht...) et aux services de renseignements militaires (l'Abwehr). La Regia Marina italienne adopte, quant à elle, un modèle commercial D, à l'instar des troupes nationalistes espagnoles pendant la guerre civile (1936-1939), tandis que qu'une Enigma T (Tirpitz) est fabriquée pour le Japon.

Les ingénieurs allemands apportent plusieurs modifications à la machine afin de garantir la sécurité du système d'encodage. Néanmoins, on sait aujourd'hui que les mathématiciens et le Bureau de Chiffrage Polonais sont en mesure de décrypter les messages (réputés incassables) de l'Enigma dès 1933. En effet, pour réduire les erreurs liées aux interférences radios, les opérateurs allemands doivent-ils transmettre la séquence d'encodage deux fois... une aubaine pour les Alliés! Des centres de décryptages sont également créés en France (Opération Z) et en Angleterre, qui s'équipent de répliques de la machine Enigma. En 1940, le programme britannique, surnommé Alan Turing Spearhead Ultra (le mathématicien Alan Turing en dirige les travaux) est déjà capable de décrypter une bonne partie des messages allemands.
En février 1942, l'arrivée d'un modèle plus perfectionné, Enigma M4, change la donne puisqu'il prive les Alliés d'informations sur les projets ennemis. Il faut, en effet, attendre près d'une année avant qu'ils ne parviennent à casser le système d'encodage.

Au total, on évalue le nombre maximal de machines en service, durant la guerre, autour de 60 000 exemplaires. Durant cette période, les Alliés décryptent quotidiennement 18 000 messages. Le dernier connu est celui de l'Amiral Doenitz, annonçant : « Le Führer est mort. Le combat continue ».

Sources: Centre Français de Recherche sur le Renseignement et Secondeguerre.net
Images: Daniel Terdiman/CNET

Par

Publié sur Cafeduweb - Historizo le lundi 6 septembre 2010
Consultable en ligne : http://historizo.cafeduweb.com/lire/11988-enigma-machine-crypter-seconde-guerre-mondiale.html