Communiqué de presse

Le mythe Enigma

La conférence retrace l'histoire de cette machine

Depuis des millénaires, les rois, les empereurs et les généraux ont dû se doter de moyens de communication efficaces pour commander leurs armées. Ils étaient conscients des risques encourus si leurs messages tombaient dans les mains d'un ennemi. Cela les a incités à créer des codes afin que seul le destinataire des messages puisse les lire. Ainsi, dans un souci de confidentialité, les nations ont créé des services secrets chargés d'assurer la sécurité des communications par la mise en place des meilleurs codes possibles.

Jules César a inventé la substitution *mono-alphabétique*. Au XVI[e] siècle, Blaise de Vigenère va mettre au point un chiffre plus efficace : la substitution *polyalphabétique*. Il a imaginé d'utiliser non plus un alphabet chiffré mais plusieurs. Son système, très efficace, n'a été brisé qu'au XIX[e] siècle par Charles Babbage.

Au début du XX[e] siècle, les cryptologues imaginent des dispositifs automatiques pour permettre un cryptage par substitution polyalphabétique. Des inventeurs ont commencé à mettre au point des machines de chiffrement électromécaniques ayant pour principe la génération de nombreux alphabets chiffrés grâce à des cylindres rotatifs que traversent des circuits électriques.

La machine à coder Enigma

La machine a été inventée par Alexander Koch en 1919. Il a vendu son brevet à Arthur Scherbius qui voulait la commercialiser pour protéger les entreprises de l'espionnage commercial et industriel. Enigma fut adoptée par la *Reichsmarine* en 1926 puis par la *Reichswehr* en 1928.

Grâce aux milliards de combinaisons possibles, les allemands avaient une confiance aveugle dans leur machine. Ils n'ont appris qu'en 1973, et avec stupeur, qu'une grande partie de leurs messages secrets avaient été décodés et avaient permis aux alliés de remporter, entre autres, la bataille de l'Atlantique et de battre l'Afrika Korps puis fut très utile lors des débarquements en Normandie et en Provence.

C'est grâce au Capitaine Gustave Bertrand des services de renseignements français, aux documents fournis par l'allemand Hans-Thilo Schmidt et aux travaux du Biuro Szyfrów polonais que les premiers messages ont été décodés dès 1932. Ces travaux ont ensuite été repris par Alan Turing à Bletchley Park au début de la guerre. Les équipes de Bertrand installées à Gretz-Armainvilliers au PC Bruno puis à Uzès au PC Cadix ont décodé, entre 1939 et 1942, plus de 13.000 messages et les ont envoyés par radio à Bletchley Park.

Les opérateurs Enigma avaient pour ordre de détruire leur machine et les livres de code pour éviter qu'ils ne tombent entre les mains de l'ennemi, de ce fait la machine est devenue rarissime.

L'Enigma 3 rotors n° 14087/jla/42 entièrement opérationnelle sera exposée.

Des démonstrations de codage et de décodage seront effectuées sur cette machine.

Contact :

Edmond Kern
06 71 40 44 68
edmondkern@yahoo.fr

AGEAT - Association de la Guerre Electronique de l'Armée de Terre
ALCMB - Association lorraine des collectionneurs de matériel de bureau
ANCMECA - Association nationale des collectionneurs de machines à écrire et à calculer mécaniques