Histoire et principe d'ENIGMA, une machine à chiffrer et à déchiffrer

Gérard GRANCHER*

Enigma est la machine à chiffrer et déchiffrer qu'utilisèrent les armées allemandes du début des années trente jusqu'à la fin de Seconde Guerre Mondiale. Elle automatise le codage par substitution. Le codage d'un message par substitution consiste à changer chaque lettre du messsage initial par une autre lettre de l'alphabet. Dès 1933 et jusqu'au début de la guerrre, grâce aux renseignements recueillis par un militaire français (Gustave BERTRAND) et au travail de trois mathématiciens polonais (Marian REJEWSKI, Jerzy RÓZICKI et Henryk ZYGALSKI), le "*Polski Biuro Szyfrów*" sut décrypter les messages allemands. Les allemands perfectionnèrent presque sans discontinuer leur machines. Les anglais, grâce en particulier au génie d'Alan Turing, réussirent à faire du décryptage des messages codés par Enigma une véritable industrie.

L'histoire d'Enigma qui mêle la Grande Histoire aux Mathématiques inspira plusieurs romans d'espionnage [2, 5].

Le Mémorial de la Paix à Caen présente deux machines Enigma.

On trouve beaucoup de choses sur Enigma qui encore aujourd'hui passionnent de nombreux internautes. Les sites se copient beaucoup les uns les autres, y compris dans leurs erreurs (schéma erroné d'Enigma). Rares sont les sites qui expliquent en quoi la théorie des permutations a contribué au décryptement d'Enigma. Voici une liste non exhaustive (la plupart en anglais) des sites qui me semblent les plus intéressants :

- Le livre de Blaise de Vignère en ligne et commenté
  `http://www.chass.utoronto.ca/~wulfric/rentexte/vigenere/chif_htm.htm`
- Histoire et usage d'Enigma
  `http://www.attlabs.co.uk/andyc/enigma/about_enigma.html`
  `http://members.aol.com/nbrass/enigma.htm`
- Décryptage d'Enigma par les polonais
  `http://www.gl.umbc.edu/~lmazia1/Enigma/enigma.html`
- Bletchley Park et la bombe de Turing
  `http://www.cranfield.ac.uk/ccc/bpark/morebpark.htm`
  `http://www.geocities.com/CapeCanaveral/Hangar/4040/bombe.html`
- Site d'Andrew Hodges sur Alan Turing
  `http://www.wadham.ox.ac.uk/~ahodges/Turing.html`

Références

[1] Gustave BERTRAND. *Enigma ou la plus grande énigme de la guerre 39-45.* Plon, 1973.

[2] FRANK, VAUTRIN. *Mademoiselle Chat.* Fayard, 1996.

[3] Krzysztof GAJ. *Szyfr enigmy, metody zlamania.* WKL, 1989.

[4] Jack I. GOOD. A.M. Turing's statistical Work in World War II. *Biometrika*, 66, 1979.

[5] Robert HARRIS. *Enigma.* Plon, 1996.

[6] F.H. HINSLEY. *British Intelligence in the Second World War, Vol 1.* HMSO, 1979.

*Laboratoire de Mathématiques Raphaël Salem, CNRS - Université de Rouen

[7] Andrew HODGES. *Alain Turing ou l'énigme de l'intelligence.* Payot, 1988.

[8] Camille JORDAN. *Traité des substitutions et des équations algébriques.* 1870.

[9] T. W. KÖRNER. *The Pleasure of Counting.* Cambridge University Press, 2000.

[10] André MULLER. *Les écritures secrètes.* PUF, 1971.

[11] André MULLER. *Le décryptement.* PUF, 1983.

[12] Jaques PATARIN. La cryptographie à clé secrète. *Pour la science*, 291, 2002.

[13] Marian REJEWSKI. An application of the theory of permutations in breaking the Enigma cypher. *Applicationes Mathematicae*, 1980.

[14] Marian REJEWSKI. Mathematical solution to the Enigma cipher. *Cryptologica*, 6, 1982.

[15] Marian REJEWSKI, Joan STEPENSKE. How Polish mathematicians deciphered the Enigma. *Annals of the History of Computing*, 3, 1981.

[16] Simon SINGH. *Histoire des codes secrets, de l'Égypte des Pharaons à l'ordinateur quantique.* JC Lattès, 1999.

[17] Blaise de VIGENÈRE. *Traicte des chiffres, ov secretes manieres d'escrire.* 1587.