publié dans: La Revue des Radioamateurs Canadiens, Juillet / Août 2009, pp. 40-44.

La machine Enigma et sa version électronique

Michel Barbeau, VE3EMB

L'Enigma

L'Enigma est une machine conçue pour chiffrer des textes dans une forme codée et illisible. Cet appareil a été inventé en 1918 par l'ingénieur allemand Arthur Scherbius, qui a vécu de 1878 à 1929. La marine allemande a adopté l'Enigma en 1925 pour sécuriser ses communications. Cette machine était également utilisée par l'Allemagne Nazi durant la deuxième guerre mondiale pour chiffrer les messages radio. Le texte chiffré était transmis en code Morse par télégraphie sans fils à la destination où une deuxième machine Enigma était utilisée pour déchiffrer le texte encodé dans sa forme originale. Les deux appareils Enigma devaient être configurés de façon identique pour que l'étape de déchiffrement fonctionne avec succès.

La machine Enigma est constituée d'un clavier, d'une unité de permutation, d'un tableau d'affichage et d'un tableau d'interconnexions. Le clavier de 26 lettres est utilisé pour la saisie du texte en clair, durant le chiffrement, ou du texte chiffré, durant le déchiffrement. Dans la version de base, l'unité de permutation comprend trois disques de chiffrement changeant les lettres les unes avec les autres. Chaque disque comporte 26 positions. Chaque fois qu'une lettre est chiffrée, le premier disque effectue 1/26 de tour, le deuxième (26×26) de tour, en moyenne, et le troisième $(26 \times 26 \times 26)$ de tour, en moyenne. D'un autre point de vue, il y a 26 exposant trois (17.576) positions initiales ou alphabets de chiffrement. Les disques sont amovibles et interchangeables. Il existe six façons différentes d'insérer trois disques dans la machine, multipliant par six le nombre de configurations initiales. Pour le fonctionnement, trois disques sont choisis parmi cinq disques différents disponibles donnant ainsi 60 dispositions différentes. Ceci crée au delà d'un million de combinaisons.

Un tableau de 26 lettres affiche le texte encodé durant le chiffrement. Le tableau d'interconnexions ajoute un niveau optionnel et additionnel de permutation. D'un point de vue électrique, il est inséré entre le clavier et le premier disque. Avant le chiffrement de chaque lettre, cette dernière peut être permutée avec une autre lettre, en fonction des câbles branchés dans le tableau d'interconnexions. L'opérateur de la machine dispose de six câbles. Par conséquent, jusqu'à six lettres peuvent être permutées. Ceci multiplie par 100 milliards le nombre d'alphabets de chiffrement, produisant un nombre total de configurations de l'ordre de 10 exposant 16. La configuration initiale était extraite d'un livre de codes, indiquant quels câbles devaient branchés, le cas échéant. La configuration initiale est appelée la clé secrète.

La deuxième guerre mondiale se déroula de 1939 à 1945 entre les Alliés (Grand Bretagne, Russie, les États-Unis, la France, la Pologne, le Canada et d'autres) et l'Allemagne (avec quelques autres pays membres de l'Axe). Pour minimiser le risque que les Alliés découvrent leur code, les allemands changeaient leur clé secrète à chaque jour.

Les codes utilisés pour les Enigma de la marine allemande portaient des noms évocateurs donnés par les allemands. Dauphin était le code principal de la marine. Huitre était la version des officiers.

Marsouin était le code utilisé par les navires navigant sur la mer Méditerrané et la mer Noire. Bigorneau était une version de Marsouin pour les officiers. Requin était le code utilisé par les sous-marins U-boat. Il était 26 fois plus difficile à casser que les autres parce qu'il fonctionnait avec une machine possédant un quatrième disque produisant le nombre astronomique de 129,651,786,900,000,000,000,000 combinaisons.

Il est remarquable de constater qu'il existe au moins sept machines Enigma originales et en bon état au Canada.

Vous pouvez examiner de près une Enigma au Musée Canadien de la guerre à Ottawa dans la section réservée à la bataille de l'Atlantique de la galerie de la deuxième guerre mondiale. Il s'agit d'une machine Enigma modèle M4 à quatre disques datant de 1943, en excellent état, qui était utilisée par la marine allemande. Le Musée Canadien de la guerre dispose également, en entreposage, d'une Enigma modèle A. C'est une version à trois disques qui était utilisée par l'armé allemande et ses forces aériennes. La question de l'origine des machines Enigma dont le musée est propriétaire a été explorée par Tony Wilson (1997), mais n'a pas été élucidée. L'hypothèse la plus plausible est qu'elles faisaient parti d'un ensemble de pièces d'équipement apportées d'Allemagne par l'auteur canadien Farley Mowat. Il a en effet occupé le rôle d'agent de renseignement durant la deuxième guerre mondiale et organisé le transport au Canada de plusieurs pièces d'équipement militaire allemand.

Il existe aussi une Enigma exposée au Musée de l'électronique et des communications militaires à Kingston (Ontario). La machine est prêtée au musée et est l'une des deux machines appartenant au Centre de la sécurité des télécommunications Canada. C'est une Enigma modèle M4. Elle a été prise, par la marine canadienne, du sous-marin U-boat U-190 quand celui-ci s'est rendu à Sydney en Nouvelle-Écosse en 1945. Le U-190 patrouillait les eaux de la côte est du Canada durant la guerre. En 1945, il envoya au fond le navire HMCS Esquimalt de la marine canadienne.

Finalement, le collectionneur canadien Richard Brisson est propriétaire de trois Enigma modèles A, K et M4. Sa collection peut être consultée sur Internet (voir le lien dans la bibliographie).

L'Enigma modèle M4 exposée au Musée de l'électronique et des communications militaires (Kingston). Notez la présence de quatre petites fenêtres sur les disques de chiffrement dans la partie supérieure. (Photo par le Musée de l'électronique et des communications militaires)

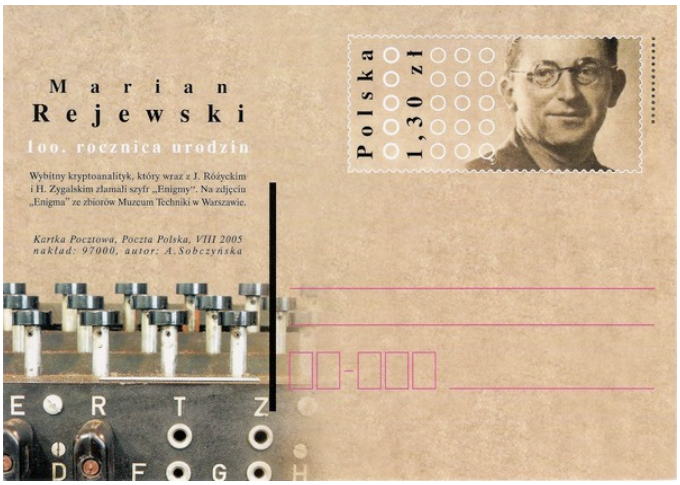
L'Enigma modèle A entreposée au Musée Canadien de la guerre (Ottawa). Notez la présence d'uniquement trois petites fenêtres sur les disques de chiffrement dans la partie supérieure. (Photo de l'auteur)

Le sous-marin allemand U-190. (Photo par Edward W. Dinsmore/Canada Ministère de la défense nationale / Bibliothèque et Archives Canada/PA-145584)

Qui a cassé L'Enigma?

En dépit du nombre extraordinairement grand de combinaisons, selon les standards cryptologiques modernes l'Enigma est une machine de chiffrement facile à casser. Cependant, à l'époque c'était tout un casse-tête pour les alliés. Marian Rejewski and Alan M. Turing ont joué des rôles clés dans les efforts qui ont mené à casser le code de l'Enigma. Marian Rejewski travaillait pour le bureau des codes polonais. Il a contribué de façon importante dans les débuts en exploitant le fait que chaque message était envoyé chiffré au moyen d'une clé de message envoyé deux fois dans l'en-tête du message, mais chiffré avec une clé secrète journalière. Pour commémorer le centième anniversaire de naissance de Rejewski, la poste polonaise a publié une carte postale prépayée en 2005. De plus, en 1983, la poste polonaise a publié un timbre commémorant le cinquantième anniversaire des efforts de cryptanalyse de la machine Enigma.

Alan M. Turing, un membre du Goverment Code and Cypher School basé à Bletchley Park en Angleterre, a fait la découverte d'une faille de l'Enigma et a conçu un ordinateur pour faciliter le déchiffrement de ses codes. L'île de Sainte-Hélène, un territoire outremer de la Grande-Bretagne dans l'Océan Atlantique a publié en 2005 un timbre pour commémorer la contribution d'Alan M. Turing. L'île de Saint Hélène a joué un rôle dans l'interception des communications de la marine allemande.



Une carte postale prépayée commémorant le centième anniversaire de naissance de Rejewski(2005).

Un timbre publié en 1983 par Poczta Polska pour commémorer les efforts polonais pour déchiffrer les codes de l'Enigma.

Un timbre, de l'île Sainte Hélène (2005) pour commémorer la contribution d'Alan M. Turing pour casser les codes de l'Enigma.

L'après guerre des machines de chiffrement à disques : Un cheval de Troie

Un aspect intéressant de l'histoire de l'Enigma et des machines à disques similaires utilisées après la deuxième guerre mondiale est l'utilisation stratégique de la capacité à les décoder. Le travail de décodage effectué à Bletchley Park a été rendu publique seulement en 1970, 25 ans après la fin de la guerre. Après la deuxième guerre mondiale, la stratégie britannique était d'encourager les pays amis à adopter des machines de chiffrement à disques semblables à l'Enigma pour sécuriser leurs communications, sans toutefois leur faire savoir que les britanniques étaient capables de décoder ce type d'échanges. La France, en particulier, fessait l'usage d'une machine de chiffrement à disques appelée Hagelin modèle C-36. L'auteur canadien John Bryden, dans le livre intitulé *Best-kept secret: Canadian secret intelligence in the second world war*, raconte cette histoire et explique que le Canada, l'Angleterre et les États-Unis, de proches collaborateurs, interceptaient et décodaient les communications du gouvernement Français de 1943 à 1963. Le bris de confiance des trois proches partenaires envers le gouvernement Français à été déclenché par un incident qui a été suivi d'une suite de malentendus. Nous sommes en 1941. La France est occupée par l'Allemagne et est gouvernée par le régime fantoche de Vichy. Les îles Saint-Pierre et Miquelon dans le Golfe du Saint-Laurent, sont

demeurées fidèles au gouvernement de Vichy. Le gouvernement de la France libre, dirigé par le général Charles de Gaulle, de son propre chef prend le contrôle des îles la veille de Noël 1941. L'initiative du général va cependant à l'encontre d'une politique qui stipule que les États-Unis ne tolèreront aucun changement de contrôle territorial dans l'hémisphère ouest par l'entremise d'une intervention militaire européenne. À partir de cet incident, le Canada, l'Angleterre et les États-Unis ont cessé de faire confiance au général de Gaulle et ils le considéraient maintenant comme un fauteur de troubles. Le Canada intercepta et décoda les communications du général de Gaulle et du gouvernement Français jusqu'en 1963. L'auteur américain David Kahn rapporte également que le National Security Agency des États-Unis avait des activités de cryptanalyse des communications diplomatiques françaises (1967). Le moment exact où ceci a été porté à la connaissance du général n'est pas connu, mais son mécontentement s'est traduit par un retrait de le France de la participation militaire à l'OTAN (1966). Une décision qui a été tout récemment renversée par le président Sarkozy (Mars 2009). Une hypothèse est que le mécontentement par rapport au Canada a propulsé le général à déclarer, du haut du balcon de l'hôtel de ville de Montréal en 1967, *Vive le Québec libre*!

La machine Hagelin C-36. Celle-ci appartient à la collection Richard Brisson. (Photo par Richard Brisson)

Où trouver des machines Enigma?

Le nombre exact de machines Enigma qui ont été mises en circulation est inconnu. Les registres ont été détruits à la fin de la guerre. Selon le professeur Tom Perera (voir le lien à son site Web dans la bibliographie), il pourrait y avoir eu jusqu'à 20.000 machines Enigma. Plusieurs d'entre elles reposent au fond de l'océan dans des sous-marins U-boat. Elles sont maintenant irrécupérables. D'autres ont été détruites. Le professeur Perera estime qu'il existe maintenant environ 200 machines en circulation. Elles sont dispendieuses et difficiles à trouver. Comme alternative, il est possible de construire sa propre version électronique de l'Enigma.

Construction d'une version électronique

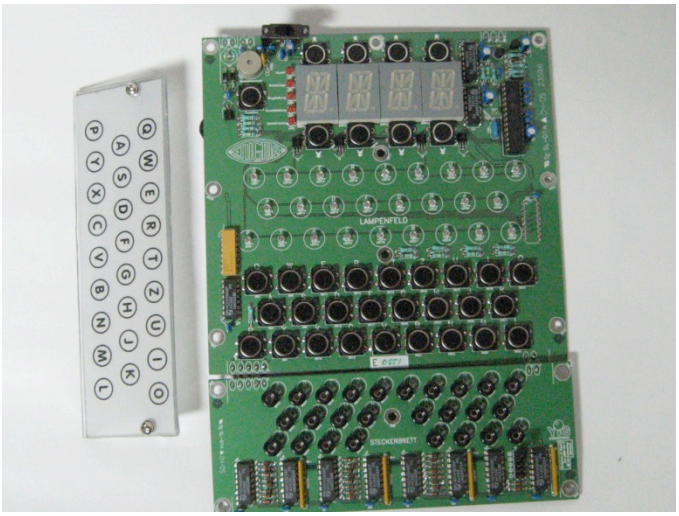
J'ai assemblé ma propre machine Enigma, version électronique, en utilisant comme base le kit Enigma-E (www.xat.nl/enigma-e). Le kit vient avec deux circuits imprimés, des composants et des

instructions d'assemblage. Le niveau de difficulté est modéré (aucun composant monté en surface). Quelques heures d'assemblage et de mise au point sont requises. Une photo montre mon unité assemblée. Le circuit imprimé principal comporte un clavier de 26 lettres et un tableau d'affichage de 26 lettres illuminées. Le petit circuit imprimé, rattaché au circuit principal, constitue le tableau d'interconnexions. Le kit électronique peut être acheté en ligne sur le site Web du musée de Blectchley Park (www.bletchleypark.org.uk).

L'assemblage final de l'Enigma électronique est montré sur une seconde photo. La boîte de bois, le tableau d'affichage en Plexiglas et le logo Enigma gravé ne viennent pas avec le kit. Les instructions d'assemblage contiennent une section sur la conception et la construction de votre propre boîte d'Enigma. N'ayant ni les outils et les habiletés requises pour entreprendre un tel projet, j'ai obtenu une boîte préfabriquée par Mark Dement. La boîte est très belle. Elle est faite de chêne blanc d'un quart de pouce avec des joints à peigne. La boîte vient assemblée et poncée. J'ai complété le travail avec deux couches de vernis. J'ai coupé deux morceaux de Plexiglas entre lesquels j'ai placé en sandwich une pellicule de plastique reproduisant les ampoules d'affichage. Les circuits sont montrés prêts à être installés sur la photo. J'ai obtenu le logo gravé Enigma du site Web www.enigma-replica.com. Une plaquette est apposée sur la partie intérieure du couvercle de la boîte. Elle contient les instructions de fonctionnement en allemand pour l'opérateur. Le texte peut être téléchargé de l'Internet, imprimé sur du papier auto adhésif et collé à l'intérieur du couvercle.

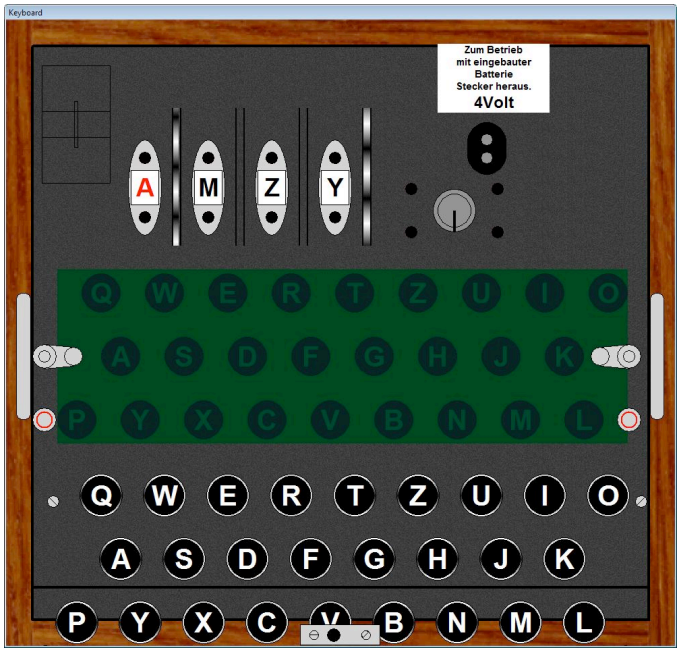
L'Enigma électronique peut être branchée à un simulateur, tel que le simulateur d'Enigma modèle M4 développé par Geoff Sullivan pour les ordinateurs personnels Windows. La machine électronique et le simulateur fonctionnent en synchronisme. Quand vous tapez une lettre sur le clavier du simulateur, le texte est affiché, chiffré ou déchiffré, sur l'Enigma électronique (selon sa configuration). L'inverse fonctionne également.

Le résultat final est très intéressant et vraiment fonctionnel. Bien entendu, il n'est pas possible de l'utiliser sur les fréquences radio amateur parce que les messages chiffrés ne sont pas permis. 73!



Les circuits de l'Enigma-E avec leurs composants et le tableau d'affichage en Plexiglas. (Photo par l'auteur)

L'Enigma-E complété dans sa boîte de bois. (Photo par l'auteur)



Le simulateur d'Enigma modèle M4 par Geoff Sullivan.

Au sujet de l'auteur

Michel Barbeau est membre de l'Ottawa Valley Mobile Radio Club, de Radio Amateurs du Canada, de Tucson Amateur Packet Radio et de l'American Radio Relay League. Ses modes de communications favoris sont la radio par paquets, PSK31 et le RTTY. Il est aussi passionné par la radio logiciel. Il a obtenu un Certificat de radioamateur (avril 1987) et un Certificat numérique de radioamateur (décembre 1987). Il est professeur d'informatique depuis 1991. Il est présentement membre du corps professoral à l'Université Carleton où il enseigne et effectue des recherches en communications radio. On peut communiquer avec lui par courriel à : michel.barbeau@sympatico.ca.

Remerciements

Je désire remercier les personnes suivantes pour leur aide à la préparation de cet article. Le professeur Michael R. Williams de l'Université de Calgary pour m'avoir indiqué l'existence d'un lien entre Charles de Gaulle et l'Enigma. Le docteur Andrew Larocci, gestionnaire des collections, pour m'avoir donné accès à des artéfacts entreposés au Musée Canadien de la guerre (Ottawa). Madame Annette E. Gillis, curatrice, pour les informations détaillées concernant la machine Enigma exposée au Musée de l'électronique et des communications militaires (Kingston). Monsieur Richard Brisson, collectionneur, pour de nombreuses informations sur l'histoire de la cryptologie.

Bibliographie

Richard Brisson, Cryptographic and Clandestine Tradecraft, home.ca.inter.net/~hagelin/collection.html, 2009.

Richard Brisson and François Théberge, Un aperçu de l'histoire de la cryptologie, Publié par le Centre de la sécurité des télécommunications Canada, 2008.

John Bryden, Best-kept secret: Canadian secret intelligence in the second world war, Lester Publishing Limited, 1993.

David Kahn, The Codebreakers: History of Secret Communications, MacMillan Publishing Co., 1967.

Tom Perera, Enigma Cipher Machines, Fialka, Nema, other Cipher Machines, Antique Computers and Calculators, w1tp.com/enigma, 2005.

Simon Singh, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, Anchor, 2000.

Tony Wilson, The Enigma Cipher Machine, Canadian Military History, Volume 6, Number 2, Autumn 1997, pp. 72-78.