Published in: Canada's Amateur Radio Magazine, July / August 2009, pp. 40-44.

The Enigma Encryption Machine and its Electronic Variant

Michel Barbeau, VE3EMB

What is the Enigma?

The Enigma is a machine devised for encrypting plain text into cipher text. The machine was invented in 1918 by the German engineer Arthur Scherbius who lived from 1878 to 1929. The German Navy adopted the Enigma in 1925 to secure their communications. The machine was also used by the Nazi Germany during World War II to cipher radio messages. The cipher text was transmitted in Morse code by wireless telegraph to the destination where a second Enigma machine was used to decrypt the cipher text back into the original plain text. Both the encrypting and decrypting Enigma machines had identical settings in order for the decryption to succeed.

The Enigma consists of a keyboard, a scrambling unit, a lamp board and a plug board. The 26-letter keyboard is used for plain text entry, during encryption, or cipher text entry during decryption. In the basic version, the scrambling unit consists of three cipher disks called rotors that permute the letters. Each rotor has 26 starting positions. Each time a letter is ciphered, the first disk does 1/26 of a revolution, the second disk does 1(26×26), on average, of a revolution and the third disk does 1(26×26×26) of a revolution, on average. Another way to look at this is that there are 26 power three (17,576) initial settings or cipher alphabets. Rotors are removable and interchangeable. There are six different possible arrangements of three rotors, multiplying by six the number of initial settings. For operation, three rotors are chosen from five different rotors with 60 possible orders. That alone creates over a million combinations.

The 26-letter lamp board displays the cipher text, during encryption, or plain text, during decryption. The plug board adds an optional and additional level of letter permutation. It is electrically inserted between the keyboard and first rotor. Before each letter is scrambled, it can be switched around with another letter, depending on the plug board (called Stecker pair) settings. Six cables are available to the operator; six pairs of letters can be swapped. Multiplying by over 100 billion the number of possible initial settings, making the total number of initial settings in the order of 10 power 16. The initial setting, taken from a code book, indicates which pairs of letters (if any) are switched with each other. The initial setting is called the secret key.

World War II was fought from 1939 to 1945 between the Allies (Great Britain, Russia, the United States, France, Poland, Canada and others) and the Germans (with the Axis). To minimize the chance of the Allies cracking their code, the Germans changed the secret key each day.

The codes used for the naval Enigmas, had evocative names given by the germans. Dolphin was the main naval cipher. Oyster was the officer’s variant of Dolphin. Porpoise was used for Mediterranean surface vessels and shipping in the Black sea. Winkle was the officer’s variant of Porpoise. Shark was the U-boat cipher and was 26 times more difficult to break than the others because of an additional fourth rotor yielding a gigantic total of 129,651,786,900,000,000,000,000 combinations.

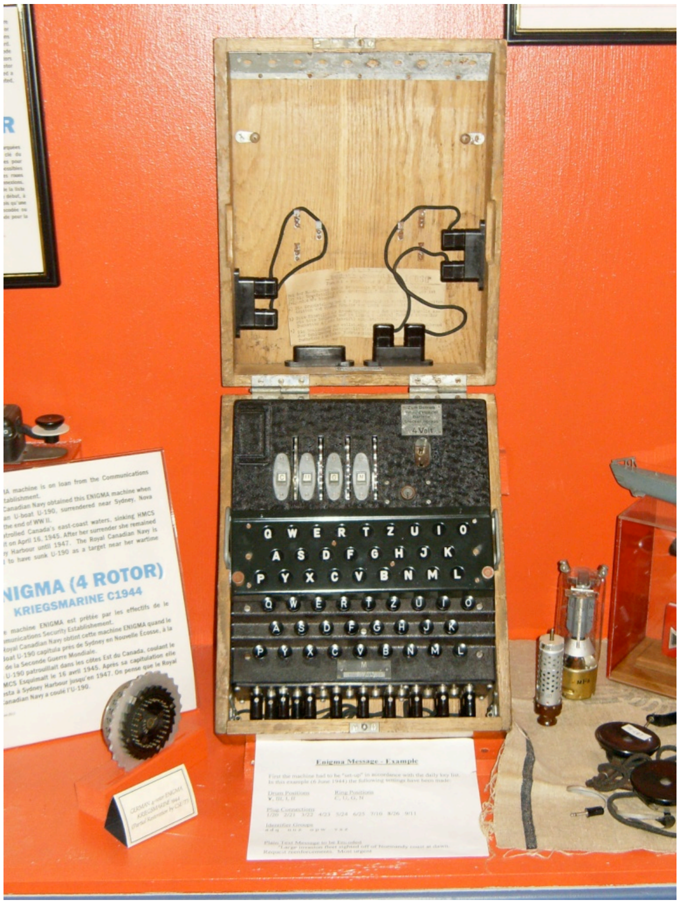
Interestingly, I’ve been able to locate the existence of at least seven original and in good condition Enigma machines in Canada.

You can closely look at an Enigma machine at the Canadian War Museum in Ottawa in the Atlantic battle section of the World War II gallery. It is a nice 1943 M4 Enigma machine with four wheels that was used by the German navy.

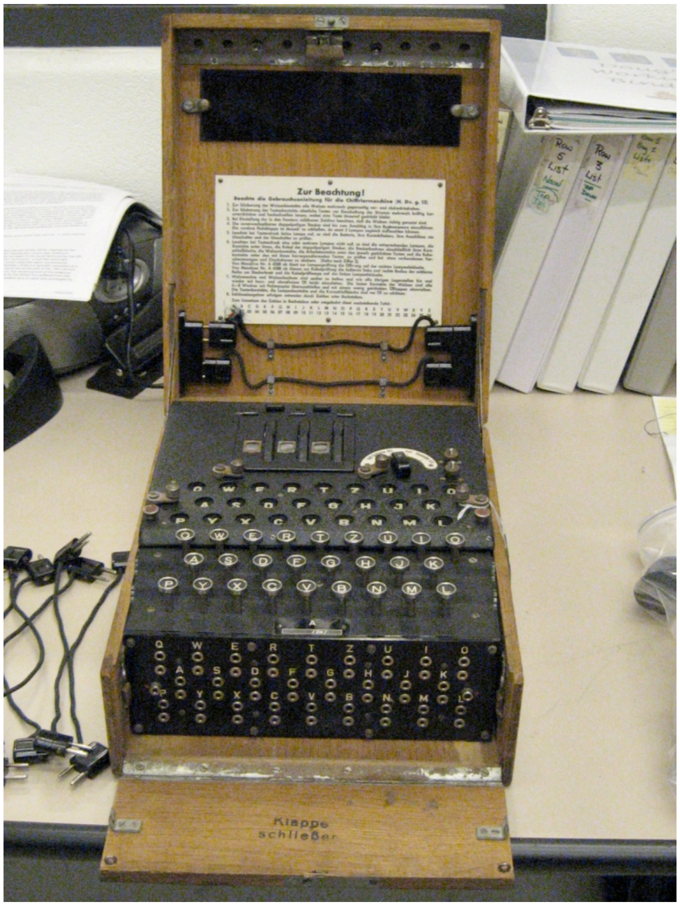
The Canadian War Museum has also in storage a Type A Enigma machine. It is a three rotor variant that was used by the German army and air force. The origin of the Enigmas owned by the Canadian War Museum has been investigated before by Tony Wilson (1997), but couldn’t be clarified. A plausible hypothesis is that they were parts of a group of items brought back from Germany by the Canadian author Farley Mowat. He served as an intelligence agent during World War II and organized the transfer to Canada of several pieces of German military equipment.

There is an Enigma on display at the Military Communications and Electronics Museum in Kingston (Ontario). The machine is lent to the museum and is one of the two machines belonging to the Communications Security Establishment Canada. It is a M4 Enigma and it was taken by the Royal Canadian Navy from the German U-boat U-190 when it surrendered in Sydney, Nova Scotia in 1945. The U-190 was patrolling waters of the east coast of Canada during the war. In 1945, it sunk the ship HMCS Esquimalt of the Royal Canadian Navy.

Finally, the Canadian collector Richard Brisson owns three Enigmas type A, K and M4. You can browse through his collection on the Internet (see the link in the bibliography).



The M4 Enigma on display at the Military Communications and Electronics Museum (Kingston). Note the four small rotor windows in the upper part of the machine. (Photo by the Military Communications and Electronics Museum)



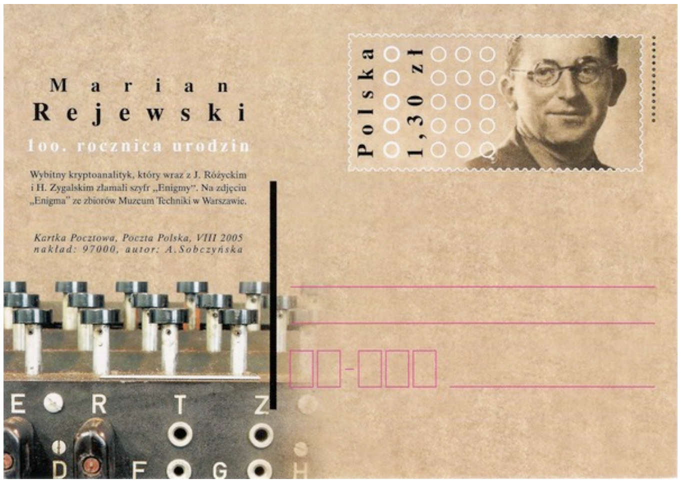
The Type A Enigma owned by the Canadian War Museum (Ottawa). Note that this version has only three rotors. (Photo by the author)

The German submarine U-190. (Photo by Edward W. Dinsmore / Canada. Dept. of National Defence / Library and Archives Canada / PA-145584)

Cracking the Enigma

Despite the extraordinarily large number of combinations, according to today’s cryptology standards the Enigma is a weak cipher. However, at that time it was quite puzzling for the Allies. Two individuals were instrumental in cracking the Enigma, namely, Marian Rejewski and Alan M. Turing. Marian Rejewski was a member of the Poland Cipher Bureau. He made important initial contributions by exploiting the fact that each message was sent encrypted with a *message key* repeated twice in the head of each message, but encrypted with a daily secret key. To commemorate the 100th anniversary of Rejewski's birth, Poczta Polska issued a prepaid postcard in 2005. This was in addition to a 1983 stamp commemorating the 50th anniversary of Polish cryptanalysis efforts against the Enigma machine.

Alan M. Turing, a member of the Government Code and Cypher School based at Bletchley Park, UK, uncovered a flaw of the Enigma and designed a computer that helped breaking it. The Saint Helena Island, a British overseas territory in the South Atlantic Ocean, issued in 2005 a stamp to commemorate the contribution of Alan M. Turing. The Saint Helena Island played a role in the monitoring of the communications of the German navy. You can read more about the story of cracking the Enigma in a book from Simon Singh (see the bibliography).



Marian
Rejewski
100. rocznica urodzin

Wybitny kryptoanalityk, który wraz z J. Różyckim i H. Zygalskim złamali szyfr „Enigmy”. Na zdjęciu „Enigma” ze zbiorów Muzeum Techniki w Warszawie.

Kartka Pocztowa, Poczta Polska, VIII 2005
nakład: 97000, autor: A.Sobczyńska

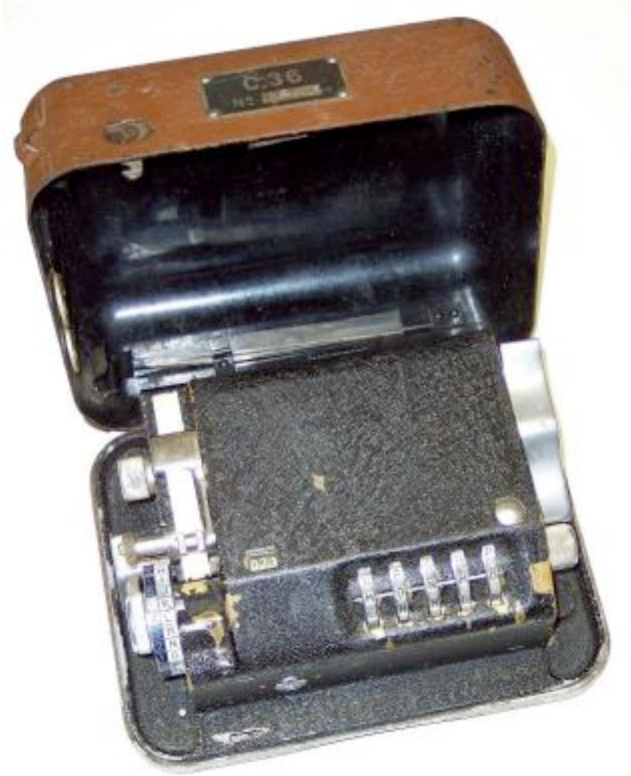
A Polish prepaid postcard issued to commemorate the 100th anniversary of Rejewski's birth (2005).

A stamps issued in 1983 by Poczta Polska to commemorate Polish decipherment efforts of the Enigma machine.

The Enigma stamp, from the Saint Helena Island (2005) to commemorate the contribution of Alan M. Turing for breaking the codes of the Enigma.

Post war use of rotor-based encryption machines: A Trojan horse

An interesting aspect of the story of the Enigma and similar post-war rotor based machines is the strategic use of the ability to break them. The code breaking work of Bletchley Park was released to the public only in 1970, 25 years after the end of the war. After World War II, the British strategy was to encourage *friendly countries* to adopt rotor-based encryption machines like the Enigma to secure their communications, without of course making them aware of the British ability to decrypt this type of traffic. France in particular made use of a rotor-based encryption machine called the Hagelin type C-36. The Canadian author John Bryden, in his book entitled *Best-kept secret: Canadian secret intelligence in the second world war*, tells the story and explains that Canada, England and United States, intimate partners, intercepted and decoded French diplomatic traffic from 1943 to 1963. The event that triggered the lack of trust of the three intimate partners in the French government is an incident that was followed by a sequence of misunderstandings. We are in 1941. France is occupied by Germany and governed by their Vichy puppet. The St-Pierre and Miquelon Islands, in the St-Laurence Gulf, are loyal to the Vichy government. The Free French government, headed by General Charles de Gaulle, on its own initiative, seize the islands on the Christmas Eve of 1941. De Gaulle's initiative was against a policy which states that the *United States would not tolerate any change of territorial control in the Western hemisphere by European military intervention*. From that point Canada, England and United States stop trusting de Gaulle and viewed him as a trouble maker. Canada was reading de Gaulle and French government traffic until 1963. The American author David Kahn also reports that the US National Security Agency had cryptanalysis activity against France diplomatic traffic (1967). The exact time when de Gaulle learned about this is unknown, but his dissatisfaction translated to French withdrawal from military participation in NATO (1966). A decision recently reversed by President Sarkozy (March 2009). An hypothesis is that the dissatisfaction with respect to Canada, in particular, snowballed his 1967 declaration from a balcony of the Montreal city hall: *Vive le Québec libre!*



The Hagelin C-36. This particular unit belongs to the Richard Brisson's collection. *(Photo by Richard Brisson)*

Getting an Enigma

It is unknown how many Enigma machines were put into circulation. The records had been destroyed at the end of the war. According to Prof. Tom Perera (see the link to his Web site in the bibliography), it can be up to 20,000 Enigmas. Several Enigmas lie on the bottom of the ocean in U-boats, unrecoverable. Others were destroyed. Prof. Perera estimates that 200 Enigmas are still in circulation. They are pricy and difficult to get. An affordable alternative, is building your own electronic version of it.

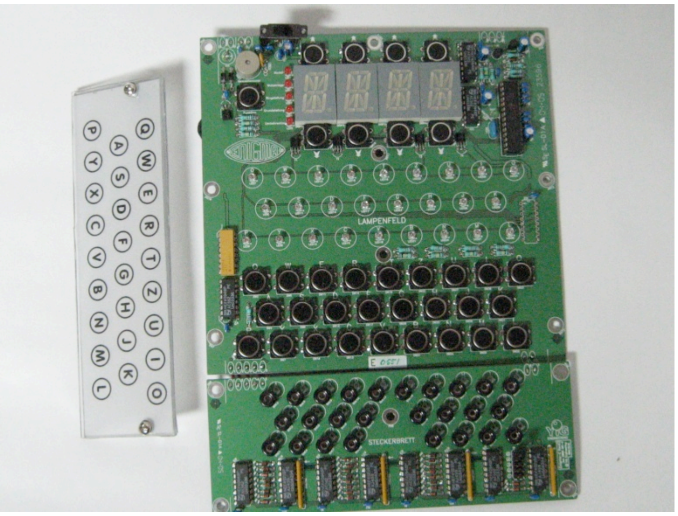
Building an Electronic Variant of the Enigma

I assembled my own electronic Enigma using the Enigma-E kit (www.xat.nl/enigma-e). The kit comes with two PCBs, parts and assembly instructions. The level of difficulty is moderate (no surface mount parts) and require few hours of assembly and debugging work. A picture shows my unit assembled. The main PCB consists of a 26-letter keyboard and a 26-letter lamb board. The small PCB, attached to the main PCB, is the plug board. The electronic kit can be ordered online from the Bletchley Park museum (www.bletchleypark.org.uk).

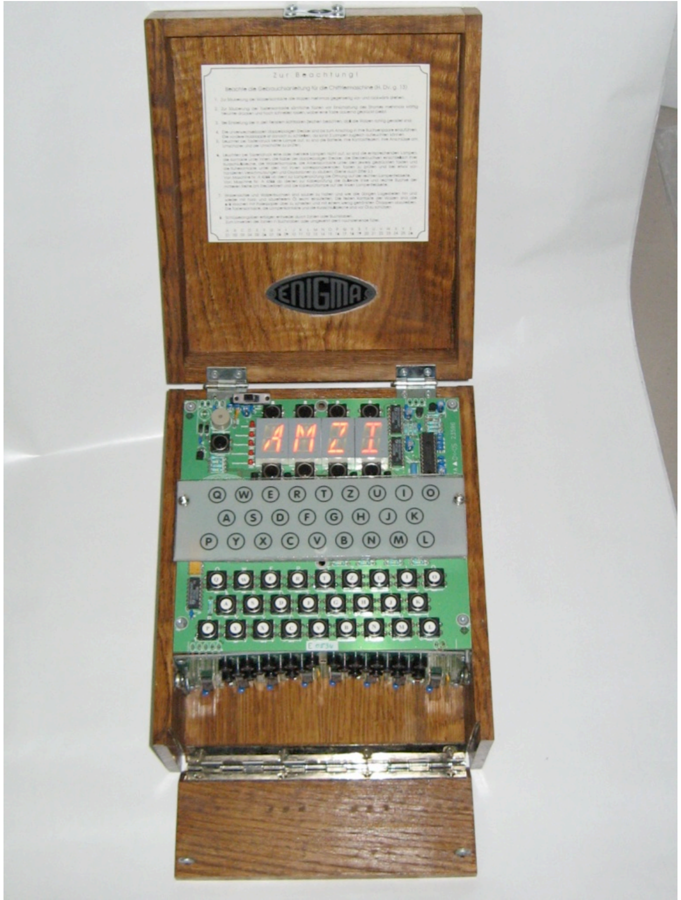
The final assembled electronic Enigma is show in a second picture. The wooden box, Plexiglas lamp board and engraved Enigma logo don't come with the kit. The assembly instructions contain a section about designing and building your own Enigma box. I did have neither the tools nor the skills to pursue such a project. I ordered a premade wooden box from Mark Dement. The box is very nice. It is made from quarter sawn white oak with finger joints. The box comes assembled and finish sanded. I completed the work with two coats of varnish. I cut two pieces of Plexiglas which are used to sandwich a lamp film that is shown ready to install in the first picture. I got the engraved Enigma logo from www.enigma-replica.com. The inside of the Enigma cover has a placard with instructions for the operator in German. The text can be downloaded from the Internet and printed on self-adhesive paper then put on the inside of the lid.

The electronic Enigma can be connected to a simulator such as the M4 Enigma simulator authored by Geoff Sullivan for Windows personal computers. The electronic device and its software emulator can operate in sync. When you type a letter on the simulator keyboard, the text is displayed encrypted or decrypted on the electronic Enigma, according to the settings. The reverse is also possible.

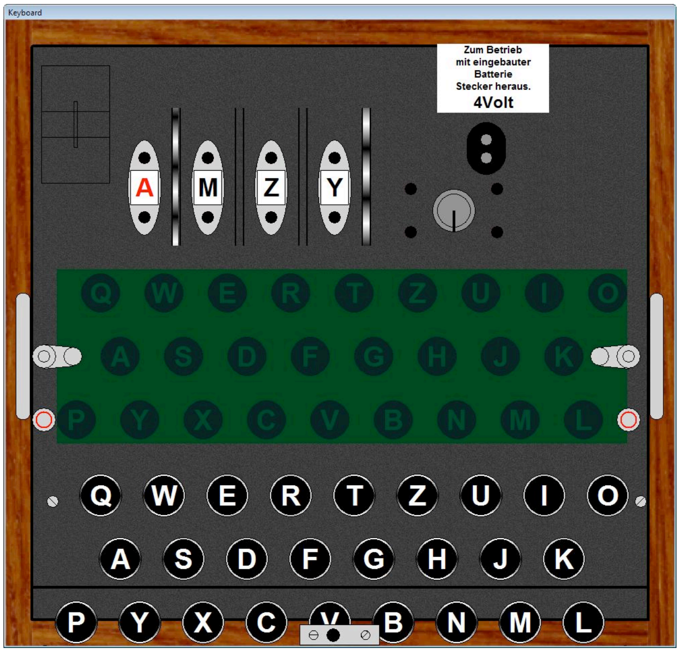
At the end it makes a nice replica which is truly operational. Of course, you cannot really use it over amateur radio frequencies because encrypted traffic is forbidden. 73!



The Enigma-E PCBs with parts and Plexiglas lamp board. (Photo by the author)



The Enigma-E with its finished wooden-box. (Photo by the author)



The M4 Enigma Simulator by Geoff Sullivan.

About the author

Michel Barbeau is a member of the Ottawa Valley Mobile Radio Club, Radio Amateurs of Canada, Tucson Amateur Packet Radio and American Radio Relay League. His preferred modes of operation are digital: Packet, PSK31 and RTTY. He also has an interest in Software Defined Radios. He has a Canadian Amateur Radio Operator's Certificate (April 1987) and an Amateur Digital Radio Operator's Certificate (December 1987). He has been a Professor of Computer Science since 1991. He is currently working at Carleton University where I teach and do research on wireless communications. He can be reached *by email at: michel.barbeau@sympatico.ca.*

Acknowledgements

I would like to acknowledge the following people for their help in the preparation of this article. Prof. Michael R. Williams form University of Calgary for pointing me to the link between Charles de Gaulle and the Enigma. Dr. Andrew Larocci, Collections Manager, from the Canadian War Museum (Ottawa) for giving me access to Enigma artefacts in storage at the museum. Mrs Annette E. Gillis, Curator, for detailed information about the Enigma on display at the Military Communications and Electronics Museum (Kingston). Mister Richard Brisson, collector, for detailed information about the history of cryptography.

Bibliography

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

Richard Brisson and François Théberge, An Overview of the History of Cryptology, A Communications Security Establishment Canada Publication, 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.