Beyond the Imitation Game: Canada's Ties to Bletchley Park

1918 marks the end of WWI but also the beginning of the Enigma story

by

Peter Berg

December 14th, 2018

The centennial commemorations of the end of World War I stir in our Canadian collective consciousness memories of a defining moment in history that shaped Canada's identity on numerous levels. Beyond WWI, much thought has also been given to how the Great War and the ensuing Versailles treaty laid the groundwork for what would become the human catastrophe of World War II. What is usually overlooked in the connections between these two wars is how intelligence and secure communication would play a crucial and much larger role in WWII, a role that was grounded in the experiences of WWI. More than any other encryption device, it was the German Enigma machine that embodied that unleashing of a covert war between rival intelligence services and capabilities, and it was the breaking of the Enigma code that gave the Allies a critical edge over the Germans. We now realize that this machine has affected many Canadian lives on the battle lines but it has also left a remarkable imprint on Canada to this day.

The Enigma machine was invented by Arthur Scherbius, a German citizen who filed his first Enigma patent in February 1918. Scherbius was a clever inventor but also a shrewd businessman. He realized the importance of secure communication not only to the German military during WWI but also to the business community, especially the banking sector. With a successful patent and machine in hand, Scherbius set out to manufacture several different versions of the Enigma during the 1920s through a private enterprise, selling the machines at first commercially and as of the late 1920s exclusively to the German military. Rooted in the disastrous failure in WWI, the German military was in desperate need of a more reliable, secure method to encrypt their communication, and the Enigma promised to be unbreakable.

How does the Enigma work? In essence, it resembles a typewriter that maps each letter of a text onto another letter of the alphabet. It is electro-mechanical in nature: by pressing a letter on its keyboard, a different letter on a lamp array lights up, and the successive, lit-up letters on the lamp array then form the encrypted text. Most importantly, this method includes two crucial features. Firstly, it begins encryption with an initial setting that can be selected from more possible settings than there are stars in the known universe. Secondly, every time one letter is encrypted, the machine changes its settings dynamically by use of rotating wheels, also called rotors, so that its logic changes with it, realized by a different internal wiring. The result is that letters are encrypted differently after each time a key is pressed and released on the keyboard. The sheer overwhelming combinatorics of the Enigma led the Germans to believe the machine was secure, and this persistent, yet false belief throughout WWII allowed the Allies to maintain one of the most important strategic advantages over the Nazis.

A vulnerability of the Enigma was that the initial settings for the encryption of a text were a combination of settings taken from codebooks provided by central command for months at a time and an individual message setting, chosen freely by the operator of the machine for any particular message. This individual setting, which consists of three or four letters, is referred to as a message key, and it had to be communicated between sender and receiver. In fact, the sender would send the message key in encrypted form along with the actual encrypted message text in the form of Morse code and via radio waves. The receiver would then use the same key, meaning

an identical initial machine setting, to decipher the text letter by letter. It was the communication of the key between sender and receiver that made it possible to break the code in the early days of the Enigma. Surprisingly, it was a young group of Polish undergraduate mathematicians who first broke the Enigma in 1932 and continued to do so on an on-going basis until the late 1930s. Equally surprising, perhaps, is the fact that any modern encryption method still relies on the sharing of a key that tells sender and receiver what "setting" is used for the encryption of a message.

In this sense, nothing has really changed since the introduction of the Enigma with one exception. While the Enigma employs symmetric encryption where sender and receiver use identical keys and set up their machines at the beginning in exactly the same way to encrypt and decrypt, respectively, more advanced encryption methods are asymmetric. These days, the receiver generates and distributes a public key that anyone can use to send him or her an encrypted message. This message can then only be deciphered with a so-called private key that differs ("asymmetric") from, but is linked to, the public key and that only the receiver possesses. The main point is then to make it extremely difficult for anyone to figure out what the private key may be. It becomes a matter of computational power to break an encrypted message and a good encryption method makes it impractically long to break the code, just as it seemed to be impractically long for anyone to break the Enigma code during WWII.

After the Germans invaded Poland, the Polish codebreaking activities and knowledge were relayed to the French and upon invasion of France by the Germans, this knowledge was finally conveyed to the British and, in particular, to Bletchley Park. This gave Alan Turing a tremendous head start and his construction of the bombe, again an electro-mechanical device but this time to rule out possible initial settings of an Enigma message, was in large part inspired by the Polish bomba, a set of Enigmas wired in series to do exactly the same logic elimination.

Two main ingredients were required for Bletchley Park to break the Enigma code: knowledge of the current makeup of an Enigma machine and a "crib". The latter was a term that described a part of an enciphered text for which the original German text was known with great likelihood. Fortunately, the German military made numerous mistakes when operating the machine, ranging from oversight to laziness, which were exploited to break the Enigma code. Encrypted messages from German weather stations, for example, were often used to obtain a crib since the messages would usually begin with the same words: time of day, followed by the location of the weather station and the word "*Wetterbericht*" (weather report). Alan Turing and his colleagues utilized these cribs in that they worked out efficient methods to determine which initial Enigma setting would map the crib onto the enciphered text that the British had intercepted. And as difficult as it was to break a message, breaking one message usually meant breaking all Enigma messages within a given Enigma network for the whole day because the message settings would only differ by the individual message settings, consisting of only three or four letters.

The other main ingredient was knowledge of the Enigma makeup. This was facilitated mostly by successful captures of Enigma machines and parts, codebooks, and other Enigma intelligence by the British Navy. This had to happen without the knowledge of the German High Command who would have otherwise likely ordered immediate modifications of the Enigma machine beyond the incremental modifications that were made anyways, thereby threatening the strategic advantage of the Allies. One person, in particular, laid out a "pinch doctrine" about how to obtain Enigma intelligence in dedicated raids onto German positions and ships: Ian Fleming, Commander in the British Naval Intelligence Division. Fleming is known to most of us as the author of the post-war James Bond novels which were undoubtedly inspired by his important role in the British intelligence service. What is less known is his lead role during the Battle of Dieppe

on August 19th, 1942, arguably Canada's darkest day during WWII. This raid was not only a disaster for Canadian troops, it was also an unsuccessful attempt to capture the new four-rotor Enigma machine that posed a serious challenge to the codebreakers at Bletchley Park in 1942. In his captivating book "One Day in August", Canadian author and military historian David O'Keefe describes very aptly and convincingly the true mission behind the Battle of Dieppe, based on years of research and an extraordinary amount of recently declassified, British military documents. Over 3,000 Canadians were killed, wounded or taken prisoner as part of a raid that was supposed to provide cover for the newly formed No. 30 Commando, a small contingent of men who were tasked to capture the four-rotor Enigma. Fleming watched the unfolding disaster from a ship at safe distance, overseeing more successful attempts by this unit later on in the war.

The raid on Dieppe, another defining moment in Canada's history but this time in WWII, now emerges as a desperate effort to end an Enigma intelligence "blackout" that had the potential to turn the War of the Atlantic back into Germany's favour. Indeed, 1942 contained a ten-month period during which the Allies could no longer read U-boat messages in the Atlantic which were now encrypted with an additional (fourth) wheel inside the Enigma. Convoys no longer knew the positions of German "wolf packs", the highly destructive formations of U-boats, and a disturbing amount of convoy ships were sent to the bottom of the ocean again. Fortunately, Bletchley Park figured out how to break the four-rotor Enigma by the end of 1942, following a capture of the machine, and any further blackouts were avoided until the end of the war, in part because the Americans joined the codebreaking efforts with formidable computing power. This allowed the Allies during D-Day to track U-boat traffic in the English Channel and German army traffic within northern France, almost instantaneously at that point, thereby massively aiding a successful invasion of continental Europe that passed battlefields of WWI where the Enigma had some of its roots. The circle closed.

The Enigma story has left its marks on modern Canada and the modern world in various ways. It was arguably the first serious, semi-automated encryption device to be employed on a large scale. Its functionality, flaws in operation, vulnerabilities and associated codebreaking methodologies are intimately linked to modern encryption technologies. However, physicists are now trying to move beyond conventional encryption and utilize quantum mechanics to generate keys for encryption that only the sender and receiver can know. In conventional key exchange, anyone can, in principle, listen in on the communication without anyone else knowing about it. This is one reason for the use of a private key that is not being communicated but kept hidden by the receiver. In contrast, when exchanging keys in quantum encryption the sender and receiver will know if someone listens in on their communication which makes this type of encryption, again in principle, inherently secure.

A Canadian leader in the field of quantum encryption is the Waterloo region, home to many physicists and encryption experts but also BlackBerry Ltd., a company that has acquired serious encryption capabilities over the last ten years. Is it any coincidence then that one of the fathers of mathematics and combinatorics at the University of Waterloo was William Tutte (1917-2002), a famous graph theorist but also codebreaker at Bletchley Park? Tutte was instrumental in breaking the Lorenz cipher machine used by the German High Command, including Hitler. Based on his advances in understanding the inner workings of the Lorenz, a more complicated device than the Enigma, it was reverse-engineered at Bletchley Park without any Allies ever having laid eyes on a Lorenz. This intellectual achievement may very well rank above the Enigma cracking. And in the spirit of Turing's bomba, another electro-mechanical machine was built, this time to break the Lorenz cipher code efficiently. It was called the Colossus and is regarded by many as the first computer in the world.

Why did the Germans never suspect that their Enigma machine was compromised? Some were, in fact, suspicious and a respected mathematician by the name of Karl Stein was called back to Berlin from the Russian front to assess the situation. He concluded after a detailed analysis that the Army and Air Force Enigmas might be vulnerable but the more advanced Navy Enigma models could only be cracked with the use of hitherto unseen computational power. Stein's assessment was correct but he did not expect that the genius of Alan Turing was at work in Britain, a genius that would help shape the modern computer, computing science, and the notion of machine intelligence through his concept of an imitation game.

And this is how the Enigma spans from the trenches of Normandy to the beaches of Dieppe and on to modern university laboratories in Canada. There are few, if any, inventions that tie together history, warfare, people's lives and technological development in such unique ways as the Enigma machine. 1918 has changed us perhaps more than we thought.

- end-