The Invention of Enigma and How the Polish Broke It Before the Start of WWII

Slawo Wesolkowski
University of Waterloo
Waterloo, Canada

Cryptography in History

From the early days of distance-based communications, people have naturally tried to disguise messages being sent from one place to another to avoid their intentions being revealed to other parties whether they were friends or enemies. For example, Julius Caesar sent confidential letters to Cicero in secret writing, Mary, Queen of Scots, sent secret messages to her followers from her prison, and Jefferson invented an encryption device that was even used by the Americans in World War II (Kippenhahn, 1999). However, with the advent of secret messages came also attempts at deciphering them. It happened that Mary Stuart's secret messages were intercepted by Britain's then secret police and decoded. In one of the messages she approved of a conspiracy against Elisabeth I, which sealed her well-known fate.

It is then only natural that cryptography was also used in messages sent through a telegraph, the telephone and eventually radio. With the advent of long range communication methods using radio signals, the use of cryptography became very important especially for coordinating army movements. The French, British, American and German armies were actively using ciphers of various kinds during World War I. In fact, the United States became involved in World War I thanks to the British decoding of a telegraph from the German director of foreign affairs, Arthur Zimmermann, to the German ambassador to the United States, Count Bernstorff. In this telegram, the Germans were offering several southern states to Mexico in exchange for attacking the US and were suggesting that the Japanese should join the war as well on the German side.

Most of the pre-World War II message encryption methods relied on the shuffling of letters or on using number representations for each word. Linguistic-based methods were easily decipherable using frequency analysis. Numeral-encoded messages merely necessitated the capture of the codebook – the codeword dictionary. The emergence of Enigma greatly complicated decryption as it was a system which could not be decoded based on linguistic analysis of the cipher text and only required keeping the key secret – a far easier task than securing the large number of codebooks. In fact, to keep the system from being broken, the Germans first changed keys every three months until 1935, then monthly until October 1936. Thereafter, they changed it every day and in 1943 every eight hours. The subsequent decoding of the "invincible" German secret writing machine was one of the most important milestones of World War II together with the invention of the atomic bomb. Without breaking the Enigma, it is very likely the war would have had a much different course. Kippenhahn quotes Herbert Franke (Kippenhahn, 1999): "Historians are… cautious. At any rate, there seems to be unanimity that without radio intelligence – especially successful on the Allied side – the war might have gone on for another two years. But that, in all probability, would have meant the dropping of the atom bomb on Germany."

The Invention of Enigma

One of the milestones in the history of cryptology is the invention of an electro-mechanical cryptographic system called Enigma (see Figure 1). The concept on which it was based was introduced in 1915 by the American Edward Hebern (Harper, 1999). Hebern devised a machine-generated code by adapting a newly produced electric typewriter. The letters in the new machines were rearranged so that the printed letters would be different from the letters on the keyboard. He simply replaced one letter with another so that the word CRYPTOGRAPHY would be printed FGTDAEJGYDWT. This operation was of course easily reversible with an appropriate set of switches. However, code generated using this type of machine was easy to decode since all Western languages have a characteristic repetition rate of letters, whatever the text, and could be broken using frequency analysis. Hebern realised this and devised another machine with rotors, which switched the connections of the electronic typewriter each time a key was pressed (Harper, 1999). Hebern eventually sold this patented Electric Coding Machine to the US Navy in 1928[1].

The principle of the rotor was crucial to the development of Enigma (Kahn, 1991). A rotor is a wired codewheel with usually twenty-six evenly spaced electrical contacts around the circumference of the disc. Since each contact can represent a letter, the rotor embodies a cipher alphabet. Therefore, some other letter dependent on the rotor *position* will replace the input letter. If the rotor did not turn, each letter would have a corresponding encryption code as in Hebern's invention. However, each time a key was pressed the rotor would move one space or 1/26th of a revolution. Therefore, if a text consisted of the same letter the first and twenty-seventh letters would be encoded in exactly the same way. In this case, a rotor has a period of 26 letters. If several rotors are placed in series, the period will increase accordingly. For example, for four rotors, the period would be 26^4 or 456,976. The internal wiring of the machine was its basic secret.

The "one-time pad" was known as the only truly secure cipher method at the beginning of the twentieth century (Kozaczuk, 1984). However, it could not be used ubiquitously since to make the system secure it required pads to be distributed periodically to all the users. This method of encrypting information was limited to important communication nets in diplomacy and intelligence gathering. However, this type of encryption was not very practical for the use of armies. Therefore, the German armed forces started experimenting with perhaps not as secure but much more convenient cipher machines as early as 1918.

[1] There was a third inventor by the name of Arvid Gerhard Damm who also came up with the rotor concept in Sweden. After his death, the son of his partner, Boris Caesar Wilhelm Hagelin took over the company. He improved on the design (notably reducing the weight of the machine from thirty-seven pounds to three pounds) and sold 140,000 of his machines during the war to the Americans (Kippenhahn, 1999).

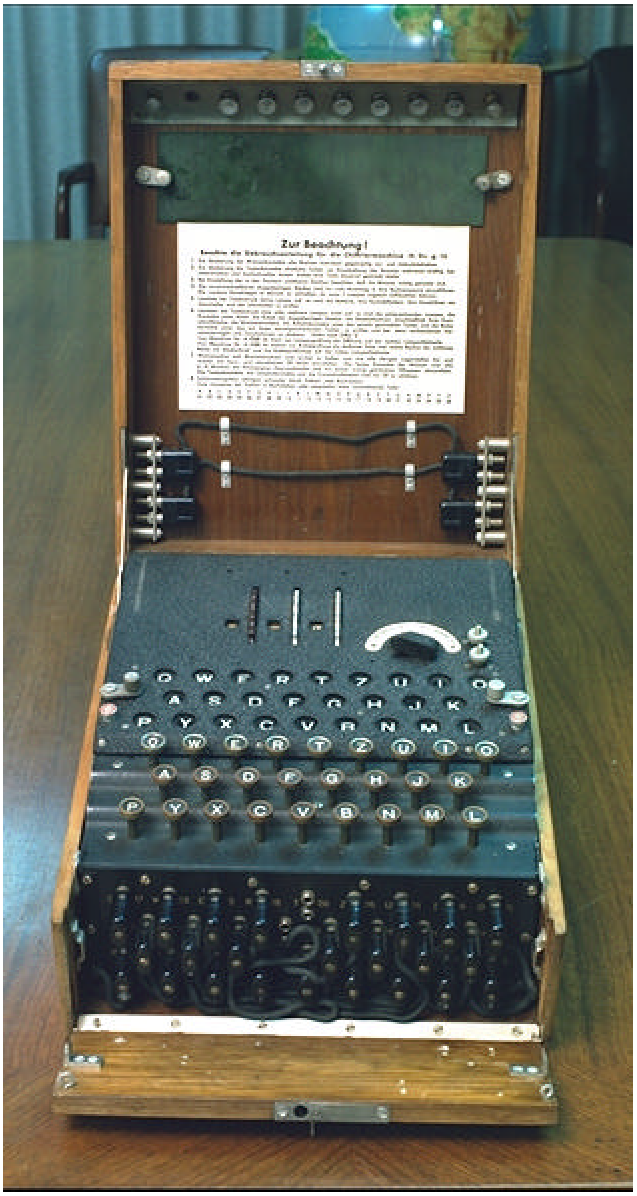

Figure 1: An Enigma cipher machine at the National Cryptologic Museum, National Security Agency, Washington, D.C., USA (source: NCM website).

A number of designs were considered including a multi-rotor machine devised by Dr. Arthur Scherbius. The memorandum he sent to the navy explained that thanks to the rotor principle, the enemy could not decipher the message even if the encoding machine was captured (Kahn, 1991). Furthermore, he asserted that given the knowledge of the message and the cipher code the encoding key could not be found. However, the navy decided not to buy his design even though it provided “good security even if compromised” “because with the present kind of naval cipher traffic, the use of machines is not worthwhile” (Kahn, 1991). Scherbius bought the patent for the *Geheimschiffrmachine,* the secret writing machine, invented by Dutchman Hugo Koch in 1919 (Harper, 1999). He improved on the design and in 1923 went into production with a machine he called “Enigma.” His improvements were to have three-rotors (Harper, 1999) and unequal rhythm in the movement of the rotors (Kozaczuk, 1984). This device was exhibited by the German Post Office at an International Postal Union Congress where it was touted to be an inexpensive and reliable means of safeguarding commercial cables and telegrams. This was noticed by the Cipher Department of the Reichwehr, the small army Germany was permitted under the Versailles Treaty. Col. Erich Fellgiebel ordered immediately its withdrawal from the commercial market. In 1926 the navy, and in 1928 the army introduced machines that were modified versions of the commercial Enigma model (Kozaczuk, 1984).

In 1930, a military version of Enigma was implemented with the commutator as the main innovation (Kozaczuk, 1984). This commutator was essentially a plugboard with twenty-six plugs and plug connections (Kahn, 1991). The plugboard would therefore add another substitution layer on top of the rotors. However, in this case not all the letters would be substituted. Only six of the letters would be connected to another set of six at any one time. For example, if the letters "A" and "T" would be connected, a letter in the message enciphered as "A" by the rotors would appear as "T" after being processed by the plugboard and vice versa. Even though only twelve letters where permutated in this way, it increased the number of possible cipher combinations by billions (Kahn, 1991).

Furthermore, to enable Scherbius' Enigmas to encode and to decode signals a reflecting cylinder was added. This device ensured that whatever signal was encrypted could be decrypted by typing in the coded message with the rotors set to the same initial position. This became the curse of the Enigma since having a machine that could encode a signal and then decode it with the same settings greatly limited the wiring configuration. The Germans did not notice this to the benefit of the Allies.

An Enigma cipher dispersed letters nearly perfectly thus short-circuiting any attempt at cracking the code using statistical calculations of frequencies of the letters of the alphabet (which could be done for earlier methods). A different set of methods had to be used to crack this new code.

The Technical University of Poznañ

The Polish Cipher Bureau - which was part of 2nd Section (Military Intelligence) of the General Staff – had already intercepted German ciphers in 1928 (right after the machine's introduction by the German army). That year, customs delayed a package sent to the German embassy in Warsaw (Harper, 1999). The Polish postal authorities insisted their offices could not be opened and the Cipher Bureau's agents examined a new military version of the commercial Enigma. However, it wasn't until 1932 that three brilliant Polish mathematicians began working for the Cipher Bureau. They were the twenty-seven year old Marian Rejewski (1905-80), the twenty-five year old Henryk Zygalski (1907-78), and the twenty-three year old Jerzy Ró¿ycki (1909-1942). How they came to be employed by the Polish intelligence services is an interesting story.

In January 1929, about twenty third- and fourth-year mathematics students at the University of Poznañ were sworn to secrecy before participating in a cryptography course (Kozaczuk, 1984). The secret course was given two nights a week (Kahn, 1983) at the University of Poznañ by Major Maksymilian Ciê¿ki (a military member of the Cipher Bureau), Antoni Palluth (a civilian employee of the Cipher Bureau) and Major Franciszek Pokorny (then-chief of the Cipher

Bureau). This course was meant to help Polish radio intelligence fight against its difficult German adversary. It was decided that the course would be conducted at the University of Poznañ due to people in this region knowing how to speak German well even though the university was not know as a mathematics center (Singh, 1999). Pomerania was a part of Germany for over 100 years since the partitioning of Poland by Prussia, Russia and Austria-Hungary in the late eighteenth century and Polish people living there had to attend school in German. Given the linguistic nature of many encryption methods it was indispensable that the students know how to speak the original language of the encrypted text namely German. This would prove to be an invaluable asset in the breaking of the Enigma as well.

A few weeks into the course, the students were given real German ciphergrams to solve (Kozaczuk, 1984). The students were told that this system had already been broken although for a time some consultants of the Polish Cipher Bureau had considered it unbreakable. The students were also told what the text was about which helped to narrow down the vocabulary used. A couple of hours later, some of the students including Rejewski, Zygalski and Ró¿ycki proved capable of decoding the message. As the course progressed, the ciphers became increasingly more difficult. Unsuccessful students started dropping out of the course and others decided they did not have enough skill to keep going. Only the above-named three students managed to reconcile their regular course work with the cryptography course. One of the exams was an actual German military communication expressed in the so-called "Double Dice" code that National Party (Nazi) foreign affairs expert Alfred Rosenberg had boasted was "insoluble" (PAJ, 1990). Rejewski, Zygalski and Rozycki, each acting on their own, broke the code. However, before the end of the course Rejewski left to study at the University of Göttingen where in the 1900's such luminaries as Gauss, Dirichlet, Poincaré and Planck had lectured.

In the summer of 1930, Rejewski came back to Poznañ where after the course ended the General Staff's Cipher Bureau set up in the underground vaults of the town's military command a suitably outfitted large room for decoding German messages. There the best students from the cryptography course were put to work. Rejewski also started working there in the fall. The laboratory was set up in such a way as to permit the students to keep doing their course work. Students would typically work 12-hour weeks selecting their own hours of the day or night. The "black chamber" was set up in the military command post for the convenience it afforded the students. The Mathematics Institute was after all a few paces away and students could come even for very short periods of time.

The students' task was to break the German encryption keys, which changed periodically. They were supplied with data from various radio signal-intercepting stations. Solving some of the more often used German military ciphers became routine. Furthermore, the young cryptologists learned how to use mistakes committed by German cipher clerks. One of these was for example the necessity to have a message of at least 50 characters. The students discovered that the Germans would actually pad shorter messages with the letter "X" and encode the composite signal. However, as time went by messages appeared in a cipher that could not be broken no matter what method was used. In the summer of 1932, the Poznañ outpost was closed and the cryptologist trio began work as employees of the Cipher Bureau in Warsaw.

The Polish Cipher Bureau (Polskie Bióro Szyfrów)

The Polish Cipher Bureau concluded that the Germans had begun using a new mechanical encryption device similar to that designed by Sherbius (Kozaczuk, 1984, & Kippenhahn, 1999). Since earlier attempts at cracking the code had been unsuccessful, Rejewski started by analyzing the six letter letters with which each enciphered message started (Kahn, 1983). However, to solve the equations he devised he needed information on the wiring of the rotors, the wiring of the plugboard, and the connections of the plug arrangements. He made the assumption that the order of the wiring between the keyboard and the rotors was the same as the order of keys on the keyboard. The Poles needed some more information on the military Enigma that was not so readily available.

The French and Czechoslovakian intelligence bureaus were also interested in reading German cryptograms. A loose working relationship was initiated between the three countries in December 1932. However, it was mainly the French and Polish teams who cooperated as Polish-Czechoslovak cooperation lasted only until 1936 (Kozaczuk, 1984). When Captain Gustave Bertrand, France’s Chief of the Bureau des Chiffres, arrived in Warsaw in December 1932 for what he later called a historical meeting, he brought with him documents detailing the inner workings of the Enigma. A year earlier, Hans Thilo Schmidt, an official of the Chiffrierstelle (the German Cipher Bureau) came to the French and offered to give them information in return for money (Kahn, 1983). The French at first did not trust him but soon Bertrand realized that Shmidt was telling the truth. Schmidt supplied the French with a copy of the German service instructions on the use of Enigma and the daily keys for September and October 1932 – i.e., the initial settings for the rotors, the ring settings, and the wiring of the plugboard.

However, this was not enough. Solving Enigma would prove to be a combination of precise linking of complex mathematical analysis with the intuitive reconstruction of individual parts. The Poles still did not know the internal wiring of Enigma. Having by then acquired a commercial Enigma, Rejewski assumed that the order of letters on the rings was the same as that on the keyboard of a German typewriter (and also the Enigma keyboard). However, this assumption proved to be a dead end and Rejewski thought that perhaps the letters were arranged in alphabetical order. Simple as it may sound, this was the correct ordering!

This was an incredible breakthrough. Kozaczuk quotes Bertrand in his book (Kozaczuk, 1983): “to [the Polish cryptologists] alone belongs all the credit and all the glory for having successfully carried through this incredible technical feat, thanks to their knowledge and perseverance, unequalled in any country in the world. They overcame difficulties that the Germans had thought ‘insurmountable,’ of which it is hard to give an idea.” Furthermore, Kozczuk quotes Deavours, a mathematician (Kozaczuk, 1983): “No doubt practitioners of group theory should introduce this property of permutations [exploited by Rejewski] as ‘the theorem that won World War II.’ [S]olving the Enigma traffic via statistical analysis, table lookups, or mechanical computation (the Poles used all three) was an immense undertaking – one that no other country was up to at that period of history.” The only methods available then outside of Poland were effective only against Enigmas without a plugboard. It is interesting to note that British and French cryptanalysts were not up to the task. Singh attributes this to an over-confidence and lack of motivation in the wake of World War I (Singh, 1999). He notes that the French “did not even bother trying to build a replica of the military Enigma machine because they were convinced that achieving the next stage, finding the key required to decipher a particular Enigma message, was impossible."

The Poles lead by Rejewski, on the other hand, managed to reconstruct the military Enigma theoretically. This enabled the Poles to build exact Enigma doubles (the AVA Radio Manufacturing Company was commissioned with building them). However, let's not forget that the keys were changing daily by then and that it was still necessary to find ways of determining what a particular key was. Rejewski and the other two mathematicians devised ways from multiple intercepted signals of deciphering the keys. What was helpful in this was the discovery that the reflecting cylinder would not permit letters to be encoded as themselves (i.e., a letter from the original text had to be encoded as a different letter). This greatly reduced the number of possible keys. Furthermore, the Poles needed at least 80 intercepts collected on the same day using the same setting on the German cipher devices for finding the actual keys.

The "Bomba"

The part of group theory concerned with the permutation of groups was very useful to the Poles (Kozaczuk, 1983). Rejewski described later in detail the methods used in solving the Enigma (Rejewski, 1979). In 1934, Rejewski developed what he dubbed the "cyclometer." This was a device which allowed a speedier recovery of daily keys by setting up a catalogue of combinations produced by the first two rotors. There were 105,456 (6 x 26^3) entries in this look up table. The cryptologists could then just look for the appropriate settings by comparing the intercepts to the entries in the table. However, after September 15, 1938, the Germans radically changed the way they encrypted messages (Kozaczuk, 1983). Now, the operator himself would select the basic position of the rotors, a new one each time, for enciphering the message key.

In mid-October 1938, Rejewski worked out a mathematical model for a device to decode keys automatically that was vastly superior to the cyclometer as it could analyze 17,576 key combinations in a two-hour period. The "bomba" or bomb in English as it was called was an electro-mechanical combination of six Polish Enigma doubles with additional devices and transmissions. It automatically stopped when the rotors aligned in the sought-after position. Thus, by setting the six initially built bombs in motion the daily keys could now be recovered in an astounding two hours! Rejewski's invention was first realized within a couple of weeks by the AVA Radio Manufacturing Company, the same company which built the Enigma doubles earlier. This achievement was supplemented with the discovery by Zygaliski of how to break the individual message keys now being used by the Germans using perforated sheets (Kozaczuk, 1983).

On December 15, 1938, the Germans yet again modified the encryption mechanism by adding a fourth and a fifth rotor to the Enigmas. This new enhancement made the Enigma invulnerable again especially given the new encoding methods introduced earlier in September 1938. However, the Poles had a lucky break. The S.D. (the SS Security Service) continued to broadcast signals on their frequencies the old way until July 1, 1939. In the first few days of January 1939, the Polish mathematicians were able to reconstruct the connections in the fourth and fifth rotors. However, the Germans introduced yet another change later that month: they increased the number of plugboard connections (i.e., letters connected on the plugboard). Now, perhaps more than sixty bombs were required to crack the code quickly. The Poles realized that they needed to get help from the French and the British.

Epilogue

In July 1939, the Poles met with the French and the British and gave each of the delegations two Enigma doubles, "bombas" and all they knew about Enigma. The British delegation was literally left speechless at this astounding development for they had not up to that time been able to crack the German code (Kozaczuk, 1983). However, it is peculiar that the British did not use Rejewski's nor Zygaliski's talents (Ró¿ycki had died crossing the Mediterranean from France to Algeria) when they finally made it to Britain via Romania, France, Spain, and Algeria (Kippenhahn, 1999). Later on, they did not give even any credit to the Poles for solving the early Enigmas, which is quite evident by the books published on accounts of the work done at Bletchley Park including the famous "The Ultra Secret" by Winterbotham (Winterbotham, 1974). There is rarely mention of the polish contribution and when it is there it is very much underrated (Hinsley and Stripp, 1993). It is very likely that without the Polish help the Allied side would have had much more difficulty in breaking the later versions of the Enigma and it is quite possible that the war would have continued much longer until perhaps the dropping of the atom bomb on Germany. After all, none of the Allied countries including the United States, Britain and France were able to decrypt German signals before the war started.

References

Stephen Harper (1999). *Capturing Enigma: How HMS Petard Seized the German Naval Codes*. Sutton Publishing, Phoenix Mill.

F. H. Hinsley and Alan Stripp (1993). Codebreakers: The inside story of Bletchley Park. Oxford University Press, Oxford.

David Kahn (1983). *Kahn on Code*. MacMillan, New York.

David Kahn (1991). *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943*. Houghton Mifflin, Boston.

Rudolf Kippenhahn (1999). *Code Breaking: A History and Exploration*. The Overlook Press, Woodstock.

Wladyslaw Kozaczuk (1984). *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two*. University Publications of America.

PAJ (1990). "The Enigma: The Secret Weapon of World War II," *Polish American Journal*. (http://www.polamjournal.com/Library/APHistory/enigma/enigma.html)

Marian Rejewski (1979). "The Mathematical Solution of the Enigma Cipher," as an appendix to Kozaczuk's *W kregu Enigmy*, pp. 369-93 (also as Appendix E in Kozaczuk, 1983).

Simon Singh (1999). *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*, Doubleday, New York.

F. W. Winterbotham (1974). *The Ultra Secret*, Harper & Row, New York.