12-2-2022

The History of the Enigma Machine

Jenna Siobhan Parkinson
Western University, jparkin9@uwo.ca

The History of the Enigma Machine

Jenna Parkinson

December 2, 2022

1 Introduction

The history of the Enigma machine begins with the invention of the rotor-based cipher machine in 1915. Various models for rotor-based cipher machines were developed somewhat simultaneously in different parts of the world. However, the first documented rotor machine was developed by Dutch naval officers in 1915. Nonetheless, the Enigma machine was officially invented following the end of World War I by Arthur Scherbius in 1918 (Faint, 2016).

2 The Mechanics and the Operation of the Enigma Machine

An Enigma machine has a keyboard with 26 keys corresponding to 26 letters, with no punctuation symbols or digits. In place of a space, the letter "X" is typically used and sentences are generally separated by the letter "Y". Below the keyboard, there is a plugboard, which is responsible for the enhancement of the security of the encipherment. Pairs of letters connected by a plugboard lead are called *Stecker partners* while the unconnected letters are referred to as *self-Steckered*. Above the keyboard, there is a bulb board that indicates the enciphered letter corresponding to each key typed. Additionally, there are three to five rotor wheels above the bulb board, each containing a movable ring. These wheels are called rotor scramblers. A ring clicks into one of twenty-six positions on the wheel. When a key is pressed, an electrical circuit within the machine closes, allowing a current to flow through the plugboard and the three wheels until it reaches a reflector. The reflector changes the direction of the current to flow back through the three wheels in reverse order, then through the plugboard to light a light bulb on the bulb board. Simultaneously, pressing a key rotates the rightmost wheel one twenty-sixth of a turn. A pin then rotates the middle wheel one twenty-sixth of a turn once the rightmost wheel completes a full rotation. Similarly, a pin rotates the next wheel one twenty-sixth of a turn when the previous wheel completes a full rotation. Thus, an Enigma machine produces a polyalphabetic substitution cipher whose substitution period depends on the number of rotor scramblers in the machine. For example, a machine with three

rotor scramblers has a substitution period of

$$26 * 26 * 25 = 16,900, \tag{1}$$

(as opposed to

$$26 * 26 * 26 \tag{2}$$

to account for the double stepping mechanism that occasionally moves the middle and left wheels simultaneously). A 3-rotor scrambler could be set in

$$26 * 26 * 26 = 17,576 \tag{3}$$

different ways. Since there are $3! = 6$ ways to arrange the rotors and 26 possible starting positions for each of the three wheels, there are

$$6 * 26 * 26 * 26 = 105,456 \tag{4}$$

possible orderings. If a machine has L leads on the plugboard, the amount of possible pairs of letters that can be interchanged is

$$\frac{26!}{(26 - 2L)! * (L!) * (2^L)} \tag{5}$$

(Durand-Richard, 2019).

3 Example of the German Enigma Protocol

Typically, German encipherments consisted of the use of two keys: a daily key, and a message key. For example, if the sender were to select the message key *NHK*, they would first have to set the Enigma machine to the daily key, then encrypt *NHKNHK*. Suppose that for a given daily key, the encrypted message produced is *FJBRMZ*. The sender would then move the rotors to the *NHK* position, and encipher the message. Then, the message receiver would enter *FJBRMZ* into their machine which would have been set up with the daily key ahead of time. If the process was executed correctly, the receiver would be presented with the repeated message key, *NHKNHK*. Then, they would move the rotors to the *NHK* position and would be able to decrypt the given ciphertext (Evans, 2019).

4 Polish Mathematics and Cryptanalysis in the 1930s

4.1 The Clock Method

From 1933 to 1936, Polish cryptanalysts used a more classical approach when deciphering German codes. They found that if two German texts were superimposed one over another, on average one identical letter among 13 letters was

observed. Thus, the same frequencies occurred if the two texts had undergone the same substitutions and if the texts had both undergone distinct random substitutions, or were comprised of random sequences of letters, only one identical letter out of 26 could be observed on average. Hence, they could determine when the middle rotor of the machine rotated by counting the amount of identical letters present. This method is referred to as the "Clock Method", it was created by Polish mathematician and cryptologist Jerzy Różycki. Manual methods took a long time to implement and did not always result in complete solutions, so more efficient approaches were developed (Durand-Richard, 2019).

4.2 The Cyclometer

In 1936, the Germans increased the number of pairs of letters swapped on the plugboard from five to between six to eight. This greatly increased the complexity of their Enigma encipherments. Thus, it became more difficult to use the methods that depended on the fact that the plugboard did not swap every letter. Polish mathematician Marian Rejewski began to refocus his research on the method of double encipherment of the cryptographic key which was heavily used by the Germans. He was able to detect a pattern that showed that the first and fourth, second and fifth, as well as the third and sixth letters were the same. This discovery was achieved through the analysis of the Enigma code as a function that takes plaintext letters and returns the letters as ciphertext. For each character position in the text, the Enigma machine used a different permutation. Starting with the daily key in the basic position, the first six letters were enciphered using the first six permutations for the day. These first six permutations were labeled **A**, **B**, **C**, **D**, **E**, and **F** (Evans, 2019).

4.3 Rejewski's Attack Method

To describe Rejewski's attack method, return to the example in section 3. It was found that the first six letters of each message formed the message key, twice enciphered. The group tasked with decyphering the code would not know that the message key was *NHK*. They would however, know that the first six letters of the intercepted message were *FJBRMZ*. Denoting the first and therefore fourth letter of plaintext by x, it could be found that $\mathbf{A}(x) = F$, and $\mathbf{D}(x) = R$ using the permutation method. Since Enigma ciphers are reciprocal, if $\mathbf{A}(x) = F$, then $\mathbf{A}(F) = x$. The composition $\mathbf{D} \circ \mathbf{A}$ is given by

$$\mathbf{D} \circ \mathbf{A}(F) = \mathbf{D}(\mathbf{A}(F)) = \mathbf{D}(x) = R. \tag{6}$$

Thus, it can be shown that $F \rightarrow x \rightarrow R$. The same logic can be used for **BD** and **CF** to show that $J \rightarrow M$ and $B \rightarrow Z$, respectively. If a sufficient amount of encrypted messages were intercepted, generally all the letters of the alphabet would occur in all six places in the opening of the messages. Rejewski then wrote out the first six letters of every intercepted message separately. These were the message keys twice enciphered. As described above, these keys had

the same letter in the first and fourth, second and fifth, and third and sixth positions. A key could then be selected randomly and its first and fourth letters would be written side by side. Then, Rejewski would find a key with the fourth letter of the previous key as its first letter. He would then write the fourth letter of the new key beside the fourth letter of the previous key. This process would be repeated until, after a finite number of steps, the first letter written was encountered once again. The second time the letter showed up in the decryption, the repeated letter would not be copied and the letters that were written beforehand would be enclosed in parentheses. Through this process, the full composite cipher of **AD** could be found. These composite ciphers would have the form

$$\mathbf{AD} = (dvpjJ2xgzyo)(eijmunqZht)(bc)(rw)(a)(s). \tag{7}$$

A similar approach would be used with the second and fifth, and the third and sixth letters of the keys to find the composite ciphers of **BE**, and **CF** respectively. The collection of ciphers are permutations given by the transformations of the set of letters onto themselves. The permutations can be represented as disjoint products of cycles assuming a characteristic form which is generally different every day. However, it was found that although the representation of the structures was different each day, each line in the cycles of the same length always appeared in pairs. This was referred to as the *characteristic structure* of a given day (Rejewski, 1981).

5 Weaknesses of Enigma Ciphers

As groundbreaking as Enigma ciphers were at the time, there were some weaknesses present in the system which were exploited by cryptanalysts when deciphering encrypted messages. The first was that a letter could never be encrypted to itself. This is due to the reflector mechanism in the machine. This property was useful when cryptanalysts had access to sections of plaintext thought to be present in the larger ciphertext. Here, a *known-plaintext attack*, which is an attack model where the attacker has access to pairs

$$(P_i, C_i), i = 1, ..., N \tag{8}$$

of known plaintexts and their corresponding ciphertexts, could be exploited in order to rule out possible locations of certain letters in ciphertext (Biryukov, 2011). Another weakness of the machine is the fact that connections on the plugboard are reciprocal. This is due to the fact that the Enigma machine exchanges letters in pairs. For example, if A is connected to C, then C is connected to A. This weakness made retrieving the plaintext from the encrypted message very convenient for the encryptor as the machine would require the same positioning for encrypting and deciphering messages (Faint, 2016).

6 World War II

The Enigma machine was heavily exploited by the Nazi Party in World War II. Hitler's surprise attacks using rapid, overwhelming force were facilitated through well organized collaboration between the German forces, ensured by the speed of their communications. Enigma played a crucial role in the secure flow of information between the air forces and the ground forces, as well as between the front lines to the rear. Many command vehicles were supplied with compact, battery-operated Enigma machines. The device was used as the primary source cryptosystem for all units below Army level in the German armed forces (Mowry, 2003). Many of the shortcomings that lead to the Allies ability to break the Enigma codes used by the Germans were a result of the way the machine was used. The Germans repeatedly used the X key as a spacer between words and many stereotypical expressions were reused in messages, such as ANX which was used as the German word for "to". Additionally, the Germans only used six plugboard leads, which left 14 letters *unsteckered*. These weaknesses in the encipherment process were found and used in the decryprion of German messages in Allied countries in World War II (Durand-Richard, 2019).

6.1 Bletchley Park

Bletchley Park, an estate in Buckinghamshire (now Milton Keynes), England became the primary centre of Allied codebreaking during World War II. The property housed the Government Code and Cypher School (GCCS) which decoded the secret communications of the Axis Powers. The crucial part of the Enigma research at Bletchley Park involved reducing the large number of possible rotor positions and their initial positions. This was done both manually and mechanically. Once the number of positions is reduced, vulnerabilities of the cryptographic system could be analyzed systematically, which resulted in specific methods to find indicators in the secret messages. Often, the German radio operators would make procedural errors such as forgetting to change the daily message key, due to a lack of time. The process of finding discovering such vulnerabilities was called "gardening" by the British cryptanalysts (Durand-Richard, 2019).

6.2 The Herivel Tip

Codebreaker John Herivel speculated that German operators often set the ring settings when the rotors were already in the machine and using the letters appearing in the initial rotor position instead of choosing the letters randomly. In some cases, the operators would also only move the rotors a few notches. If a significant amount of operators were exploiting these practices, it would greatly reduce the number of possibilities for each letter from 17,576 to about 30 (Smith, 2011). The exploitation of German over-confidence to break Enigma code became known as the Herivel Tip to some of the staff at Bletchley Park. Codebreakers implemented the Herivel Tip for weeks with no success until the

Germans invaded France in May 1940. From that point on, it never failed (Durand-Richard, 2019).

6.3 *'Banburismus'*

Developing methods to reduce the time spent breaking the Enigma code led to the creation of a probabilistic approach to the problem. Alan Turing developed a method called *Banburismus*. This approach extended the clock method discussed in section 4.1. The clock method and Turing's *Banburismus* are similar in the sense that both aim to attack a cipher by the index of coincidence, a method developed by American cryptographer William Freidman, which involved placing two enciphered texts next to each other and counting the number of times that identical letters appear in the same position in both texts (Champaigne, 1955). Since the initial rotor positions were given for an entire day, the rotor positions could be the same as their starting positions for another message. If this occurred, the parts of the two messages encrypted with the same rotor positions were said to be 'in depth' and the letters were repeated at a rate of 1/17. To compare two messages in depth, each would be punched onto a card that was the same length as the message. The letters of the alphabet would be written in consecutive columns along each card and a hole would be perforated for each consecutive letter of each message. Then, the two messages would be superimposed over a light, which would shine through the cards where repeated letters occurred. The positions where the light shone through the card were called 'a fit'. Approximately 200 messages were required for this method to be efficient. A large staff was hired and trained to carry out this method, which began its use in March 1940. The first successful use of this procedure was May 8, 1940, and in autumn 1941 *'Banburismus'* began running at full efficiency, where 400 messages would be read daily. This technique was used until September 1943, when more efficient methods could be used instead (Durand-Richard, 2019).

7 Conclusion

Breaking the Enigma code was a great challenge before and during World War II. The work of many mathematicians and engineers was vital to the its success, where cryptanalytic methods had to be developed using mathematics and logic to surpass the increasing number of possible encryption combinations of Enigma. Many of the methods exploited during World War II relied heavily on human computation. After the war, the focus shifted to building computers and Alan Turing developed the theoretical Turing machine which would become very important in the field of cryptography with the development of programming languages.

References

Biryukov, A. (2011). Known Plaintext Attack. In: van Tilborg, H.C.A., Jajodia, S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5906-$5_5$88

Champaigne, H. H. (1955, January). The Index of Coincidence. Retrieved from https://www.cryptomuseum.com/people/friedman/files/NSA$_T IOC_1$955.*pdf*

Durand-Richard, M., amp; Guillot, P. (2019). From Poznan to Bletchley Park : the history of cracking the ENIGMA machine. CIIT Lab Workshop on History of Cryptography, Faculty of Electronc Engineering. https://doi.org/http: ciitlab.elfak.ni.ac.rs

Evans, H. A. (2019). Recreation of the Polish Cyclometer and Its Role in the Breaking of Enigma. http://www.eng.cam.ac.uk/uploads/news/files/recreation-polish-cyclometer-and-its-role-breaking-enigma-hal.evans.pdf

Faint, S. (2016). The Enigma History and Mathematics. UWSpace. https://doi.org/http://hdl.handle.net/10012/11023

Mowry, D. P. (2003). German cipher machines of World War Ii. National Security Agency, Center for Cryptologic History.

M. Rejewski, "How Polish Mathematicians Broke the Enigma Cipher," in Annals of the History of Computing, vol. 3, no. 3, pp. 213-234, July-Sept. 1981, doi: 10.1109/MAHC.1981.10033.

Smith, M. (2011, February 13). John Herivel obituary. The Guardian. Retrieved November 14, 2022, from https://www.theguardian.com/world/2011/feb/13/john-herivel-obituary