Implementation of the Enigma Machine

Ramit Bathula
CSE Department
PES University
Bangalore, India
bathularamit@gmail.com

R Shailesh
CSE Department
PES University
Bangalore, India
shaileshrajendran@gmail.com

Abstract: This project entails the working of The Enigma Machine, which was built during the Second World War and created by Arthur Scherbius and Richard Ritter. The Enigma had a very sophisticated method of encrypting and decrypting messages, and it took a lot of hard work to break its code. This project covers the implementation of the machine using a simple program in Python.

Key Words - Enigma, Encryption, Decryption, Rotors, Reflector

I.INTRODUCTION

[4] Cryptography is a technique to achieve the confidentiality of messages. During the 2nd World War encryption of messages was one of the most important tools/techniques to win the war. The Germans were keen on keeping their messages as secure as possible during the war, so they used a very powerful encrypting device which was deemed as one of the most powerful encrypting devices of its time

II. HISTORY OF THE ENIGMA

[2] The Enigma was built by Arthur Scherbius and Richard Ritter. It was first built for commercial purposes from the early 1920s and adopted by military and government services of several countries, most notably Nazi Germany before and during World War II. Several different Enigma models were produced, but the German military models, having a plugboard, were the most complex. With its adoption by the German Navy in 1926 and the German Army and Air Force soon after, the name *Enigma* became widely known in military circles.

There were various versions of the Enigma that were built for various purposes. The first Enigma machine built by Scherbius and Ritter, in the year 1953, was called a printing Enigma (Schreibende Enigma) as it printed the ciphertext onto a piece of paper.

This wasn't a very cost-effective machine as the paper was very expensive at that time and the machine had a lot of technical issues. For this reason, Scherbius developed a machine that produced its output on a lamp panel rather than on paper. The first model was the Enigma A that was introduced in 1924. It was also known as *Gluhlampenmaschine* (glow lamp machine).

In 1926, the design of the glow lamp Enigma was improved. The German keyboard layout (QWERTZ...) was introduced. Furthermore, the reflector (UKW) could be set to 26 different positions. The machine became known as the Enigma D.

The military Enigma was later built and was an improvement over the commercial one. It had a plugboard (Steckerbrett) as well which made it exponentially harder to decrypt messages that were encrypted by it. It was ready in 1932 and it had a double-ended plugboard. The sales of the commercial enigmas across international borders from this point had to be authorized by the German military.

III. PARTS OF THE ENIGMA

[2] The Enigma is made up of mainly four parts. The keyboard (User Interface), the Plugboard also called the Steckerbrett in German, the different rotors, and finally the reflector. All these parts are very crucial for the complete working of the Enigma.

A. The User Interface/ Keyboard

The user interface is a very simple keyboard of 26 letters, corresponding to the 26 letters in the alphabet. It is used to insert the input into the machine. But also, the pressed keys activate a mechanism that changes the state of the first rotors, rotating it with one unit, thus changing the encryption key after every press of a certain button. The interface also displays the final encrypted character to the user by lighting up the respective character displayed on the keyboard, after it has passed through the various rotors and the reflector.

B. Plugboard (Steckerbrett)

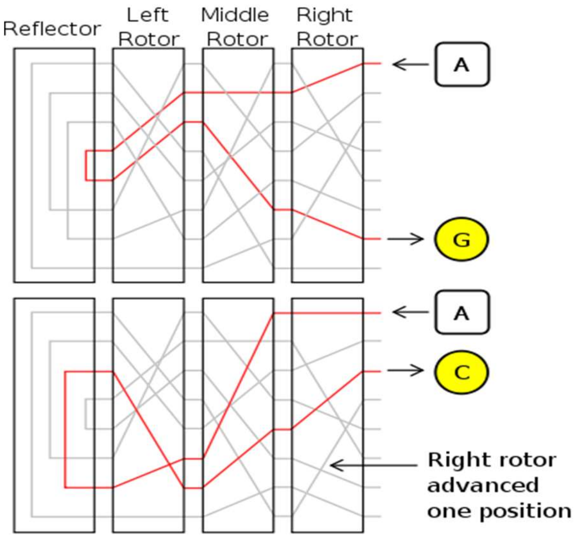
The Steckerbrett is a tableau of sockets that was created to make the decryption mechanism harder. But it was the weakest part of the machine. It is a mechanism that connects 2 letters one from the input layer and another from the output layer. That encodes the input letter as the output layer connected to it, without using the next parts of the machine. However, even if such a letter is pressed the rotors are turned anyway. Enigma I, Enigma II, and Enigma M4 are the only models that have a steckerbrett at the front. The Steckerbrett was manufactured exclusively for the German Armed Forces and was patented by the Reichswehr, which is why it was not available to other Enigma users.

C. The Rotors

The rotors are the most important part of the Enigma as it does most of the encrypting. The rotors are special gears with 26 pins. Every pin is related to a letter in the English alphabet. Inside the body of the rotor, 26 wires connect each pin on one side to contact the other in a complex pattern. The Army and Air Force Enigmas were used with several rotors, initially three. Later, this changed to five, from which three were chosen for a given session. Rotors were marked with Roam numerals to distinguish them: I, II, III, IV, and V, all with single notches located at different points on the alphabet ring. This variation was intended as a security measure.

D. The Reflector

The reflector adds an extra layer of encryption to the Enigma and it's one of the main features which make the enigma unique. The reflector takes the character from the third rotor and maps it to the respective character for that particular letter.



IV. THE MATHEMATICS INVOLVED

The Enigma transformation for each letter can be specified mathematically as a product of permutations. Assuming a three-rotor German Army/Air Force Enigma, let *P* denote the plugboard transformation, *U* denote that of the reflector, and *L*, *M*, *R* denote those of the left, middle and right rotors respectively. Then the encryption *E* can be expressed as:

$$E = PRMLUL^{-1}M^{-1}R^{-1}P^{-1}.$$

Combining three rotors from a set of five, each of the 3 rotor settings with 26 positions, and the plugboard with ten pairs of letters connected, the military Enigma has *158,962,555,217,826,360,000* different settings (nearly 159 quintillion or about 67 bits). As we can see, the number of possible combinations that can be achieved by the Enigma is so high that any conventional method of deciphering the text will take an extremely long time(decades).

V. THE WORKING OF THE ENIGMA

The Enigma is first set to the preferred setting and then the user can type in the required text. Once the user types a character the corresponding encrypted character will glow on the device.

Once a key is pressed several encryptions take place.

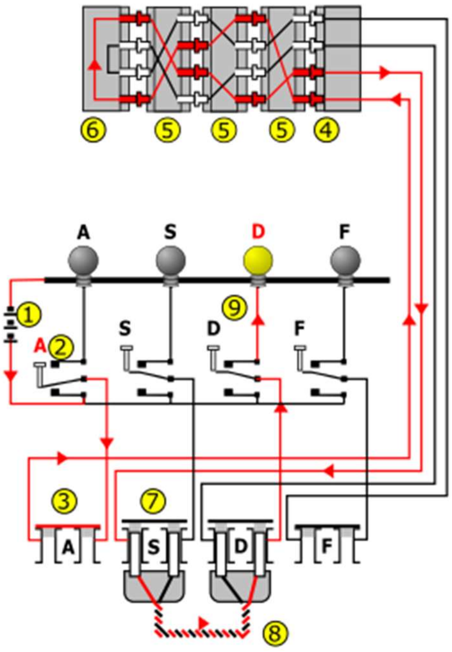
At first, the pressed key will be matched with its corresponding letter from the plugboard. This matched letter is then fed as input into the first rotor which uses a substitution cipher to encrypt the key. For every 26 movements of the rightmost rotor, the middle rotor moves once and for every 26 moves of the middle rotor, the left-most rotor will move once. There is also a notch on every rotor, and when the rotor aligns with this notch, the adjacent rotor rotates once. This was done to achieve a high level of encryption. After passing through the 3 rotors, the reflector maps the key to its corresponding reflective character that was given by the user. The reflector then sends the key back into the final rotor and this sends a signal to the second and that will send it to the first. Since we have a double-ended Plugboard, the encrypted key will get mapped one final time to its corresponding character from the plugboard and the final encrypted character will be shown by a glowing bulb.

A. The Electrical pathway

An electrical pathway is a route for current to travel. The mechanical parts act by forming a varying electrical circuit. When a key is pressed, one or more rotors rotate on the spindle. On the sides of the rotors are a series of electrical contacts that, after rotation, line up with contacts on the other rotors. When the rotors are properly aligned, each key on the keyboard is connected to a unique electrical pathway through a series of contacts. Current, from a battery, flows through the pressed key, into the newly configured set of circuits and back out again, ultimately lighting one display lamp, which shows the output letter.

Current flows from the battery to the plugboard. Next, it passes through the plug "A" (3) via the entry wheel (4), through the wiring of the three installed rotors (5) and enters the reflector (6). The reflector returns the current, via an entirely different path, back through the rotors (5) and entry wheel (4), proceeding through plug "S" (7) connected with a cable (8) to plug "D", and another switch (9) to light the appropriate lamp.

The repeated changes of the electrical path through an Enigma scrambler implement a polyalphabetic substitution cipher that provides Enigma's security. The diagram on the right shows how the electrical pathway changes with each key depression, which causes rotation of at least the right-hand rotor. Current passes into the set of rotors, into and back out of the reflector, and out through the rotors again.



VI. HOW THE ENIGMA WAS DEFEATED

[3] The Enigma machine had its flaws which led to the allies cracking the enigma.

The first flaw was the daily transmission of the weather reports. The German boats in the Atlantic communicated with the European stations about the daily weather because the weather reports were important information as they helped the German U-boats to plan their attacks on the Atlantic convoys. The transmission always started with the same wordings every day and hence this helped the allies in a major way in cracking the enigma.

The second flaw was one of the major reasons how the Enigma was cracked. The second flaw is when encrypting the same alphabet cannot be used to encrypt itself. For example, XYZ encryption with "XYZ" is not feasible, and it led to a massive flaw in the encryption. British mathematicians and scientists used this rule to develop their encryption method. Under this rule, messages can be encrypted with the same character. For example, every day when the transmission starts, British scientists looked for the word "Weather" in an encrypted format.

Even with knowing the first word being "Weather", it is still mathematically impossible to decrypt it.

Mathematicians and scientists realized that to break the enigma they needed a machine as it will be practically impossible to solve it by humans alone.

Alan Turing devised a machine that would be called the "Bomb". When the weather word's encrypted match is found, it's fed to the bomb, which ran all combinations and output the configuration of the Enigma for that day. The code breaker kept their secret and only released decrypted information for critical operations. By the end of the war, about 600 Bombs were operating from either side of the Atlantic. These decrypted messages were called Ultra.

VII.CONCLUSION AND FUTURE WORK

The Enigma was one of the most brilliantly devised encrypting machines of its time and hence even to this day people still find it a piece of art. It took many scientists to come up with an idea to break the Enigma code. Although it was broken, it did show that a powerful encrypting algorithm can secure data. With recent advancements in technology security of data is one of the most integral parts of data communication.

The Enigma can not only be seen as a weapon used by the German military but also as the inspiration for the encryption of data.

Any future work would involve finding new algorithms and using new ciphers to make it harder to break the enigma code.

VIII. ACKNOWLEDGEMENT

We are extremely grateful to PESU ISFCR for giving us this wonderful opportunity which enabled us to learn a lot in this domain. It was a great experience being able to learn more about the enigma machine and how it helped change the Second World War. We would like to convey our sincere gratitude to Prof. Vineetha B, Assistant Professor, Dept. of CSE, PES University, Bengaluru for always inspiring us to conduct regular research for this project.

VIII. REFERENCES

[1] https://pypi.org/project/py-enigma/

[2] https://enigmamuseum.com/

[3] https://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code

[4] https://brilliant.org/wiki/enigma-machine/

[5] ELEN, A. Enigma(ch-2,3,4), the invention of the enigma machine, 2014.

[6] A review on mathematical strength and analysis of Enigma Kalika Prasad and Munesh Kumari.