THEORY OF COMPUTATION

PROJECT REPORT

A SIMULATOR OF A ENIGMA MACHINE.

Submitted To: Anurag Goel Sir.

Submitted By: Kritesh Rauniyar (2K19/CO/196)

Manav Agrawal (2K19/CO/216)

Abstract

ENIGMA has a very inspiring story as it shows how mathematicians can save lives. It is one of the most famous cipher machines of all time. It's a code machine called the Enigma machine used by Nazi Germany in World War II to send secret, coded messages.

The Enigma machine was invented by the German engineer Arthur Scherbius at the end of World War I. This was unknown until 2003 when a paper by Karl de Leeuw was found that described in detail Arthur Scherbius' changes. The German firm Scherbius & Ritter, co-founded by Arthur Scherbius, patented ideas for a cipher machine in 1918 and began marketing the finished product under the brand name Enigma in 1923, initially targeted at commercial markets. The name is said to be from the Enigma Variations of English composer Edward Elgar. Early models were used commercially 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. Japanese and Italian models were also in use. With its adoption (in slightly modified form) by the German Navy in 1926 and the German Army and Air Force soon after, the name Enigma became widely known in military circles. Pre-war German military planning emphasized fast, mobile forces and tactics, later known as blitzkrieg, which depend on radio communication for command and coordination. Since adversaries would likely intercept radio signals, messages had to be protected with secure encipherment. Compact and easily portable, the Enigma machine filled that need.

1 Introduction

The Enigma machines are a series of rotor cypher machines that use electro-mechanical rotors. The earliest devices, built by German engineer Arthur Scherbius at the close of World War I, were primarily employed to secure commercial, diplomatic, and military communication. Enigma devices grew in complexity and were widely employed by the German army to encrypt radio messages during World War II.

ENIGMA had 158,962,555,217,826,360,000 combinations of encryption of string.

An enigma is made up of four major components: a user interface, a Steckerbrett, three rotors, and a reflector. Each component performs a specific function, but when combined, they can encrypt a message in such a way that it may be hard to decrypt without knowing the enigma's original parameters.

The anatomy of an Enigma

The user interface	Stackerbrett	The Alpha Rotor	The Beta Rotor	The Gama Reflector	The Reflector
	A <-> Y M <-> Z -------- T <-> O	A B C D E - - - x z	A B C D E - - - x z	A B C D E - - - x z	Z X - - - E D C B A

One of the most important characteristics of enigma is that for proper decryption, the user requires the enigma's initial settings from when the message was encrypted. If one parameter is different, the work becomes difficult to complete.

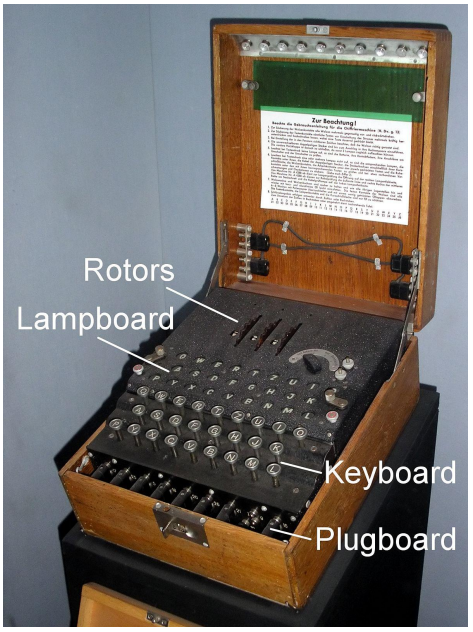


Fig: Enigma

2 User Interface

Each letter of the alphabet is represented by 26 keys on the keyboard. It is used to feed data into the machine. However, pressing certain keys activates a system that modifies the state of the first rotors by rotating it by one unit, hence altering the encryption key after each press of a specific button.

2.1 Steckerbrett / Plugboard

Another technique developed to make the decryption mechanism tougher is the steckerbrett / plugboard, which is a tableau of sockets. In reality, it was the machine's weakest link. It's a system that joins two letters from different layers, one from the input layer and the other from the output layer. This encodes the input letter as the output layer associated with it, without requiring the use of the machine's subsequent components. Even if such a letter is pressed, the rotors are still rotated.

Short wires are used to link pairs of letters that will be permuted to set up the keyboards. Because a (red) wire is used to connect these two letters/plugs, the letter W will be replaced with a D and the letter D with a W in the illustration below. Similarly, the letter V will become the letter Z, and the letter Z will become the letter V.

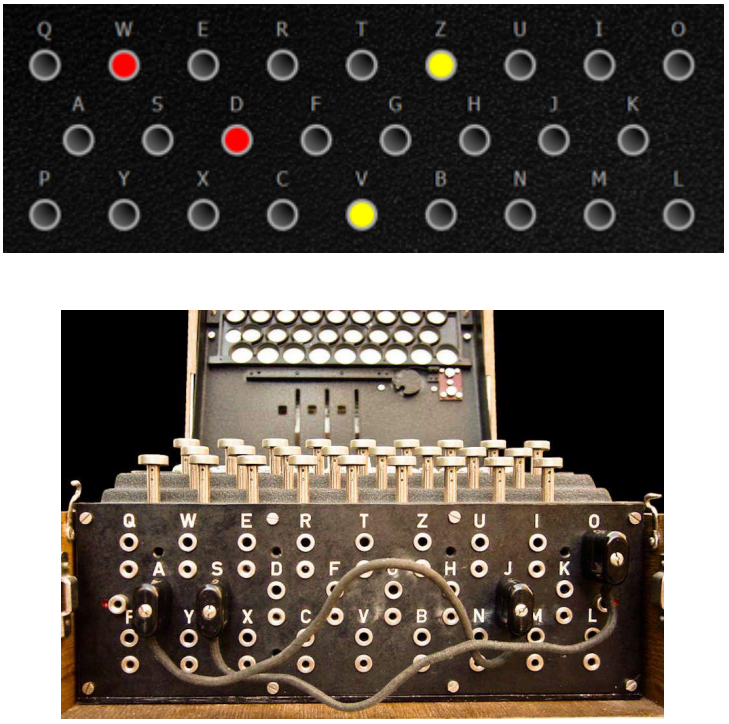


Fig : Steckerbrett / Plugboard

2.2 Rotors

The rotors are 26-pin special gears. Every pin corresponds to a letter in the English alphabet. When an electric signal reaches a rotor in a mechanical machine, it is transmitted to the next rotor at the same location. Every letter will be encoded as itself at location (0, 0, 0). The letter A, on the other hand, will be encoded as B, B as C, and so on at state (1, 0, 0).

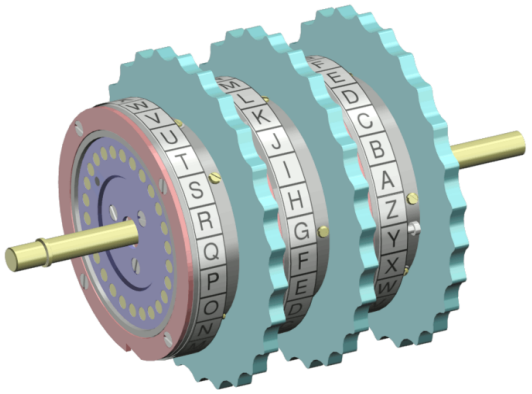


Fig: Rotors

Caesar cipher algorithm of encryption is used as the main principle in the enigma system.

2.2.1 Caesar Cipher Algorithm in Cryptography

The Caesar Cipher is one of the earliest and most straightforward encryption methods. It's basically a substitution cipher, in which each letter of a given text is substituted by a letter located a certain number of positions down the alphabet. With a shift of one, for example, A would be replaced by B, B by C, and so on. Julius Caesar is said to have called the approach after himself, as he used it to communicate with his officials.

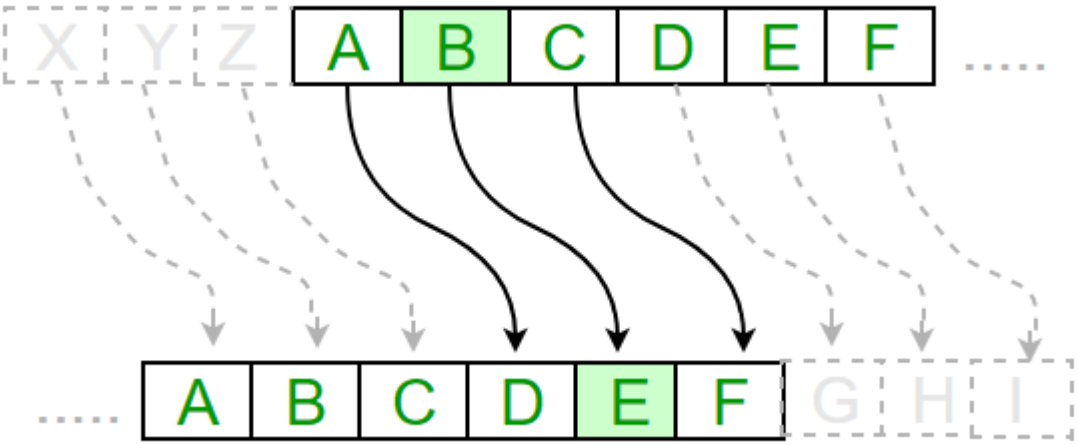


Fig: Caesar cipher when K = 3

In the case shown above A will be replaced with D, B with E, C with F, and so on.

In such a way, each rotor encrypts the message. The variable K in permutations in the algorithm is actually the number of turns from the 0 — state.

But that's not all; every 26th rotation of the first rotor, the second rotor rotates as well.

In the same manner, as the second rotor, the third rotor rotates after every 26th spin of the second rotor, but unlike the first pair of rotors, the second also rotates when the third does.

2.3 Reflector

Another type of rotor found inside the machine is the reflector. The reflector will reflect the electrical current back through the rotors after the letter has passed through the three rotors from right to left, sending the encrypted letter through the rotors from left to right for another three stages of encryption and then through the plugboard for a final substitution cipher. A permutation cipher is applied to the letter as it passes through the reflector.

2.4 Keyboard

The user input is retrieved using the keyboard. The asymmetric encryption machine is the Enigma machine. It can therefore be used to encrypt and decrypt a communication with the same settings. As a result, the keyboard is used to either enter the plaintext to be encrypted or the ciphertext to be decrypted.

Each letter of the alphabet is represented by 26 keys on the keyboard. This means that no spaces or punctuation marks will be used to link encrypted communications.

It's important to note that the keyboard begins with the letters QWERTZ rather than QWERTY. This is owing to the fact that the letter Z is more commonly used in German than the letter.

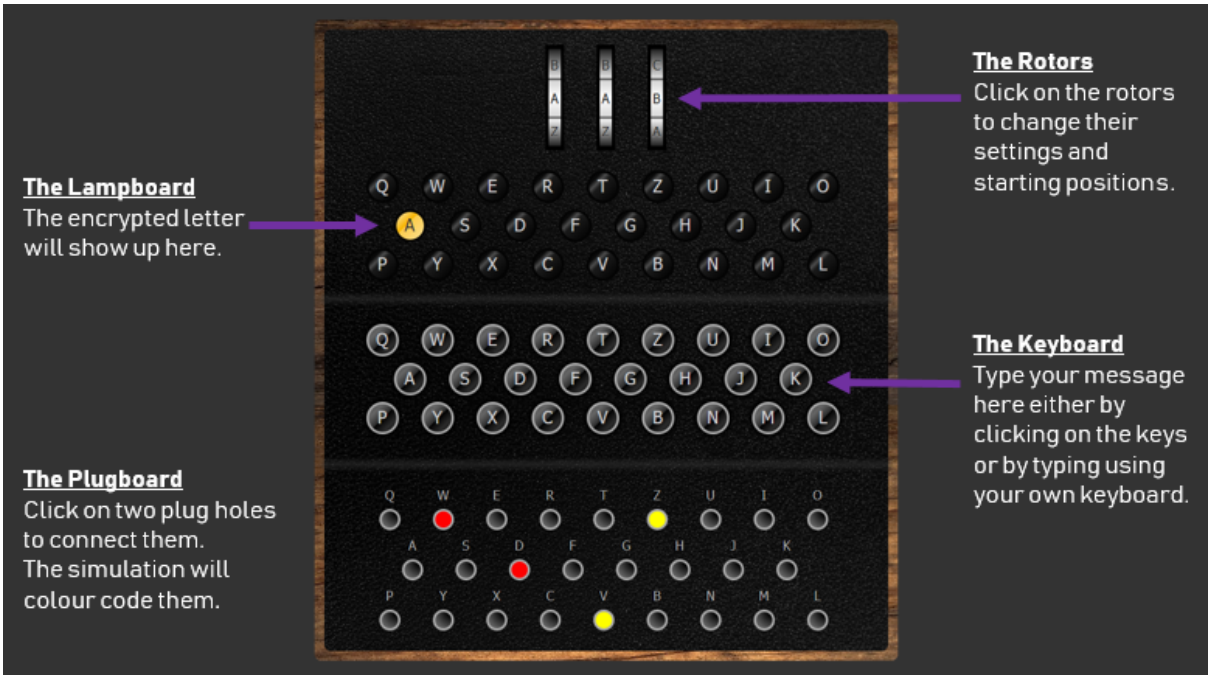
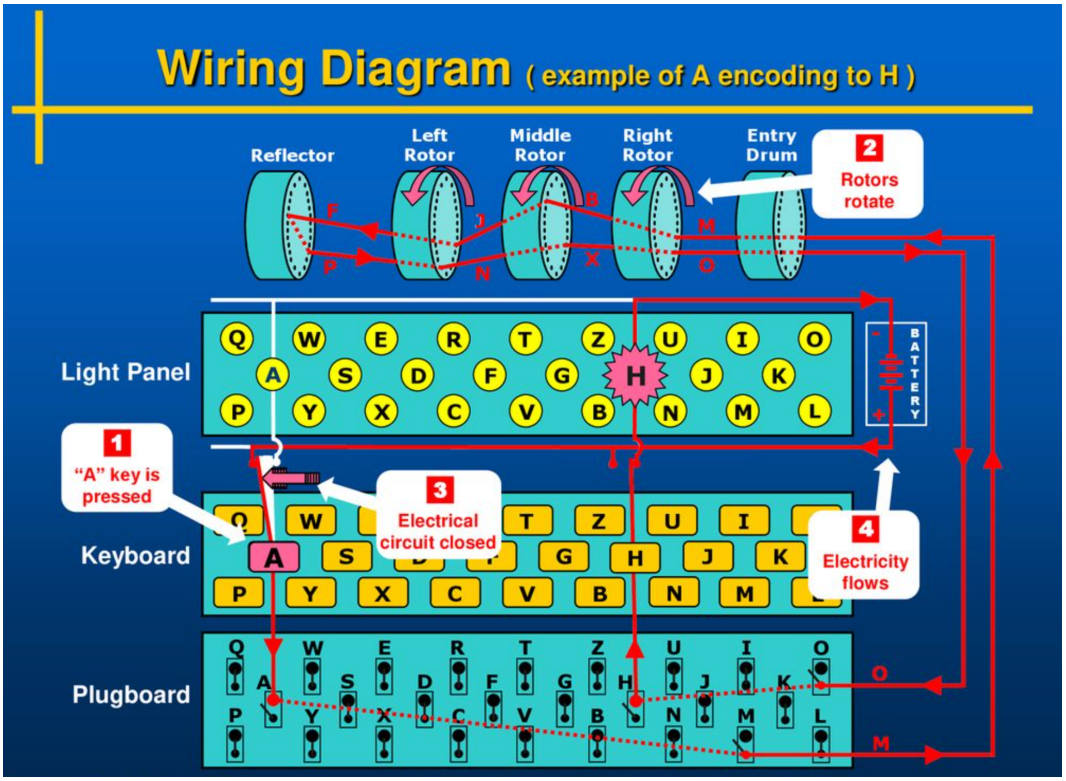


Fig: Main section of Enigma

2.5 Lampboard

The lampboard is the last stage of the encryption process, and it displays the results (encrypted letter). There are 26 light bulbs in total, one for each letter of the alphabet.

3 Working



STEP 1:
Keyboard Input: A

STEP 2:
Rotors Position: AAE
Plugboard Encryption: M
Wheel 3 Encryption: B
Wheel 2 Encryption: J
Wheel 1 Encryption: F
Reflector Encryption: P
Wheel 1 Encryption: N
Wheel 2 Encryption: X
Wheel 3 Encryption: O
Plugboard Encryption: H

STEP 3:
Circuit is closed

STEP 4:
Output (Lampboard): H

---

4 Implementation:

We created a python program on the mechanism of the ENIGMA machine and implemented it in a webpage using HTML, CSS, javascript. The following are the screenshots for the same:

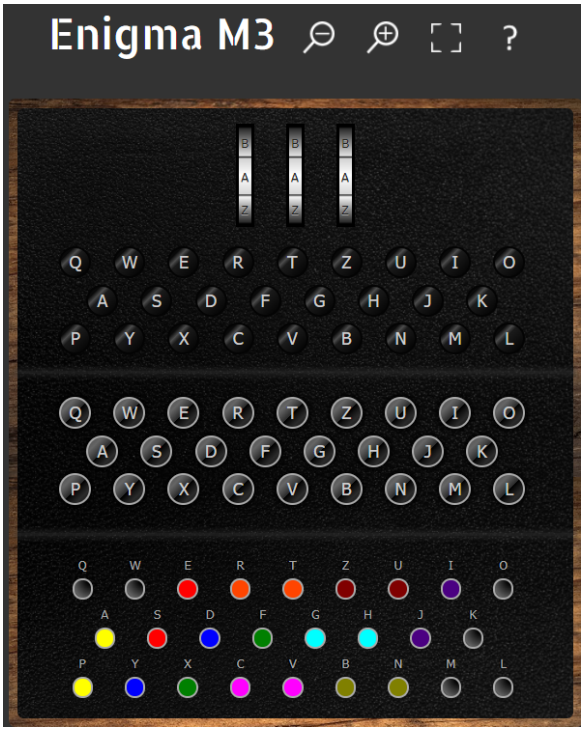
PYTHON PROGRAM OUTPUT:

```
    ##### Enigma Encoder #####

Enter text to encode or decode:
HELLO

Encoded text:
 VBSEN
```

```
print("  ##### Enigma Encoder #####")
print("")
plaintext = input("Enter text to encode or decode:\n")
ciphertext = encode(plaintext)

print("\nEncoded text: \n " + ciphertext)
```

```
  ##### Enigma Encoder #####

Enter text to encode or decode:
VBSEN

Encoded text:
 HELLO
```

WEB PAGE OUTPUT:



Encryption Steps:

```
Keyboard Input: H
Rotors Position: AAB
Plugboard Encryption: G
Wheel 3 Encryption: O
Wheel 2 Encryption: M
Wheel 1 Encryption: O
Reflector Encryption: M
Wheel 1 Encryption: C
Wheel 2 Encryption: P
Wheel 3 Encryption: X
Plugboard Encryption: F
Output (Lampboard): F
```

Encryption Steps:

```
Keyboard Input: F
Rotors Position: AAB
Plugboard Encryption: X
Wheel 3 Encryption: P
Wheel 2 Encryption: C
Wheel 1 Encryption: M
Reflector Encryption: O
Wheel 1 Encryption: M
Wheel 2 Encryption: O
Wheel 3 Encryption: G
Plugboard Encryption: H
Output (Lampboard): H
```

5 Cracking the ENIGMA code

A team of scientists, mathematicians, and cryptographers are credited with cracking the Enigma code. Alan Turing was the head of this historic team. He, along with his colleague Gordon Welchman, made his own version of the Bombe Machine (the Bombe Machine was originally invented by the Poles, but it was unable to effectively decipher the codes as quickly as was required). The machine was better than the Polish version of the Bombe machine, but it also required a very, very long time to decipher any code, which was bad news for Britain and the other Allied nations. Turing had to come up with an idea that could allow the Bombe Machine to crack the code much faster than that.

5.1 FLAW IN THE ENIGMA CODE:

Suppose we encrypt a message that contains a total of 3 words. The first word of the message was, let's say, 'SCIENCE'. Now, the first letter to be encrypted is 'S', so when the 'S' key is pressed on the keyboard of the Enigma Machine, an electric signal is generated that travels through a lot of wires and rotors and ultimately lights up a different letter (say, 'M'). So the 'S' in 'SCIENCE' would be encrypted as 'M'.

Similarly, the other words would be encrypted as different letters than they actually were. On one end of the Enigma Machine, you typed 'SCIENCE IS AWESOME', but the encrypted output might have looked something like 'MKSQER PO QAPEKRQ', or something entirely different.

Every letter was encrypted as a letter that was different from itself. Never once did it happen that a letter was encrypted as itself.

Quite simply, when we typed 'S', it could be encrypted as any one letter of A, B, C….X, Y, Z. Any letter out of the 26 letters could be the, but not S. Therefore, an 'S' would never be encrypted as an 'S'.

This was the single flaw in the Enigma code. Alan Turing using this flaw developed his Bombe machine which cracked the ENIGMA code.

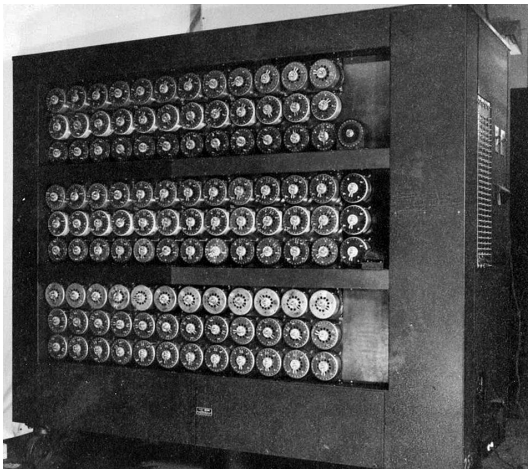


Fig: Bombe

6 Conclusion and Result

We developed a computer program that simulates the working of an ENIGMA machine. We implemented this algorithm to a webpage and the program was able to encrypt and decrypt text which closely resembles the principle of working of ENIGMA.

7 References

- https://www.britannica.com/topic/Enigma-German-code-device
- https://en.wikipedia.org/wiki/Enigma_machine
- https://en.wikipedia.org/wiki/Enigma_machine#See_also
- https://en.wikipedia.org/wiki/Enigma_rotor_details
- https://www.cs.cornell.edu/courses/cs3110/2018sp/a1/a1.html#cipherstring
- https://www.youtube.com/watch?v=G2_Q9FoD-oQ&t=464s&ab_channel=Numberphile
- https://www.youtube.com/watch?v=V4V2bpZlqx8&ab_channel=Numberphile