FUNCTIONING AND ENCIPHERING OF ENIGMA MACHINE

[1]Kishan Patel, [2]Nishtha Ranpara
[1]Student, [2]Student
[1]Computer Engineering,
[1]Indus University, Ahmedabad, Gujarat, India

ABSTRACT **:** The objective of this studies is to offer a quick detail on Enigma cipher device and its running. This study gives assessment on encryption method before and during international battle II. The growing use of cryptography leads a few major struggles of the second one world battle to an unpredictable and sudden result. This survey will lead us to how the Enigma codes where encrypted in earlier times.

Index Terms: Cryptography, Enigma machine, Encipherment, rotors, plug board, reflector, lamp board, and keyboard.

I. INTRODUCTION

Cryptography is where security engineering meets mathematics. It provides us with the tools that underlie most modern security protocols.

Enigma is a portable cipher machine, famous for the role it played in World War II. The breaking of Enigma codes is one of the reasons for the Allies victory. The Enigma machine is a piece of spook hardware invented by a German and use by Britain’s codes breakers as a way of deciphering German signals traffic during World War II.

II. History of Enigma?

Enigma was invented by the German engineer Arthur Schermie’s at the end of World War I.

The Enigma machine is a bit of spook equipment concocted by a German and utilized by Britain's codebreakers as a method for decrypting the German signs activity amid World War Two. It has been guaranteed that in view of the data increased through this gadget, threats amongst Germany and the Allied powers were abbreviated by two years.

III. What is Enigma Machine?

Enigma refers to a person or a thing that is mysterious or difficult to understand. Amid World War II, the Germans were utilizing an encryption code called Enigma – which was fundamentally an encryption machine that encoded messages for transmission.

The fundamental rule of an Enigma machine figure is that of letter substitution, implying that each letter of our plaintext (undeciphered message) is substituted by another letter.

Enigma machine is basically a confused substitution figure machine. It comprises of a plug board, a light board, an arrangement of rotors and a reflector. The machine accompanied a few rotors, every rotor contained an arbitrary substitution letter set.

The user would select between 3 and 5 rotors to use at any one time, depending on the size of the machine. The plug board was another variable for the machine. Certain letters would be connected reciprocally to each other [3]. The total possible combinations an Enigma machine can generate are around $1.58x10^{20}$.

IV. Working of Enigma Machine.

Enigma Machine is operated mechanically, with an electric signal passed through wires and various mechanical parts. The easiest way to explain the mechanics is to follow the journey of a single letter from keyboard to lamp board.

The figure 1 shows the path the signal takes from pressing the letter ‘T’ on the keyboard to the ‘G’ lamp lighting up.

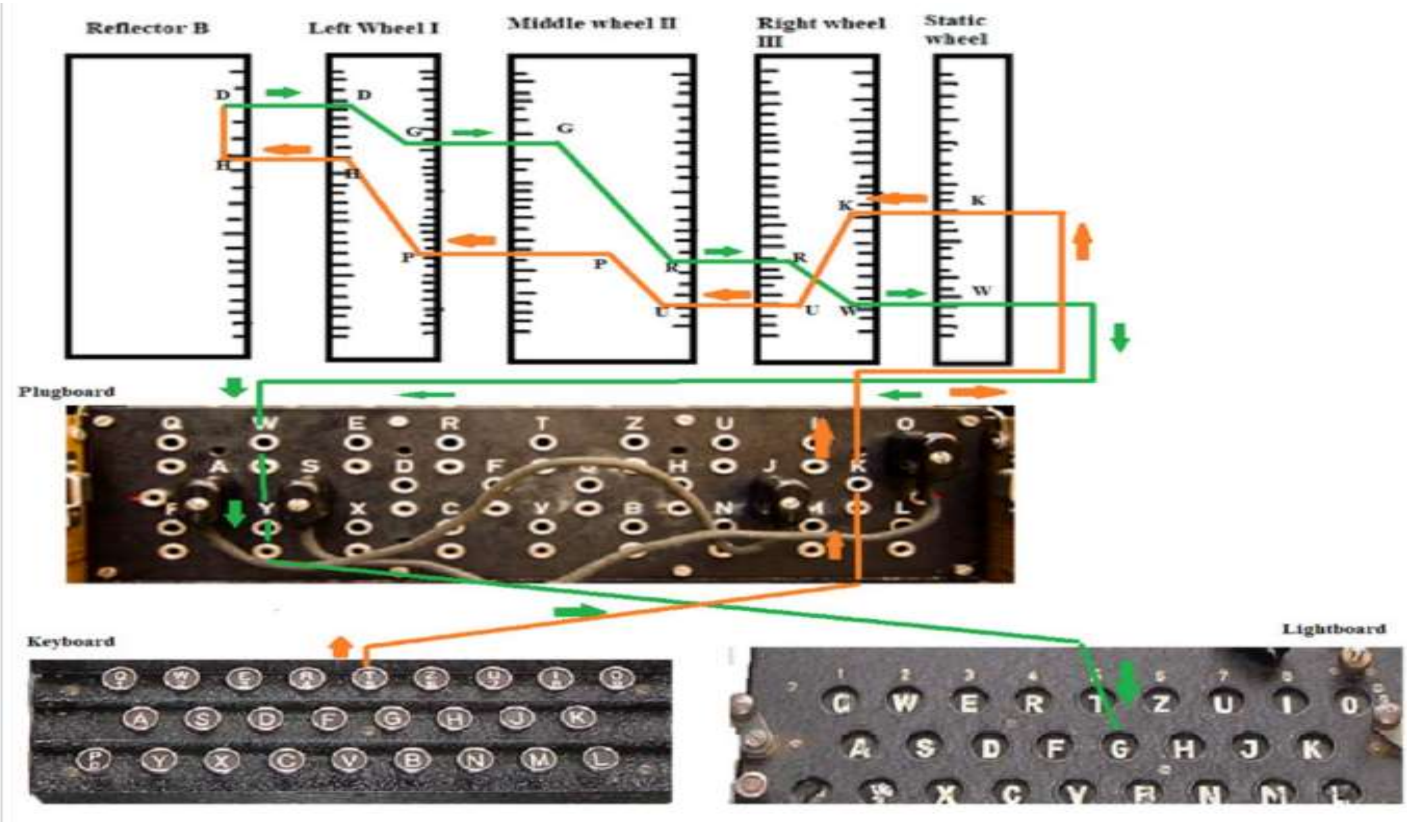

figure 1: Working of Enigma Machine

4.1 Keyboard

At the point when the operator presses the letter 'T' on the keyboard it makes an electric signal that starts the trip through the Enigma machine wiring that will end with a light flashing on the light board.

4.2 Plugboard

The principal stop on the flow is the plugboard. Here the signal is associated with the 'T' input on the plugboard. A portion of the letters on the plugboard will be wired up to different letters (the plugs), causing the signal to be diverted. In the event that the 'T' input isn't plugged to another letter, at that point our signal will pass straight to the 'T' output. In our case, though the 'T' is plugged to the 'K', so the signal is diverted to a new path, the letter is now 'K'.

4.3 Static Rotor

The following stop is the static rotor, which as the name proposes does nothing to the signal. It basically transforms wires into contacts (the signal passes only when the contacts touch). Along these lines, our signal is yet the letter 'K'. The static rotor output is associated with the contribution of the correct rotor.

4.4 Rotors

There are five possible rotors that can be utilized as a part of any request for the three rotor positions: right, center, left. Every rotor has an inward ring of contacts and an external ring of contacts and their aim is to scramble the flag. The external ring contacts interface every rotor to the next rotor (or the static rotor/reflector) and its own internal ring. The inward ring contacts can be turned in respect to the external ring which brings about much more possible connections (and hence, letter substitutions). The entire rotor itself can be pivoted with respect to the static rotor, so the static rotor 'A' output isn't connected with 'A' input on the rotating rotor.

Furthermore, as each letter is entered the rotors rotate by one position, so that the same letters are never connected in the same message. Each rotor had notches (different rotors have the notch in different positions) which when reached, causes the next rotor to its left to step forward too. In the case of the middle rotor, it causes the left rotor to step as well as itself.

4.5 Reflector

The reflector takes the input and reflects back the electrical signal for its return journey through the rotors. There are two possible reflectors, each of which is wired up differently so that the input letter is transformed to a different letter when reflected.

Because of the way the Enigma machine is designed, it is important that the signals must be scrambled when reflected. If you enter the cipher text you will get back the message in clear text form. So, if the reflector output and its input are the same letter when the signal passes back through the rotors then they will just unscramble what was already scrambled and the original unencrypted letter is obtained back.

4.6 Reverse journey

The reflected signal now goes back through the rotors, which work similarly in turn around. Along these lines, our letter 'D' goes through the left rotor and progresses toward becoming 'G', which at that point goes through the centre rotor and moves toward becoming 'R', which at that point goes through the correct rotor and moves toward becoming 'W'. The signal stays unaltered as it goes through the static rotor once more (connecting contacts to wires), before it goes through the plugboard - here the signal is again left as it is if there is no plug or changed if the letter 'W' is plugged to another letter. For our situation the 'W' is stopped to the letter 'G', so our plugboard output is 'G'.

4.7 Lamp Board

The last stop is the lamp board, where the output of plugboard is connected to the corresponding lamp for that letter.

The output letter is noted by the Enigma machine operator and then the next letter in the message is entered, and so on for every letter in the message.

V. Message Encryption in Enigma Machine

To encrypt your message with an Enigma machine, you would essentially type a letter and record which comparing letter lit up on the letter set. For each key press, the rotors would move and the message was dealt with as one, so you needed to send the full start to finish message to your beneficiary. The

encryption framework endeavored to get around recurrence investigation by first

Scrambling the letters with the attachment board (imagined frontmost) – which exchanged sets of letters around including a lot of multifaceted nature, and after that encoding the message with the rotors, which moved for each character in the messa9ge. This implies you could type a similar letter consistently, however Enigma would yield a cluster of various individual letters.

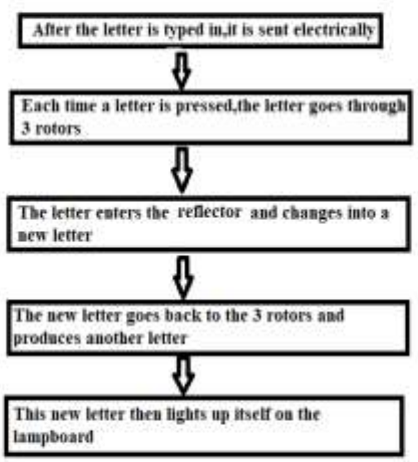
After the letter is typed in,it is sent electrically
Each time a letter is pressed,the letter goes through 3 rotors
The letter enters the reflector and changes into a new letter
The new letter goes back to the 3 rotors and produces another letter
This new letter then lights up itself on the lampboard

figure 2: Steps of Encryption

5.1 Enigma Encipherment

The 'key' for the enigma comprises of a few components:

1.The rotors and their request
2. The rotor begin positions.
3. The ring settings
4. Steckerverbindungen, or plug board settings.

5.1.1 The Rotors

Accept that our rotors are I, II, III moving from left to right, and we are attempting to encipher the letter 'A'. We will expect for the present that as the letter 'A' is enciphered every rotor is in its begin position ('AAA'). Since our rotors are I, II, III moving from left to right, the character A will initially experience rotor III. Every rotor applies a straightforward substitution operation. The substitution table for rotor III can be seen below.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

```
BDFHJLCPRTXVZNYEIWGAKMUSQO
```

B is replaced with D, C is replaced with F and so on. So after the letter 'A' experiences the rotor, it turns out as a 'B'. The letter 'B' is currently inputted through rotor II, where it is replaced by 'J' and so forth. This is best portrayed utilizing a table given below

III	II	I	Reflector	inv(I)	inv(II)	inv(III)
A->B	B->J	J->Z	Z->T	T->L	L->K	K->U

After the letter experiences rotors III, II, I it at that point hits the reflector and experiences another basic substitution. After coming out from the reflector, the letter is sent back through the rotors in the reverse direction (means inverse substitution is applied).

We can see from the table that after the enciphered letter returns out rotor III toward the end, we are left with the letter U.

5.1.2 Incrementing the Rotors

A typical error while executing the enigma is accepting the rotors go about as a standard odometer, there are however a couple of key contrasts. Every rotor has a notch which makes the rotor its left to step. Rotor I makes the next rotor to step on transition from Q to R, rotor II on the transition E to F and so forth. Rotors I through V are utilized as a part of the Wermacht enigma, later more rotors were included which had two notches.

I	II	III	IV	V	VI	VII	VIII
Q	E	V	J	Z	Z, M	Z, M	Z, M

At the point when a rotor steps, it likewise makes the rotor to its right to step. This isn't seen when the second rotor steps, since the primary rotor steps each key press. But, when the third (left most) rotor steps, it makes the second rotor step moreover.

5.1.3 The Ring Settings

The ring settings are given as a 3 letter string e.g. 'FAM'. In the past discourse I have assumed that every rotor's basic substitution cipher was fixed. The ring settings give the capacity of moving the substitution cipher as follows. With a ring setting of 'A's' (or 1), rotor I's substitution resembles this:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
EKMFLGDQVZNTOWYHXUSPAIBRCJ
```

With a ring setting of 'B' (or 2), rotor I's substitution looks like this:

```
ZABCDEFGHIJKLMNOPQRSTUVWXY
EKMFLGDQVZNTOWYHXUSPAIBRCJ
```

5.1.4 The plugboard settings

The steckerverbindungen (plugboard) is an additional layer of security which comprises of 13 wires which plug into its socket on the front of the enigma machine. Each wire interfaces 2 letters e.g. P to O. These pairings are indicated as a major aspect of the key material. At the point when a letter is written, before it goes into the principal rotor, it experiences the substitution as per the plugboard, at that point after the letter turns out it is put through the plugboard substitution again before being output.

An example of plugboard setting is as follows:

PO ML IU KJ NH YT GB VF RE AC (This means P and O are swapped, M and L are swapped etc.).

The plugboard altogether expands the strength of the enigma cipher, more than including another rotor could.

VI. Conclusion

The developers of the Enigma machine were much confident about the security of Enigma. After the second world war it was seen that cryptographers came to know that the Enigma was unbreakable. Enigma was a complex and a powerful. The advantages and disadvantages of machine were found as well as the method of applying the code produced by Enigma. The advantage of machine is that the cipher it uses are of random substitution without any formula. Although it is easy to find a key to a single random substitution ciphers, the Enigma machine makes it much harder by using 9 layers of encryption. The disadvantage is that the machine never encrypted a letter to itself, and hence the use of cribs was possible as well as the group theory. The breaking of Enigma with the available methods of that time difficult task and the hardwork and dedication of the cryptanalysts was appreciated.

REFERENCES

[1] http://www.counton.org/explorer/codebreaking/enigma-cipher.php

[2] https://www.archives.gov/files/publications/prologue/1997/fall/turing.pdf

[3] MTAT.07.006 Research Seminar in Cryptography The Enigma Cipher Machine by Kadri Hendla

[4] http://www.bbc.co.uk/history/topics/enigma

[5] http://enigma.louisedade.co.uk/howitworks.html

[6] http://practicalcryptography.com/ciphers/enigma-cipher/

[7] https://sites.google.com/a/umn.edu/historpedia/home/science-technology/cryptography-in-the-world-war-ii-fall-2012

[8] https://learncryptography.com/history/the-enigma-machine

[9] Robert ChurchHouse,Codes and Ciphers by Julius Caesar,The Enigma and the Internet,Cambridge Publication.

[10] https://en.wikipedia.org/wiki/Enigma_machine

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

[12] https://en.wikipedia.org/wiki/Automatic_Computing_Engine

[13] http://www.bbc.co.uk/history/worldwars/wwtwo/enigma_01.shtml

[14] https://www.dcode.fr/enigma-machine-cipher

[15] https://www.dcode.fr/enigma-machine-cipher

[16] https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma#The_Enigma_machines

[17] https://www.codesandciphers.org.uk/enigma/example1.htm