International Journal of Research in Engineering, Science and Management
Volume-2, Issue-2, February-2019
www.ijresm.com | ISSN (Online): 2581-5792

The Enigma Machine II

Komal Bawane[1], Shital Zile[2], Pritee Meharkure[3], Soniya Barapatre[4], Shailesh Kurzadkar[5]
[1,2,3,4]*Student, Dept. of Computer Tech., Karmaveer Dadasaheb Kannamwar College of Engg., Nagpur, India*
[5]*Professor, Dept. of Computer Tech., Karmaveer Dadasaheb Kannamwar College of Engg., Nagpur, India*

***Abstract*: In this paper we are investigates and describes the German mechanical cipher machine called enigma, and presents a possible way to its decryption. During World War II, the Germans used a typewriter-like machine named enigma to encrypt military messages. We make an attempt at a historical introduction, and non-technical background information is provided. This paper includes a c program that simulates enigma, and a method to break its code [1].**

***Keywords*: Electro mechanical devices, ciphers, cryptography, military communication, military communication.**

1. Introduction

The Enigma machines are a series of electro-mechanical rotor cipher machine, mainly developed and used in the early-to mid-20th century to protect commercial, diplomatic and military communication. Enigma was invented by the German engineer Arthur Scherbius at the end of World War. 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. Several different Enigma models were produced, but the German military models, having a plug board, were the most complex. Japanese and Italian models were also in use [2].

2. Related work

Enigma machine is simple to describe, but infuriating to break. Straddling the border between mechanical and electrical, Enigma looked from the outside like an oversize typewriter. Enter the first letter of your message on the keyboard and a letter lights up showing what it has replaced within the encrypted message. At the other end, the process is the same: type in the "cipher text" and the letters which light are the decoded missive [2].

Inside the box, the system is built around three physical rotors. Each takes in a letter and outputs it as a different one. That letter passes through all three rotors, bounces off a "reflector" at the end, and passes back through all three rotors in the other direction.

3. Description of Enigma

Main parts of an Enigma machine are the keyboard, the set of plug board and the lamps. Encipherment of letters is performed electrically. When a key is pressed, an electrical current starting from the key Flows through the rotors and lights one of the 26 lamps, which shows the output letter.

A. The Rotors

Rotors are the most important part of an Enigma machine. Rotor is a disc about 10 cm in diameter and it's usually made of hard rubber or Bakelite. On one face are 26 brass pins forming a circle; on the other side are corresponding electrical contacts. Each pin represents a letter in the alphabet. Inside the rotor are 26 wires connecting the pins on one side to the contacts on the other side; It is the usage of several rotors and their movement that provides a much more complex encryption. Stepping of the rotors is controlled by a ratchet 1 and pawl mechanism. On the right advances one position (one 1/26th of a full revolution). Press the middle rotor will step, too. This happens once for every 26 steps of the first Likewise [3].

B. The Plug board

The plug board is in the front of the machine. The plug board offers a reconfigurable wiring, adding a great deal of strength to the encryption. An operator chooses two letters and connects them on the plug board with a cable. Those letters are swapped before and after the rotor encryption. For example, if we have a pair A and K and the operator presses K then the plug board swaps the letters and A is sent to the rotors. There can be up to 13 such pairs [3].

C. Enigma Accessories

Some types of Enigma had extra accessories that made the using of the machine easier. Such were, for example, the "Schreibmax", the little printer, which replaced the lamps, and the remote lamp panel, which eliminated the operator ability to read the decrypted text. There was also an extra plug board switch, named the Uhr, which allowed the operator after connecting the plugs to turn the extra switch to one of the 40 positions, thus reconfiguring the plug wiring [3].

4. Enigma in use

For the message encrypted on one Enigma machine to be decrypted successfully on some other Enigma machine, both Important observation was that machines had to be set up the same way; they had to have the same initial states. That means that the rotor selection and order, the initial position of the rotors, the plug board connections and ring settings had to be the same. Those message settings make up the Enigma cryptographic key. In practice, this was solved by the means of

codebooks, which informed the operator how to set up their Enigma that particular day. The codebooks contained information about the choice and order of rotors and the ring and plug board settings. The starting position of the rotors was (pseudo-) randomly selected by the operator and transmitted along with the decrypted message. Message settings, turn the

Rotors to the indicated positions and decrypt the rest of the message. Second problem was the repetition of the message key, which resulted in a relation between the first and the fourth, the second and the fifth, the third and the sixth character. Later, during the Second World War, the codebooks were only used to set up the rotors and ring settings.

Bombe, a machine named after and inspired by the Polish Bombay [4].

5. The Turing bombe

The bombe relied on cribs - known plaintext cipher text fragments. An example of a crib is given in example.

An example of a crib. Position 1 2 3 4 5 6 7 8 9 10 11 12 Crib A T T A C K A T D A W N Cipher text W S N P N L K L S T C S ♦ A bombe would consist of sets of rotors with the same internal wiring as German Enigma rotors. These sets would be wired up according to a menu prepared by the code breakers. The rotors would step through all possible rotor settings and at each position, an electrical test would be applied. If the test led to logical contradiction, that setting could be ruled out. If it did not, then the rotors would step through all possible rotor settings and at each position, an electrical test would be applied. If the test led to logical contradiction, that setting could be ruled out. If it did not, then the machine would stop and that setting would be further examined on an Enigma replica. The test worked by making deductions from cribs. Finding cribs wasn't always easy. It required knowing German military jargon and the communication habits of the operators. Fortunately, the Germans were helpful in producing them. Also very useful was the fact that no letter could be encrypted to itself. It helped to locate the position of the crib in the cipher text, because a number of positions where a letter from the crib clashed with the same letter in the cipher text could be ruled out. What made it harder, was the use of a plug board. Without it, the testing of the rotor settings could have been performed encrypting the crib letter on an Enigma and comparing the result with the cipher text. If there was a match, next crib letter would be encrypted etc. With the plug board, this process was much more difficult, because it was unknown what the crib and cipher text letters were transformed to. Before looking at Turing's solution to this, let's agree on some mathematical notions. Let us have 4 some given scrambler position S and let's denote the starting position by S1, the same position with the rightmost rotor turned one position by S2 and so on. We also denote the plug board transformation by P. It is important to note that P (P(x)) = x, because the plug board swaps the letters. The encryption E of a letter x can be then written as E(x) = P(S (P(x))). Also, due to the fact that decryption is the same as encryption, E(E(x)) = x. Turing noticed that, even though the values for P(A) or P(W) (from 5.1) were unknown, the crib still provided known relationships among out [2].

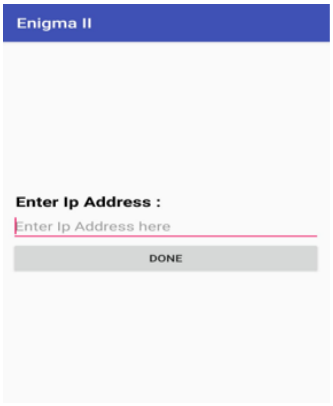

Fig. 1. Enigma II

Fig. 2. Message

Fig. 3. Text

Blowfish is a symmetric encryption algorithm meaning that is uses the same secret key to both encrypt and decrypt message. Blowfish is also a block cipher meaning that it device a message up into fixed length blocks during encryption and decryption.it has been extensively analyzed the reasonably secure by the cryptographic community implementation examples are available from server source.

In cryptographic circles plain text is the message you are trying to transmit that message could be medical test report a firmware upgrade anything else that can be represented as a stream of bits.

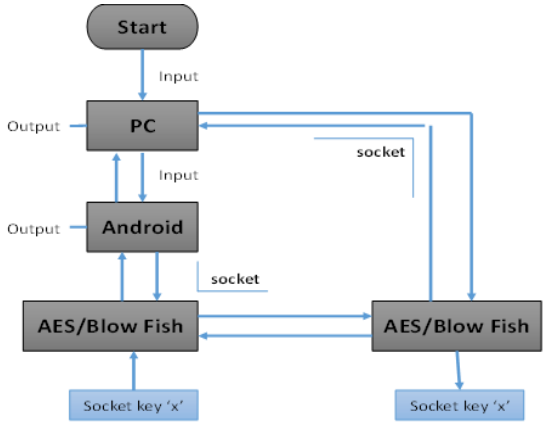

Fig. 4. Flowchart

6. Future scope

Enigma is a block chain-based protocol using groundbreaking privacy technologies to enable scalable end-to-end decentralized applications. With Enigma, "smart contracts" become "secret contracts," where input data is kept hidden from nodes in the Enigma network that execute code. This functionality finally makes block chains and smart contracts useful. Enigma is the missing piece to a decentralized future [5].

7. Conclusion

By 1945, almost all German Enigma traffic could be decrypted within a day or two. Yet the Germans were confident of its security and openly discussed their plans and movements. After the war it was learnt that the German cryptographers were aware that Enigma was not unbreakable, they just couldn't fathom that anyone would go to such lengths to do it. Enigma was a complex and powerful device. It could have been unbreakable, had the indicator procedures been more secure and German operators more careful. The breaking of Enigma with the 6 methods available at that time was a very hard feat and the dedication of cryptanalysts was admirable.

References

[1] MTAT.07.006 research seminar in cryptography in enigma cipher machine author by Kadri Handle publish by Nov 28, 2005
[2] Alan Turing research by Andrew Hodges. Princeton university press, the enigma 2014.
[3] A Simple Enigma author by Stephen Cass, January 2015.
[4] Breaking the enigma research by Dmitri Gabbasov, June 2015.
[5] A. Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data", Cryptography and Network Security, 2017.