Enigma Evolution & Cryptanalysis

Abdulmunim Shakir Al-Duri

Al-Fiqh Department, Imam A'Adhum University College / Iraq
E-mail of the corresponding author: ambaghdad@gmail.com

Abstract — This paper shows the history of the Enigma machine which was invented by German. It describes the main components of the Enigma and how it works within the initial and final designs. The paper, also, explain the attempts to break the Enigma by Poles and Britain through the weakness that leaded to success. That success was due to many reasons that the bad key management represented the main factor of them.

Keywords — Enigma, bombes, Rejewski, bad key management, rotor, Arthur Scherbius, atom bomb.

I. Introduction

Messages encryption methods previous to the World War II depended mostly on the shuffling of letters or on representing each word by a number. Using frequency analysis made the linguistic-based methods easy to be decrypted. Also, the need to gain the codebook is very necessary for the numeral-based messages. The appearance of Enigma, which was a great complicated encryption system that could not be decoded using frequency analysis of the cipher text and it required to keep the key secret instead of keeping many codebooks. German secret-writing machine was one of the greatest milestones of World War II beside of the atomic bomb invention. It seems that without breaking the Enigma the World War II would continue for two years more and, consequently, a dropping of the atom bomb on German would occur.

II. History

Enigma, the electro-mechanical cryptographic system, was one of the most important inventions in the history of cryptography. Its concept was based on an electric typewriter produced by the American Edward Hebern in 1915[1][2].

The Enigma was invented by a German inventor Arthur Scherbius in 1918 [3] This was confirmed by a number of references, despite the existence of a historical mistake in some reference as example in a recent publication of the National Security Agency, United States of America, History and Publication Division states that "*Hugo Koch, a Dutchman, conceived the machine in 1919, Arthur Scherbius first produced it commercially in 1923*"[4] According to the books of David Khan, Friedrich elaborated to clarify this historical error *"On April 15, 1918, Scherbius wrote to the Office of the Imperial Navy (Reichs-Marineamt) and offered his invention for examination.*"[5] The Imperial Navy did not buy the machines because of the opinion in that time, ciphering by hand was sufficient [6] Wesolkowski emphasized that the armies did not see it as a practical method for encryption.

In early 1918, the German armed forces started testing as much more convenient cipher machines [2]. He also mentioned, Dr. Arthur Scherbius had produced the Enigma after making improvements on the previous design by using three rotors [1][2]. The German Post Office exhibited the Enigma at an International Postal Union Congress and advertised it as an inexpensive and reliable device to protect commercial cables and telegrams. The German navy in 1926 and then the army in 1928 modified it after withdrawing it from the markets producing a new military version of Enigma [7][2].

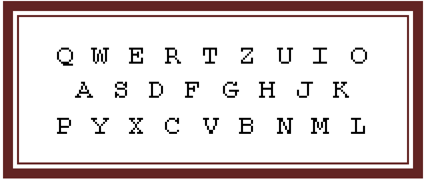
III.Design

Kris Gaj and Arkadiusz Orlowski described the Enigma machine as "*a small portable electromechanical machine equipped with battery. It had dimensions and looks of a typical typewriter*" [8]. There were two main designs of the Enigma machine:

A. *Initial Design*

It was consisting of three main parts:

1) Keyboard:
It contained 26 letters. It didn't contain numbers, punctuation characters, or function keys [8]. It was used to input plaintext letters. It had a slightly different arrangement of keys than keyboard used nowadays [9].



Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L

Fig. 1 The Enigma keyboard

2) Panel of bulbs:
A panel that consisted of 26 bulbs marked with the same letters of the keyboard [8].
3) Rotor:
"*A rotor is a wired code wheel with usually twenty-six evenly spaced electrical contacts around the circumference of the disc. Since each contact can represent a letter, the rotor embodies a cipher alphabet. Therefore, some other letter dependent on the rotor position will replace the input letter. If the rotor did not turn, each letter would have a corresponding encryption code as in Hebern's invention.*"[2]

Of course, the Enigma as all electrical devices is useless without a power supply making the bulbs light that is represented here by a battery [9].

B. *final Design*

The additional part to the three main parts was the plugboard. In 1930, a military implemented a new version of Enigma with the commutator as the main innovation [7][2]. The commutator was mainly a twenty-six plugs plugboard and plug connections. Therefore, another substitution layer on top of the rotors would be added by the plugboard. However, not all the 26 letters would be substituted in this case. The connection would be between two sets of six letters each at a time [10][2].

Description of Enigma rotor as mentioned by Kadri Hendla [11]:

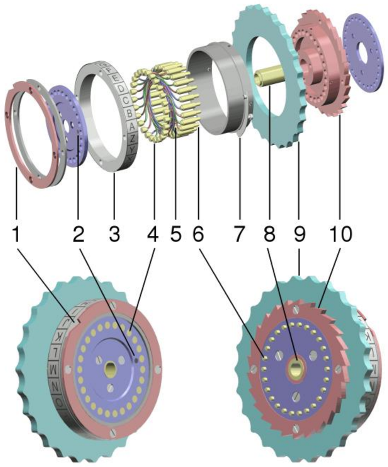


Fig. 2 the Enigma rotor

1. Notched ring.
2. Marking dot for "A" contact.
3. Alphabet ring.
4. Plate contacts.
5. Wire connections.
6. Pin contacts.
7. Spring-loaded ring adjusting lever.
8. Hub.
9. Finger wheel.

10. Ratchet wheel.

IV. Algorithm

From the prospect of the electrical not the mechanical action, the Enigma machine consists of four components that are easy to be noticed when the main top cover is opened. May be the question of how does the Enigma machine work is hard because the answer depends on two factors; who was using it and when they were using it? This answer is for the Enigma that was attacked by the Polish mathematicians in 1932.

Simply, the operator keys the plaintext letter on the keyboard and the corresponding letter on the panel of bulb lights, which represents the cipher text letter. Then the operator should write each lighted letter, and so on till the plaintext finishes.

But before that simple action, some configuration should be set according to the given key. The first, the six plugs of the plugboard would connect six pairs of letters. The plugboard effect was to swap the selected 6 pairs of letters and let the other 14 letters pass through unchanged. The electrical charge passed into the rotor system after passing through the plugboard [9]. The second, is to set the rotors according to that day given key [11].

V. cryptoanalysis

Breaking Enigma over two historical phases, the first phase was before the beginning of World War II by the Polish, and the second phase was during the World War II by British. All of these efforts from multi-country had resulted in the break of this machine.

A. *Polish Pre World War II:*

In 1929, the Polish government selected a number of students to participate in a cryptology course and most of these students from the University of Poznan, and among these students three students were selected later to work with the Government Henryk Zygalski, Jerzy Rozycki, and Marian Rejewski [9]. The best of these students in terms of intelligence and knowledge, Marian Rejewski, He was the first students who were selected in the analysis and test of strength of Enigma [8]. In 1934, Rejewski invented the cyclometer, a machine for preparing a card catalog of the length and number of chains for all 17,576 positions of the rotors for a given sequence of rotors [11]. Rejewski was to discover the mistake committed by the Germans.

The beginning of each message contains an encrypted key twice. Then his goal is to study rotors and to discover which one was in use, until he reached to the alphabet rings that had been set on the rotors [12]. Unfortunately, during polish creating a number of techniques to help breaking this machine such as Bombe, German in September 1938 changed the procedure for giving message keys.

The techniques that the Poles had by now perfected were ineffective, and in December 1938 the Germans introduced two new rotors, there were then five rotors, any three of which would be used at one time. In January 1939, they increased the number of plug pairs to ten [13]. This phase ended after the Germany's invasion of Poland.

B. *British during World War II:*

In July 1939, there was a tripartite meeting to exchange information about Enigma, the meeting was among the French, British and Poles who gave the precious gift that contain all the information suitcases in addition to Polish bombes to British [14]. After that and after Britain get this valuable information they were able to invent "British Bombe" and with the existence of this invention in addition to the use of parts of fragments of the plaintext called cribs, Britain lunched known plaintext attack against Enigma. After that Gordon Welshman has developed Alan turning bombe [8]. Britain managed to break Enigma and knew all the information that eventually led to the victory of the Allies.

VI. Result

The result is illustrated in the table below:

TABLE I
Cryptanalysis

Period	Attack	Weakness
1934	Cyclometer key found in about 15 minutes	Global message keys
1935-1938	Rejewski's bombe	Encrypted message keys twice
1940	Turing's bombes	daily settings of the Enigma machines

VII. Discussion

Results show that the main reason which led to break the Enigma is bad management of the keys, this bad keys management started when Germans use globals message keys method which led to the invention of cyclometer by Rozycki. After that Germans stopped using this method, unfortunately they did another fatal mistake by encrypting key twice that enabled Rozycki to break enigma using bombe. Although, some believe the factors that helped to break enigma were the use of mathematics and the diversion of information by spies, as it was indicated by Chris Christensen " *success in breaking the Enigma cipher can be attributed to three factors: fear, mathematics, and espionage*"[15] .

According to my point of view these factors are helping factors but the main factor was the bad key management. Germans had strong cipher machine but they did not use it in an optimum use.

VIII. CONCLUSIONS

Any researcher looking at the Enigma history will notice that conflict and competition is still continuing up to now. There is a number of different historical stories, and each country wants to either be attributed to the idea of the Enigma or the idea of breaking it**.** Despite the differences in these historical stories, they agree that enigma is a terrifying cipher machine at that time. Its idea used even in the modern encryption algorithms, and even breaking of it, which led to the idea of the computer in its current form.

The Enigma can be broken now in a very short time because the size of the key is very small with the techniques of this era but this does not prevent the development where the key length can be increased by adding large numbers of rotors or changing its technical works, and finding an effective technique in the management of keys makes enigma back to work again.

REFERENCES

[1] Stephen Harper (1999)."*Capturing Enigma: How HMS Petard Seized the German Naval Codes"*. Sutton Publishing, Phoenix Mill.

[2] Slawo Wesolkowski.*"The Invention of Enigma and How the Polish Broke It Before the Start of WWII".* University of WaterlooWaterloo, Canada

[3] C.A. Deavours and L. Kruh, "*Machine Cryptography and Modern Cryptanalysis*", Artech House, Dedham MA (1985).

[4] Friedrich L Bauer, "*An error in the history of rotor encryption devices*", Cryptologia 23(3), July 1999, page 206

[5] Bauer, Friedrich L., "*Decrypted Secrets: Methods and Maxims of Cryptology*". 4th ed. New York: Springer, 2006

[6] Karl de Leeuw, J. A. Bergstra, "*The History of Information Security: A Comprehensive Handbook*". UK: Elsevier Science, 2007.

[7] Wladyslaw Kozaczuk, "*Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two"*. University Publications of America.1984.

[8] Gaj, Kris; Orłowski, Arkadiusz, "*Facts and myths of Enigma: breaking stereotypes",* George Mason University, Fairfax, VA 22030, U.S.A.; Institute of Physics, Polish Academy of Sciences Warszawa, Poland

[9] Chris Christensen, "*Polish Mathematicians Finding Patterns in Enigma Messages*", Mathematics Magazine, 80 (4), October 2007.

[10] Kahn, David, "*Seizing the Enigma: The Race to Break the German U-Boats Codes*", 1939-1943. Boston: Houghton Mifflin (T), 1991

[11] Kadri Hendla, "*The Enigma Cipher Machine, Research Seminar in Cryptography*", 05.12.2005

[12] Christine Large,"*Some Human Factors in Codebreaking*" .Trust Director, The Mansion Bletchley Park MK3 6EB UK

[13] Beryl Plimmer, "*Machines Invented for WW II Code Breaking*". SIGCSE Bulletin. Vol 30. No. 4. December 1998.

[14] Slawo Wesolkowski, "*The Invention of Enigma and How the Polish Broke It Before the Start of WWII*" University of Waterloo Waterloo, Canada

[15] Chris Christensen, "*Machine Ciphers*". Fall 2006. MAT/CSC 483.url: http://www.nku.edu/~christensen/section%2017%20machine%20ciphers.pdf, retrived:28.2.2010 .

[16] Rudolf Kippenhahn,"*Code Breaking: A History and Exploration*". The Overlook Press,Woodstock. 1999.