Survey on Enigma Machine

Aadesh Darawade[1], Sanket Gaikwad[2*], SuyashChavan[3,]Deepti Dave[4]
[123]U.G. Student, SOE, ADYPU, Lohegaon, Pune, Maharashtra, India
[4]Senior Faculty-IT, iNurture, Bangalore, India

Abstract- Aim of the given survey is to give a brief summary on the Enigma cipher machine and its cryptanalysis during the Second World War and before it. As new technologies came into existence,people often find it necessary to leave the old technologies out of the syllabus and the students miss out the historical impacts and the importance old technologies used to have. The discipline is so broad and deep that people have to carefully choose what concepts and technologies they study in deep, what they mention in momentary, and what they leave out. Leaving out the important historical developments deprives the students of historical context and the evolution of technology into the profession. This paper presents a brief description on Enigma Machine.

Keywords- Enigma machine, Cryptanalysis, Plug Board

I. INTRODUCTION

The Enigma Machine is one of thefamous cryptography devices those were used in the history of this profession. The Enigma machine marked a transition into practice of cryptography from creativity as well as technology based solution. After the World War I, it became obvious that cryptography had to beimprove beyond just simple substitution. Technology came to the front and electromechanical devices like the Enigma became popular. Both sides of the war used rotor based devices with different degrees for success while the World War II.

As the Enigma played a great historical role in World War II, it has been popularized in television, movies, and historical fiction. Many students may have seen the movie U-571 and several of the other shows and historical accounts centered on the Enigma Machine. This historical knowledge is something that they, as cryptography instructors can exploit to the advantage and use to captureattention of students.

The Enigma Machine provides with the opportunity to raise a number of critical topics in the classroom including some history lessons, the role of technology in cryptography, and how it has evolved with improvements in technology. There are numerous Enigma-based classroom activities that could provide students hands on experience with encryption and decryption.

II. HISTORY OF ENIGMA

There really is no single Enigma Machine. It was a family of encryption/decryption machines that were based on a series of rotating cipher wheels. The original Enigma machine was patented in 1918 to provide secure business communication. The Enigma was later adopted by the military and played a significant role in the Second World War. Like most encryption technologies, the Enigma machine evolved as the military addressed weaknesses to makeit more secure and easier to use. Different variations of the Enigma Machine were used during the world war by Germany and Japan.

The Enigma machine was first deduced by Polish decipherers who passed their information on the British government. The Britishers employed Alan Turing and a team of cryptographers and code experts. Alan Turing himself led the invention of the Bombe device that helped defeat the Axis by breaking the ciphertext produced by Enigma machine. The Bombe was a brute force solution. The Bombe worked by simulating as many Enigma machines as possible. Attacking the Enigma machine using a Bombe machine shows that while brute force solutions may be inelegant, they can be effective.After World War II, technologybased encryption devices sustained to improve. The United States moved towards encoded teletype devices like the SIGABA machine and Enigma transitioned from a state-of-the-art device to become a historical footnote.

The electromechanical Enigma machine was the bridge between ciphers and digital encryption procedures.In 1918 German engineer Arthur Scherbius applied for a patent for a mechanical ciphering device. The earliest Enigma machines were commercial models. German military accepted Enigma in the 1920s (Navy in 1926, Army in 1928). Over the years they made many changes to Enigma to make it secure, most important of these being the adding of the plugboard. A number of other countries, for example Italy, Switzerland and Spain, also used the marketable versions of Enigma.

III. DESCRIPTION OF ENIGMA

3.1 The Rotors

Rotors are the utmost important part of an Enigma machine. A rotor is a disc around 10 cm in diameter and it's usually made of hard rubber or bakelite. On one face there are 26 brass pins forming a circle on the other side there are equivalent electrical contacts. Each pin is used to represent a letter in the alphabet. Inside the rotor are 26 wires connecting the pins on one side to the contacts on the other side; the wiring is different for each rotor. The rotor also has a finger wheel for turning the rotor by hand and an alpha-bet ring, so the operator can see the rotor position. In the earlier versions of Enigma the alphabet ring was fixed; the later versions allowed adjusting the alphabet ring relative to the core wiring. This position of the ring is known as the ring settings. These rotors are placed in the machine side by side, which causes the pins and contacts of the neighbouring rotors to form an electrical connection. To control the stepping of the rotors, each rotor has a ratchet wheel and a notch (or several notches). In the mil-itary versions of Enigma the notches are placed on the alphabet ring.When placing each rotor into the machine, it can be set to one of 26 positions. Typically Enigma had three rotors, although there was a four-rotor version of Enigma (M4) used by German Navy. Later Army and Air Force Enigmas were also equipped with more rotors, but only three would be inserted into the machine at a time. The Navy had always used more rotors: first five, then seven and finally eight.Each rotor alone represents a simple substitution cipher. 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 and pawl mechanism.

Each rotor has a equivalent pawl and the stepping is achieved over the pawls engaging the ratchets. Every time a key is pressed, the first rotor on the right advances one spot (one 1/26th of a full revolution). When the notch on that rotor is aligned with the pawl of the mid rotor, then on the next key press the mid rotor will step, too. This occurs once for every 26 steps of the first rotor. Similarly, for every 26 advances of the middle rotor, the third rotor steps once. Furthermore, every time the third rotor steps, the second rotor also advances one additional position. This is called double stepping, because the second rotor steps twice during one key press.Almost all Enigmas have a reflector following the last rotor. When the current passes the rotors it is reflected back through the rotors, but by a different route. The reflector makes Enigma self-reciprocal - encryption is the same as decryption. Also, the reflector lets no letter to encrypt to itself.From now on, unless otherwise specified, we are talking about three-rotor Enigma with the reflector and the plugboard.

3.2 The Plugboard

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

3.3 Enigma Accessories

Some types of Enigma had extra fittings that made the using of the machine easier. Such were, for example, the ”Schreibmax”, the little printer, which substituted 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 joining the plugs to turn the ex-tra switch to one of the 40 positions, thus reconfig-uring the plug wiring.

IV. ENIGMA IN USE

For the message encrypted on one Enigma machine to be decrypted effectively on some other Enigma machine, both machines had to be set up the same way; they had to have the same initial states. This meant that the rotor selection and order, the initial position of the rotors, the plugboard connections and ring settings had to be the same. Those message settings made 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 code-books contained information about the choice and order of rotors and the ring and plugboard settings. The initial position of the rotors was (pseudo-) randomly selected by the operator and transmit-ted along with the decrypted message. The exact method of message comprising is called the ”indi-cator procedure”.

One of the earliest indicator procedures was for the operator to set up the machine as directed by the codebook, choose his random starting position (message settings) and encrypt it twice by the use of the ground setting (global starting position of rotors, as given in a codebook). The double encryption was for detecting transmission errors. Then user would turn the rotors to his own starting position and encrypt the actual message. The receiving operator would have set up the machine the same way and other user would decrypt the first six letters of the ciphertext, get the actual message settings, turn the rotors to the indicated positions and decrypt the rest of the message.This indicator procedure suffered from two secu-rity flaws. First, the use of a global ground setting was by itself a bad idea. If enemy captured a codebook, they could easily decrypt all messages. 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 code-books were only used to set up the rotors and ring settings. An operator chose a random startposition and a random message key for each message. He then set the rotors to the selected startposition, for example WZA, and encoded the message key, for example SXT.

V. CRYPTANALYSIS OF ENIGMA

Since the German Navy began victimisation they increased Enigma in 1926, the decoding of their messages was impossible. French cryptanalysts reportedly gave up and deemed Enigma unbreakable. Enigma was designed to be secure albeit the enemy captured one in every of the machines. The Poles still had to return up with how to induce daily machine configurations. In 1932, Polish scientist Marian Rejew-ski discovered how to seek out the bottom settings and message keys. He worked out the indicator procedure, that at that point was to cipher the message key chosen by the operator double and to transmit this encrypted message setting within the starting of the message. This resulted during a relation between the letters. for instance, if the ciphertext of the duplicated message key was JXDRFT, then it had beenillustrious that J and R (1,4 pair), X and F (2,5 pair), D and T (3,6 pair) were originally a similar letter. it had beenattainable to seek out chains of however the identical letters modified, for instance, from J to R to J once more (a chain with a length of 2)

In 1934, Rejewski fictional the cyclometer, a machine for getting ready a library catalog of the length and varietyof chains for all seventeen,576 positions of the rotors for a given sequence of rotors [2]. The cyclome-ter was, in essence, 2 Enigma machines facet by facet with their paw wheels o set by 3 places [4]. compilation of the catalog took over a year (it had one hundred and five,456 entries.

On All Saints' Day, 1937, the Germans modified the reflector wirings and therefore the library catalog turned useless [3].

The Poles didn’t surrender and commenced building a replacement catalog. Since the codebreaking strategies up to now relied on all message keys having a similar startpositions, the catalogs and therefore thecyclometer were in active once more [4]. a very important observation was that generally the one,4, 2,5 or 3,6 pairs were identical (for example, PST PWA) [3]. Another Polish cryptologist, Hen-ryk Zygalski, accomplished that the prevalence of these pairs (called ”females”) trusted the wheel or-der and therefore the begin position. If enough of such pairs occurred, it would be attainable to seek out a singular configuration that all of these doubles might occur [4]. The technique accustomed try this, is thought as ”per-forated sheets” or ”Zygalski sheets”. the strategy concerned giving birth a series of perforated sheets over each other and shining a lamp beneath. everysheet had twenty six rows and columns, marked at the facet with letters of the alphabet. there have been twenty six sheet during a set (one set depicted one attainable position of the rotors), one for every position of the leftrotor.

The rows of a sheet depicted the position of the center rotor, Rejewski fictional a ma-chine that might take a look at them mechanically. it had been known as ”bomba” (plural ”bomby”) and it consisted of 3 sets of scramblers (a set of rotors and a re-flector), placed one machine cycle apart and driven by a motor. in contrast to Enigma, the bomba had separate terminals for input and output letters. If it had been assumed that the primary 3 letters of a coded message, for instance HJQ, depicted the plain-text, for instance ANX, input terminals H, J, and Q were energized and output terminals A, N, and X monitored. The machine stepped through all cycles till a match was found, then stopped. for every take a look at run sixbomby were needed. [3] In 1939, the German Army increased the complexity of its Enigma in operation procedures. They additional 2rotors to Enigma, 3 of which might be used at a time. The Germans conjointly began to use a replacementindicator procedure, no longer encipher-ing the message keys twice, thus making it harder for the Poles, whose methods of breaking Enigma relied on the double-encrypted message keys. The Poles, fearing the German invasion, contracted military alliances with Britain and France and de-cided to share their work on Enigma. They gave the British and French each a Polish-reconstructed Enigma and the details how to solve it. Until then, the British had had no real success in breaking Enigma.

5.2 Breaking of Enigma, World War II

Although the British now knew the Enigma-breaking techniques, they had to remain alert to German cryptographic advances. The German Army practices had become more secure and the Navy had always had more security.The British codebreakers had their headquarters at Bletchley Park. Many talented mathemati-cians worked there, for example, Alan Turing, who, along with Gordon Welchman, designed the British bombe, a machine named after and inspired by the Polish bomby.

5.2.1 The Turing Bombe

The bombe relied on cribs - known plaintext-ciphertext fragments. An example of a crib is given in 5.1.

Example 5.01 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
Ciphertext	W	S	N	P	N	L	K	L	S	T	C	S

A bombconsist of sets of rotors with same internal wirings as German Enigma rotors. These sets would be wired up according to a menu prepared by the codebreakers. The rotors will go 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. [5]

The test worked by making deductions from cribs. Finding cribs wasn't always easy. It re-quired knowing German military jargon and the communication habits of the operators. Fortu-nately, the Germans were 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 ciphertext, because a number of positions where a letter from the crib clashed with the same letter in the ciphertext could be ruled out. What made it harder, was the use of a plugboard. Without this the testing of the rotor settings could have been performed encrypting the crib letter on an Enigma and comparing the result with the ciphertext. If there was a match, next crib letter would be encrypted etc. With the plugboard, this process was much more difficult, because it was unknown what the crib and ciphertext letters were transformed to. [5]

Before looking at Turing's solution to this, let's agree on some mathematical notions. Let us have

some given scrambler position S and let's denote the starting position by S_1, the same position with the rightmost rotor turned one position by S_2 and so on. We also denote the plugboard transforma-tion by P . It is important to note that P (P (x)) = x, because the plugboard 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 de-cryption is the same as encryption, E(E(x)) = x.

Turing noticed that, even though the values for P (A) or P (W) (from 5.01) were unknown, the crib still provided known relationships amongst these values. Using these relations, it was possible to reason from one to another and potentially derive a logical contradiction, in which case the rotor set-ting under consideration could be ruled out. The process of this reasoning is described in 5.02 from [5].

Example 5.02 Let us assume that, for example, P (A) = Y. Looking at position 10 (in 5.1), we no-tice that A encrypts to T, and T = P (S_{10}(P (A))). We can apply transformation P to both sides of that formula, and we obtain P (T) = S_{10}(P (A)). We now have a relationship between P (A) and P (T). If P (A) = Y , and for the rotor settings under consideration, for example, S_{10}(Y) = Q, we can deduce that

$$P (T) = S_{10} (P (A)) = S_{10}(Y) = Q.$$

It shows how P (T) can be completely determined if P (A) is known.

We also notice that T encrypts to W at position 2. Similary, we can deduce,

$$P (W) = S_2(P (T)) = S_2(Q) = G.$$

At position 1, A encrypts to W. The self-reciprocal property of Enigma means that at this position W would also encrypt to A. From that we can deduce a value for P (A), say,

$$P (A) = S_1 (P (W)) = S_1(G) = F.$$

At this point we have come to a logical contra-diction, since in the beginning we had assumed that P (A) = Y . This means that our initial as-sumption was incorrect and so for this rotor setting P (A) =6 Y .

For a single setting of the rotors, each possibil-ity for P (A) could be tried. If all of the possi-bilities lead to a contradiction, then the rotor set-ting could be eliminated from consideration. The bombe mechanised this process, performing the log-ical deductions near-instantaneously using electri-cal connections, and repeating the test for all 17,576 possible settings of the rotors. The bombe con-sisted of several sets of Enigma rotor stacks wired up together according to the instructions given on a menu, derived from a crib. In addition, each Enigma stack rotor setting is offset a number of places as determined by its position in the crib; for example, an Enigma stack corresponding to the fifth letter in the crib would be four places further on than that corresponding to the first letter. [5]

Although Turing's bombe worked in theory, in use it required impractically long cribs to rule out sufficiently large numbers of settings. Gordon Welchman came up with a way of using the symme-try of the Enigma stecker to increase the efficiency of the bombe. His suggestion was an attachment, called the diagonal board, that further improved the bombe's effectiveness. [5]

5.2.2 Breaking of the Naval Enigma

The Navy variant of Enigma was quite harder to break. Naval Enigma had set of eight rotors, from which three was chosen. Also the Navy used much more secure procedures and starting from 1937, an entirely different coding system, that involved using trigram and bigram substitutions [8]. A trigram (a group of three letters) was chosen from a codebook, encrypted at ground settings and, with the help of the bigram tables, turned into bigrams (pairs of letters), that were then transmitted in the message header. The recipient looked those bigrams up in his bigram tables, turned them back into trigrams and decrypted, to get the real message key [10].

The Poles had in 1937 managed to decrypt some Navy messages, due to a fortunate incident. A German torpedo boat had not received its instructions on the new system, and he was told in a message sent

Through another cipher which the Poles could break, to use the old system. Some messages from that boat were enough for the Poles to find ground settings for that day. Still, it wasn’t enough for them to work out the new indicator system. They suspected that it was a bigram substitution, but got no further. [8]

In 1939, Alan Turing, starting from where the Poles had left off, worked out the complete indi-cator system. In 1940, he was joined by Peter Twinn and together they started deciphering older Naval messages from 1938 (at that time Navy was still using only 6 plugs on the plugboard and those messages were easier to break). This task was helped by the EINS catalog (it was noticed that most frequently used word in Navy messages was ”eins” and a catalog of the encipherment of ”eins” at all 105,456 possible start positions was composed). In 1940, the British captured an armed trawler Polares and ac-quired some settings-lists and plaintext-ciphertext messages. That allowed them to partially recon-struct the bigram tables.

They developed a method, called Banburismus, for finding out the message keys. Banburismus works on the encrypted message keys and requires that the indicators had been encrypted using the same message settings. The idea of Banburismus is to guess the plaintext corresponding to those indicators by the statistical analysis of the mes-sages. Banburismus is based on observation that if two sentences in any natural language are taken and laid one above the other, then there are many more matches (places where two corresponding let-ters are the same) than there would have been, had the sentences been just random streams of letters. If two messages encrypted by Enigma at the same settings are taken, those matches would occur just as they did in the plaintext. If the message set-tings were not the same then the two ciphertexts would compare as if they were just random gibber-ish and there would be about one match every 26 characters. [6]

The codebreakers at Bletchley took two messages whose indicators differed only in the third charac-ter (for example, CGB and CGF), punched those messages onto thin cards (banburies) and slid those cards over each other, counting the holes that over-lapped at each offset. It was possible that if there

was a large number of the same cipher letters at some offset, that the there was the same offset be-tween the rightmost rotor start letters. [11] Using many such indicator pairs they constructed a “chain” of letters, for example G–B-H—X-Q, which could then be tried to lay over a letter sequence of an Enigma rotor. Some positions could then hope-fully be ruled out, due to breaking either the “self-reciprocal” (example 5.03) or the ”no-self-ciphering” (example 5.04) property of Enigma. [6]

Example 5.03 This position violates “self-reciprocal” property of Enigma. Letter G enciphers to B, but B enciphers to E.

.. G ... ... B ... H ... ... X ... Q

A B C D E F G H I J K L M N O P Q ♦

Example 5.04 This position violates “no-self-ciphering” property of Enigma. Letter H apparently enciphers to H.

... .. G ... ... B ... H ... ... X ... QA B C D E F G H I J K L M N O P Q ♦

When other, different chains are laid over the re-maining possibilities, choices can be further nar-rowed. With any luck, eventually there will be only one possibility left and from that, the right-most rotor used can be detected. If the British were lucky, the middle rotor could also be identi-fied, leaving significantly less wheel orders to be run on the bombes. The Banburismus was used until 1943, when the latest generation of bombe became so fast that it was easier just to brute-force the keys. [6]

VI. CONCLUSION

By 1945, almost all German Enigma messages 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.[7]

Enigma was a complex and powerful device. It could have been unbreakable, had the indicator pro-cedures been more secure and German operators more careful. The breaking of Enigma with the methods available at that time was a very hard feat and the dedication of cryptanalysts was admirable.

VII. REFERENCES

7.1 Journal Article

[1]. Enigma Machine from Wikipedia, the Free En-cyclopedia. http://en.wikipedia.org/wiki/Enigma machine

[2]. Cyclometer from Wikipedia, the Free Encyclo-pedia. http://en.wikipedia.org/wiki/Cyclometer

[3]. Bill Momsen. Codebreaking and Secret Weapons in World War II. http://home.earthlink.net/˜nbrass1/enigma.htm

[4]. Tony Sale. The Breaking of Enigma by the Polish Mathematicians. http://www.codesandciphers.org.uk/virtualbp /poles/poles.htm

[5]. Bombe from Wikipedia, the Free Encyclopedia. http://en.wikipedia.org/wiki/Bombe

[6]. Banburismus from Wikipedia, the Free Ency-clopedia. http://en.wikipedia.org/wiki/Banburismus

[7]. Cryptanalysis of the Enigma from Wikipedia, the Free Encyclopedia. http://en.wikipedia.org/wiki/Cryptanalysis

[8]. Tony Sale. The difficulties in breaking German Naval Enigma. http://www.codesandciphers.org.uk/virtualbp /navenigma/navenig1.htm

[9]. Tony Sale. Turing’s Work. http://www.codesandciphers.org.uk/virtualbp/navenigma/navenig2.htm

[10]. Tony Sale. Using the K Book and Bigram ta-bles. http://www.codesandciphers.org.uk/virtualbp/navenigma/navenig3.htm

[11]. Tony Sale. Banburismus. http://www.codesandciphers.org.uk/virtualbp/navenigma/navenig4.htm