MTAT.07.006 Research Seminar in Cryptography
The Enigma Cipher Machine

Kadri Hendla

November 28, 2005

Abstract

The aim of this survey is to give a brief overview on Enigma cipher machine and its cryptanalysis before and during the Second World War. The survey is mostly based on the articles [1] and [7] on Enigma from Wikipedia.

1 Introduction

Enigma is a portable cipher machine, famous for the role it played in World War II. The breaking of Enigma codes is considered to be one of the reasons for the Allies victory.

2 History of Enigma

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

3 Description of Enigma

Main parts of an Enigma machine are the keyboard, the set of rotors, the plugboard 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.

3.1 The Rotors

Rotors are the most important part of an Enigma machine. A 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; the wiring is different for each rotor. The rotor also has a finger wheel for turning the rotor by hand and an alphabet 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. The 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 military 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 contained 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 corresponding pawl and the stepping is achieved through the pawls engaging the ratchets. Every time a key is pressed, the first rotor on the right advances one position (one 1/26th of a full revolution). When the notch on that rotor is aligned with the pawl of the middle rotor, then on the next key press the middle rotor will step, too. This happens once for every 26 steps of the first rotor. Likewise, 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 the front of the machine. The plugboard offers a reconfigurable wiring, adding a great deal of strength to the encryption. An operator chooses two letters and connects them on the plugboard 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 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 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 plugboard 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.

4 Enigma in Use

For the message encrypted on one Enigma machine to be decrypted successfully on some other Enigma machine, both 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 plugboard 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 plugboard settings. The starting position of the rotors was (pseudo-) randomly selected by the operator and transmitted along with the decrypted message. The exact method of message composing is called the "indicator 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 using the ground setting (global starting position of rotors, as given in a codebook). The double encryption was for detecting transmission errors. Then he would turn the rotors to his own starting position and encrypt the actual message. The receiving operator would have set up his machine the same way and he 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 security flaws. First, the use of a global ground setting was by itself a bad idea. When 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 codebooks 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. Lets say that UHL was the result. Next he set the rotors accordingly to the message

key SXT and encoded the message text. Then he transmitted the first startposition (WZA) in the plain, followed by the encoded message key (UHL) and the ciphertext. The receiver set his machine to the position WZA, decoded the message key UHL, set the rotors to SXT startposition and decoded the message.

It is often said (in [3], [7]) that Enigma would have been an unbreakable system (at least in practice), had the Germans used it more carefully. The Enigma operators were often lazy or untrained, choosing easy message settings, like keyboard diagonals or triples of the same letter, their girlfriends initials, etc. and repeatedly using those settings, instead of choosing a new one for each message. [3] Routine messages were sent out day after day at about the same time, from the same place, of the same length and starting in exactly the same way [10], for example, "anx" ("an" = "to" in German, with "x" as a word separator) [3]. On one occasion, a German operator was asked to send a test message and he just pressed the T key repeatedly. When the codebreakers acquired a long message without a single T in it, they immediately realized what had happened [7]. All this made it easier for cryptanalysts trying to break Enigma.

5 Cryptanalysis of Enigma

5.1 Breaking of Enigma, Pre-World War II

Since the German Navy began using their enhanced Enigma in 1926 (the Army soon followed suit), the decryption of their messages was in practice impossible. Both the English and French cryptanalysts reportedly gave up and deemed Enigma unbreakable. But the Poles succeeded.

The Poles had purchased a commercial version of Enigma, but since the Germans had customized Enigmas, they didn't succeed in decrypting the messages. With the help from the French, they had obtained instructions for using Enigma and some outdated sheets of monthly key settings, which helped them to figure out the internal wirings of the three rotors. But Enigma was designed to be secure even if the enemy captured one of the machines. The Poles still had to come up with a way to get daily machine configurations. [3]

In 1932, Polish mathematician Marian Rejewski discovered a way to find the ground settings and message keys. He figured out the indicator procedure, which at that time was to encrypt the message key selected by the operator twice (using the global ground setting) and to transmit this encrypted message setting in the beginning of the message. This resulted in a relation between the letters. For example, if the ciphertext of the duplicated message key was JXDRFT, then it was known that J and R (1,4 pair), X and F (2,5 pair), D and T (3,6 pair) were originally the same letter. It was possible to find chains of how the identical letters changed, for example, from J to R to J again (a chain with a length of 2).

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 [2]. The cyclometer was, in essence, two Enigma machines side by side with their right hand wheels offset by three places [4]. Compiling of the catalog took over a year (it had 105,456 entries), but after that, finding daily settings took about 15 minutes [2].

On November 1, 1937, the Germans changed the reflector wirings and the card catalog turned useless [3]. The Poles didn't give up and started building a new catalog. That took less than a year, but in September, 1938, the Germans changed their indicator procedures, no longer using global ground setting for encrypting the message key, but letting the operator choose the startposition and transmitting that in the clear along with the message. Since the codebreaking methods so far relied on all message keys having the same startpositions, the catalogs and the cyclometer were ineffective once again [4].

An important observation was that sometimes the 1,4, 2,5 or 3,6 pairs were identical (for example, PST PWA) [3]. Another Polish cryptanalyst, Henryk Zygalski, realised that the occurrence of those pairs (called "females") depended on the wheel order and the start position. If enough of such pairs occurred, it might be possible to find a unique configuration for which all of those doubles could occur [4].

The technique used to do that, is known as "perforated sheets" or "Zygalski sheets". The method involved laying a series of perforated sheets over one another and shining a lamp underneath. Each sheet had 26 rows and columns, marked at the side

with letters of the alphabet. There were 26 sheet in a set (one set represented one possible position of the rotors), one for each position of the leftmost rotor. The rows of a sheet represented the position of the middle rotor, columns the position of the rightmost rotor. If a female was possible for some position of the rotors, a hole would be cut in that position. When the sheets were laid over each other and a light shone through in one place, a possible key had been found. [3]

Trying all those possible keys on an Enigma machine took a lot of time. Rejewski invented a machine that could test them automatically. It was called "bomba" (plural "bomby") and it consisted of three sets of scramblers (a set of rotors and a reflector), placed one machine cycle apart and driven by a motor. Unlike Enigma, the bomba had separate terminals for input and output letters. If it was assumed that the first three letters of a coded message, for example HJQ, represented the plaintext, for example ANX, input terminals H, J, and Q were energized and output terminals A, N, and X monitored. The machine stepped through all cycles until a match was found, and then stopped. For each test run 6 bomby were required. [3]

In 1939, the German Army increased the complexity of its Enigma operating procedures. They added two rotors to Enigma, three of which would be used at a time. The Germans also started to use a new indicator procedure, no longer enciphering 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 decided 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 mathematicians 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 5.1 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 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 codebreakers. 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. [5]

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 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 it, 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 transformation 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 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 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 setting under consideration could be ruled out. The process of this reasoning is described in 5.2 from [5].

Example 5.2 Let us assume that, for example, $P(A) = Y$. Looking at position 10 (in 5.1), we notice 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

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

While the crib does not allow us to determine what the values after the plugboard transformation are, it does provide a constraint between them. In this case, it shows how $P(T)$ is 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 contradiction, since in the beginning we had assumed that $P(A) = Y$. This means that our initial assumption was incorrect and so for this rotor setting $P(A) \neq Y$.

$\diamondsuit$

For a single setting of the rotors, each possibility for $P(A)$ could be tried. If all of the possibilities lead to a contradiction, then the rotor setting could be eliminated from consideration. The bombe mechanised this process, performing the logical deductions near-instantaneously using electrical connections, and repeating the test for all 17,576 possible settings of the rotors. The bombe consisted 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 symmetry 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 a lot harder to break. Naval Enigma had a set of eight rotors, from which three would be 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 was told, in a message sent

in 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 indicator 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). [9] Still, without the bigram tables, they were unable to attack German traffic. In 1940, the British captured an armed trawler *Polares* and acquired some settings-lists and plaintext-ciphertext messages. That allowed them to partially reconstruct 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 messages. 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 letters 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 settings were not the same then the two ciphertexts would compare as if they were just random gibberish 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 character (for example, CGB and CGF), punched those messages onto thin cards (banburies) and slid those cards over each other, counting the holes that overlapped 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 between 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 hopefully be ruled out, due to breaking either the "self-reciprocal" (example 5.3) or the "no-self-ciphering" (example 5.4) property of Enigma. [6]

Example 5.3 This position violates the "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 5.4 This position violates the "no-self-ciphering" property of Enigma. Letter H apparently enciphers to H.

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

When other, different chains are laid over the remaining possibilities, choices can be further narrowed. With any luck, eventually there will be only one possibility left and from that, the rightmost rotor used can be detected. If the British were lucky, the middle rotor could also be identified, 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]

6 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.[7]

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

methods available at that time was a very hard feat and the dedication of cryptanalysts was admirable.

References

[1] Enigma Machine from Wikipedia, the Free Encyclopedia.
http://en.wikipedia.org/wiki/Enigma_machine

[2] Cyclometer from Wikipedia, the Free Encyclopedia.
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 Encyclopedia.
http://en.wikipedia.org/wiki/Banburismus

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

[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 tables.
http://www.codesandciphers.org.uk/virtualbp/navenigma/navenig3.htm

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