THE ENIGMA CODE

Cracking the Enigma

To what extent Enigma revolutionized the transport of information?

2018-2019

G2

ABID CHAREF Samy – BARRET Hadrien – THOMAS Clémentine – VERNOUX Thomas – VIGNAUD Samy

1. Introduction

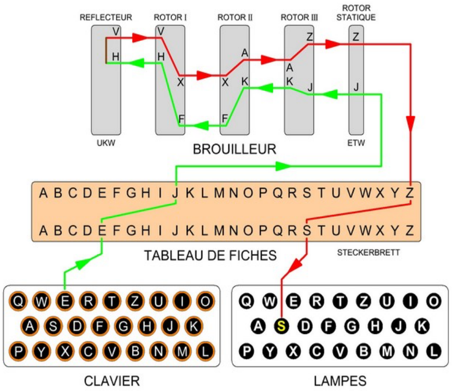
Enigma is a handheld electromechanical machine used in the encryption and decryption of information which was created in 1919. Yet its simplistic appearance, the machine is actually considered as one of the most dreadful encryption systems of the history. It presents itself as a writing machine, which was first used for commercial purposes, and then in 1926, bought by the German army. Indeed, its impact during the first years of war is unheard-of, it made completely unpredictable the messages of the Germans and Axis powers. Close to defeat, The Allies united their forces by calling for the help of the best mathematicians of Europe in order to find a solution. Finally, in 1940, Alain Turing developed the first algorithm to break the code and thus created the first computer in history.
In this study we will try to show how Enigma revolutionized the transport of information. First, we'll focus on the Enigma machine and then we'll highlight the methods that scientists used in order to crack the code.

2. The Enigma machine

A) The functioning of the Enigma machine

The Enigma machine fits in a small wooden box not bigger than a typewriter. Inside the box there is nothing more than few gears and cables that connect a keyboard (plugboard) to a lamp panel where each lamp is associated to a letter of the roman alphabet.
To encrypt a message, one must type letter by letter said message and, after each stroke on the keyboard, wright down the letter illuminated on the lamp panel. Moreover, to decrypt a received message, the operator needs the parameters of the encrypting machine and then just to type the encrypted message back on the keyboard to get the meaningful message.
When someone trikes the keyboard, it closes an electrical circuit. This circuit goes through three scramblers which are each substituting two letters of the alphabet. If someone pressed the letter A on the keyboard, at the exit of the first scrambler we might get a D, that will then be "transformed" by the following scramblers. After the last scrambler there is a reflector which feeds back to this scrambler the substituted letter. At this point the circuit works the same as on the way in, with the notable exception that it leads to the lamp panel. On the picture below there is a simple representation of the circuit.

Meanwhile someone is using Enigma, after each stroke the first scrambler rotates by 1/26th of a circle.



Once the first scrambler is back at its initial position, the second scrambler then rotates in the exact same way by 1/26th of a circle. The same relationship exists between the second scrambler and the last one. This particular functionality is some of what makes Enigma a great encryption machine.

B) Combinatorial problem

The combinatorial encryption system of the Enigma machine is interesting because it is really hard to decipher an intercepted message. The complexity of the mechanism is based on the presence of scramblers. It allows the fact that two letters typed on the keyboard one after the other are not connected. This creates a large number of possible links. There are three scramblers aligned in a jammer and each having twenty-six electrical contacts on each side, randomly connected. So, each rotor corresponds to a coded alphabet. Each time a letter is typed on the keyboard, the first scrambler rotates one notch, which completely changes the coded alphabet into another. When the first scrambler has made a complete rotation, the second scrambler turns up a notch, etc. We call them poly-alphabetic substitutions. The three aligned scramblers create $26 * 26 * 26 = 17{,}576$ different combinations, in addition to the possibility of switching them. In the jammer there is also a reflector which allows for example that if A is coded as B then B is coded as A. The machine has also a table of sheets. Ten plugs are connected every day, which results in the permutation of twenty letters. This creates $1{,}507{,}382{,}749{,}377{,}250$ possibilities. Finally, if we multiply the possibilities created by the three scramblers by the possibilities created by the plugs, we obtain an impressive number of combinations exceeding billions of billions.

3.Cracking the Enigma: The Bomb

In this section we will underline the flaws of the machine and therefore understand how the mathematicians managed to crack it. First of all, we must highlight one aspect of Enigma, paramount in its functioning.

Indeed, as an extra precaution, the Germans had the great idea of using the day key settings in order to send a new message key for each message. The message keys would have the same plugboard settings and scrambler arrangement as the day key, but different scrambler orientations. First, the sender sets its machine according to agreed day key for example (QCW), then he randomly picks a new scrambler orientation for the message key, say PGH and thus encipher it conforming to the day key. To put it in a nutshell, the message key is typed into Enigma twice; for example, the message: PGHPGH is enciphered as IAHGEZ.

A) The polish solution

At first sight the system seemed to be impregnable, but the Polish cryptanalysts were undaunted. Indeed, they managed with the help of some great minds such as Marian Rejewski to crack the code by understanding Enigma's main weakness: repetition.

Rejewski's strategy for attacking Enigma focused on the fact that repetition is the enemy of security: repetition leads to patterns, and cryptanalysts thrive on patterns. The most obvious repetition in the Enigma encryption was the message key which was enciphered twice at the beginning of every message. Rejewski would receive intercepted messages where the first six letters contained the message key. In each case, the 1st and 4th letters are encryptions of the same letter, same for the 2nd and 5th etc.… If he had access to enough messages in a single day, then he would be able the alphabet of relationships. Here is an example:

1	A	F	W	B	H	L	X	Y	Z
4	F	W	A	Q	G	R	S	D	K

The next step, probably the most important one, consists on determining the day key by looking at the table of relationships. Rejewski would look for patterns within the table, hence he began to study one particular type of pattern: the chain letters. If we use the example presented before, we have: A

→ F → W → A (3links). (The chain is complete). Thanks to those links, Rejewski could reduce the number of possibilities to 105 456 instead of ten million of billion. Finally, the polish would test all the remaining positions, find the correct one and therefore unravel the Enigma cipher.

B) The Bomb

Yet, this solution wasn't enough. Indeed, the Nazis would optimize the machine before the beginning of the war by using for example five scramblers instead of 3, which would lead to a bigger number of possibilities hence table of relationships harder to find. For that reason, all the brilliant minds of that time joined forces at Bletchley Park in order to find a solution, that turned out to be quite simple.

The first step was to suppose a word that could be in the message, for example "WETTER" which means weather in German. Next, they needed to find the exact place of the word in the message in order to uncover the enciphered letter of W, E, T .... Which isn't difficult because they knew that a letter can't be encrypted by itself. Therefore, they would write WETTER behind the intercepted message and try to find the good position of the word. Indeed, this method eliminates many different combinations possible and therefore simplify the combinatorial problem.

Thanks to this idea, the scientists of Bletchley park lead by Turing built the famous "Bomb", and thus cracked the Enigma code.

4.Conclusion

"Mathematicians have won the war!" shouted a man in the film "A Beautiful mind".
Without the accomplishments of these great scientists, the Allies would have probably lost the war. This fight against this Nazis' machine marks the beginning of a new era in cryptography. Enigma revolutionized the encryption of information and is the transition from manual to automatic in cryptography. It also initiated the digitization of many areas of our current world such as security or cybercommerce.