UNIVERSITATEA
BABEŞ-BOLYAI

# History of computer science
# - Encrypted Machine -

Nicolas Frangi

French Student nicolasfrangi@outlook.fr

# Contents

# 1 Introduction

During the World War I, the amount of cipher messages and xdecipher messages increased enormously. The radio made possible the communication and abled the division, corps and army levels to transmit messages faster and in a secure way. By this time, a nation needed to secure all of this transmitions by encoding messages in order to give some strategic protocols to the front. In the same time, Thomas Jefferson, Etienne Bazeries, Parker Hitt and Joseph Mauborgne developped a machine that combined polyalphabetic cipher system, alphabets written on strips of card board that slid along in a frame and turn it into a cipher cylinder. Thanks to that, after the World War I, the first cipher machine appeared.

In the $20^{\text{th}}$ century, the improvement of the machine continued. Indeed, one Army did not want to escape an important message to the other one. By this fact, smart people make the effort to create complexed and secured machine to facilitate the communication. We will see in this report the improvement of the electromechanical machine during this century, how the Turin's device make possible to solve the Enigma and then, the heritage of Enigma.

# 2 Electromechanical improvement

A few years after the Wolrd War I, Jefferson, Bazeries, Hitt and Mauborgne, located in four different countries, implemented a device that generate a polyalphabetic ciphertext. This method consists in corresponding a letter for example the ***A*** with an other letter ***F***. This means when I am writing ***Czggj***, you will decipher the word and read ***Hello***. The device used small and standard typewriter keyboards. The machine automatically change the cipher message into an understanding word by the rotor (fig.1).

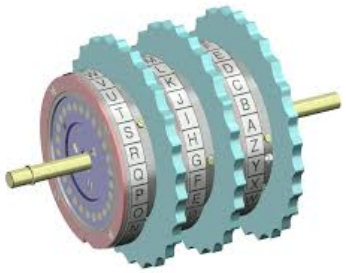


Figure 1: 3 rotors

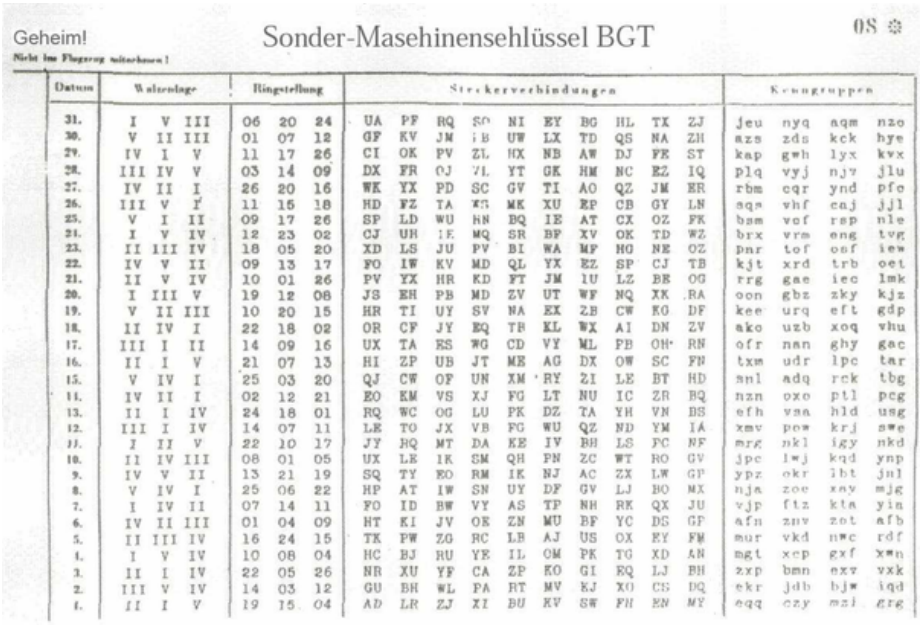
In this time, all the rotors machines had in common is that the rotor has been used to encipher a letter. When the rotor rotated for the first time, a letter appeared, but if the user put the same letter a second time, he should seen a different substitution letter. This is due to the period of 26 letter. Then, if you decided to put an other rotor you will give the decryption more difficult. Truly, if you have just one rotor, the period becomes 26 and you only have 26 mixed cipher alphabets. On an other hand, if you add two rotors, you will have 26 x 26 = 676 periods so 676 mixed cipher alphabet. The cipher was more difficult to decipher thanks to the number of rotors.

Then, Arthur Scherbius created a machine, inspired by the Hugo Koch's patent. This ciphering machine was based on desynchronizing rotors to do both encryption and decryption with a set of three rotors in fixed positions, allowed to do a 17,576 alphabet period. He sold his first version to the German Navy and others examples like the Enigma-D, the more spreading machine. In 1929, the German Army modified the model D by adding 2 more rotors to strengthen the security. At this time, German had a machine that can did 1,054,560 alphabet period.

By the end of the war, German placed an other rotor in order to secure the device and the deciphering (54,837,120 periods). Moreover, they fixed a half-rotor called *reflector* and a *plugboard*. This plugboard is like an old fashion telephone, counts ten wires and each wire connect two letters into a pair and they can be swipe over. So, it is an extra level of scrambeling only available for military. These two componants allow to the machine to add about 150 trillion combinations of letters to the period. People tried to make the machine unbreakable by adding rotors in order to multiply the number of periods and to involve machine to make them more secure as possible.

By the way, the people who cipher and decipher the message needed the same machine and the same settings. So they have to know how to adjuste the machine before ciphering or deciphering the code. To do that, this two people had a sheet of paper (figure 2) renewed each month. In this paper, it is written the settings of each day for a month. Thanks to this paper they have succeded to send message but sometimes, the paper were stolen by spies and given to the French and British. At the outbreak of war, Germans changed the cipher system daily to increase the security and to give the understanding of the code more difficult.

The nice point of this story is that the Navy used soluble ink in order to keep the secret if the boat sank.



Geheim!

Nicht ins Flugzeug mitnehmen!

Sonder-Masehinensehlüssel BGT

08 ❁

| Datum | Walzenlage | Ringstellung | Steckerverbindungen | Kenngruppen |
|---|---|---|---|---|
| 31. | I V III | 06 20 24 | UA PF RQ SO NI EY BG HL TX ZJ | jeu nyq aqm nzo |
| 30. | V II III | 01 07 12 | GF KV JN IB UW LX TD QS NA ZH | azs zds kck hye |
| 29. | IV I V | 11 17 26 | CI OK PV ZL HX NB AW DJ FE ST | kap gwh lyx kvx |
| 28. | III IV V | 03 14 09 | DX FR OJ VL YT GK HM NC EZ IQ | plq vyj njv jlu |
| 27. | IV II I | 26 20 16 | WK YX PD SC GV TI AO QZ JM ER | rbm cqr ynd pfo |
| 26. | III V I | 11 15 18 | HD FZ TA KS MK XU EP CB GY LN | aqs vhf caj jjl |
| 25. | V I II | 09 17 26 | SP LD WU HN BQ IE AT CX OZ FK | bsm vof rsp nle |
| 24. | I V IV | 12 23 02 | CJ UH IE MQ SR BF XV OK TD WZ | brx vrm eng tvg |
| 23. | II III IV | 18 05 20 | XD LS JU PV BI WA MF HG NE OZ | pnr tof osf iew |
| 22. | IV V II | 09 13 17 | FO IW KV MD QL YX EZ SP CJ TB | kjt xrd trb oet |
| 21. | II V IV | 10 01 26 | PV YX HR KD FT JM IU LZ BE OG | rrg gae iec lmk |
| 20. | I III V | 19 12 08 | JS EH PB MD ZV UT WF NQ XK RA | oon gbz zky kjz |
| 19. | V II III | 10 20 15 | HR TI UY SV NA EX ZB CW EG DF | kee urq eft gdp |
| 18. | II IV I | 22 18 02 | OR CF JY EQ TB KL WX AI DN ZV | ako uzb xoq vhu |
| 17. | III I II | 14 09 16 | UX TA ES WG CD VY ML PB OH RN | ofr nan ghy gac |
| 16. | II I V | 21 07 13 | HI ZP UB JT ME AG DX OW SC FN | txm udr lpc tar |
| 15. | V IV I | 25 03 20 | QJ CW OF UN XM RY ZI LE BT HD | snl adq rck tbg |
| 14. | IV II I | 02 12 21 | EO KM VS XJ FG LT NU IC ZR BQ | nzn oxo ptl pcg |
| 13. | II I IV | 24 18 01 | RQ WC OG LU PK DZ TA YH VN BS | efh vsa hld usg |
| 12. | III I IV | 14 07 11 | LE TO JX VB FG WU QZ ND YM IA | xmv pow krj swe |
| 11. | I II V | 22 10 17 | JY HQ MT DA KE IV BH LS FC NF | mrg nkl igy nkd |
| 10. | II IV III | 08 01 05 | UX LE IK SM QH PN ZC WT RO GV | jpc lwj kqd ynp |
| 9. | IV V II | 13 21 19 | SQ TY EO RM IK NJ AC ZX LW GP | ypz okr ibt jnl |
| 8. | V IV I | 25 06 22 | HP AT IW SN UY DF GV LJ BO MX | nja zoe xny mjg |
| 7. | I IV II | 07 14 11 | FO ID BW VY AS TP NH RK QX JU | vjp fiz kta yin |
| 6. | IV II III | 01 04 09 | HT KI JV OE ZN MU BF YC DS GP | afn znv zot afb |
| 5. | II III IV | 16 24 15 | TX PW ZG RC LB AJ US OX EY FW | mur vkd nwc rdf |
| 4. | I V IV | 10 08 04 | HC BJ RU YE IL OM PK TG XD AN | mgt xcp gxf xwn |
| 3. | II I IV | 22 05 26 | NR XU YF CA ZP EO GI EQ LJ BH | zxp bmn oxv vxk |
| 2. | III V IV | 14 03 12 | GU BH WL PA RT MV KJ XO CS DQ | ekr jdb bjw iqd |
| 1. | II I V | 19 15 04 | AD LR ZJ XI BU KV SW FH EN MY | eqq czy mzi grg |

Figure 2: Paper code

# 3 A flaw in the system

Before the period of the Second World War II, the machine called Enigma was one of the best unbreakable cipher machine. French and British acquired this machine on september 1939 in order to work on and to decipher Enigma. By november 1939, a brilliant mathematician, Alan Turing who was working in part-time for the British Government's Code and Cypher School took up his full-time to work at Bletchley Park. He began trying to crack and decipher the military codes.

Figure 3: Alan Turing

However, Alan Turing started to use the Bombe. This is the name given to a machine developped by Turin and Welchman, inspired to the electromechanical machine designed by Rejewski, Zygalski and Rozicki. This machine allowed to increase the speed of the codebreaking process. In simple word, when a message was intercepted, code breakers had to search cribs. These cribs were pieces of plain text written in the encrypted message. Once one was located, they associated with special techniques the letters of ciphertext and their plain version. Then, they entered the associations in the machine. The Bombe replicated the rotors and ran through all the possible settings to find the key that belong to the given pieces of cipher and plain text. When the Bombe have found these settings, all the messages with these parameters could be deciphered.

This tool can retrieved by cryptanalysis different sources of codes. It had an important role during the war because it could avoid suspicion against the German's. It was used carefully mainly after a real source could be confirmed in order to not be suspected and to not let the German thought that their ways of communications are deficient.

# 4 The heritage of Enigma

In a mean time, when the Swiss knew that the Enigma had been broken by cryptanalysts, the Captain Arthur Alder, a mathematician's professor working at the University of Bern designed a new model of a machine between 1941-1943. The first prototype became available on the spring of 1944. Then, on 1945, began a production of 640 machines but the first machine was only used on 1947. This machine, called Nema (a), is composed with 10 wheels but only 5 are electrical. Four of them are the coding wheels and have got 26 contacts at either side. The fifth one is like the reflector of the Enigma machine, it can only be setting. It also contains a lamp panel with 26 letters of the alphabet, which match with the keys on the keyboard. The most of this machine is that the spacebar and these keys are connected to an electronic typewriter (or a teletype). Therefore, this machine has been improved by its design and its difficulty to be deciphered but inherited of some weaknesses of the Enigma, like this fact: one letter can never be enciphered into itself.

In an other hand, let me introduce the Fialka machine (b). This machine had been used during the Cold War Era by the Soviet and has been unveiled only in 2005 because the Soviet kept this device secret. It is also a cipher machine, but this time, inspired by the Enigma machine and the Nema one. We can see that Fialka derive of the Nema because it does not contains 5 but 10 electrical wheels, and each one has got 30 contacts with mechanical pins to control stepping. It does not contains a plugboard and the reflector has been eliminated because it was a weakness of the Enigma. It is composed with unitary and disassemblable rotors that offered to the machine a better way to encrypted a message. We have to know that a daily key book was nec-

essary to set the machine in order to cipher or decipher a message. This book, as its name implies, contains day key for one month. One of a day key, valid for 24 hours, consists of a key table and a punched card. Thanks to those elements, you can fixe the rotor systems, initialize the order of the rotors on the axle and set the parameters to decrypt the message.

(a) Nema

(b) Fialka

# 5 Conclusion

During the $20^{th}$ century, plenty of machines were born to secure communication with people particularly in the time of War. Most of them had been used in order to deliver message secretely but some partisans decided to crack and decipher message to know what possible strategy could be opered for the opposit army. Thanks to these codebreakers, the improvement of Machine increased throughout this century and people tried to make more secure and more efficient encoding cipher machine. Nowadays, we can broadcast a message only in typping on a smartphone or with a messaging service on a laptop. Moreover, the communication is not secure at all because of laws and the implementation of application. All day long, because of microphones putting on our devices, we are listening, tracking and spying that make people not free, and make our private life vulnerable.

# 6 Bibliographie


• John.F.Dooley, Springer, *A brief history of cryptology and cryptographic algorithms*

• LilHelpa, Rotor Machine, 03/13/2020, `https://en.wikipedia.org/wiki/Rotor_machine`

• Bot de pluie, Hugo Koch, 01/22/2020, `https://fr.wikipedia.org/wiki/Hugo_Koch`

• `https://math.dartmouth.edu/~jvoight/Fa2012-295/EnigmaSimManual.pdf`

• `https://calculate.org.au/2015/02/03/crack-enigma-code/`

• `https://www.babelio.com/auteur/Alan-Turing/104559`

• `https://en.wikipedia.org/wiki/NEMA_(machine)`

• `https://www.cryptomuseum.com/crypto/nema/index.htm`

• `https://en.wikipedia.org/wiki/Fialka`