King’s College London

The Enigma Machine

Cryptography

Student: Lourenço Santos (K21209242)

Dr. Ievgeniia Kuzminykh

Prof. Luca Viganò

Content

List of Figures

History and type of cipher

The Enigma Machine was invented in 1918, the last year of WW1, by Arthur Scherbius. This machine was specially used by the German military to encrypt their communications during WW2. It started out to protect commercial privacy, but the Nazis developed additional mechanisms to adapt to the battlefield. As an example of these mechanisms, we have the plugboard to substitute the input letter to another one, which increased significantly the complexity. (Jiaxin Guo, 2022)

Breaking down the Enigma machine was one of the top priorities for the Allies, and it was achieved by Alan Turing as we'll discuss later on.

This machine uses a form of substitution encryption, which is a straightforward way of encoding messages, but easy to break, such as the Caesar cipher. The main difference between them is that each time a letter was mapped to another, the entire encoding scheme changed.

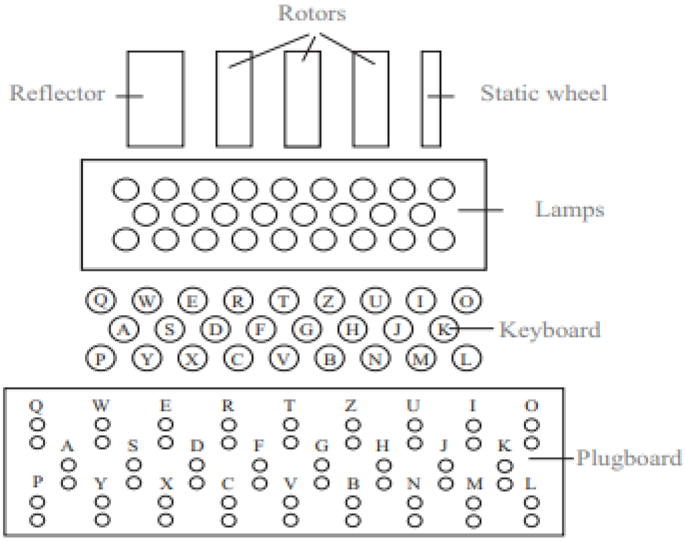
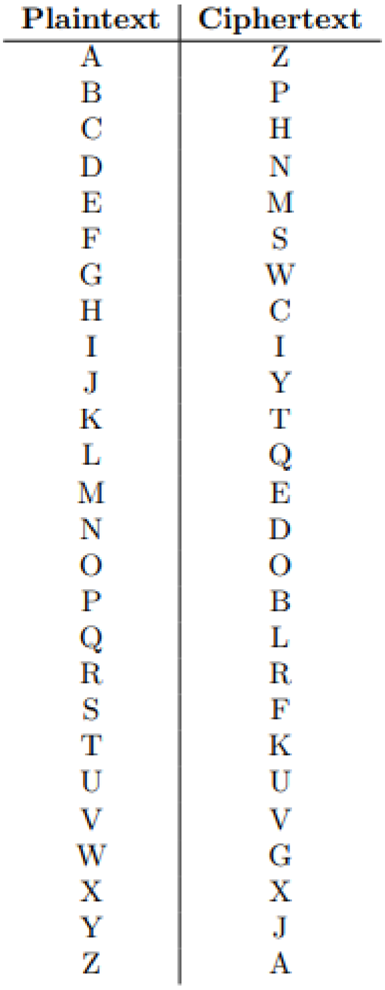


Figure 1- Components of an enigma machine (Jiaxin Guo, 2022)

Encryption

The *plugboard*, aka *steckerbrett*, was added by the German army to the Enigma Machine in 1930, which allows letters to be swapped. Enigma's plugboard had an electrical port for each letter, and operators were given 10 chords to connect various letters. Essentially, 10 letters would be swapped with 10 other letters.

For example, imagine the operator was told to connect the 10 wires in the following way: AZ, BP, CH, DN, EM, FS, GW, JY, KT, LQ. Then the *plugboard* would essentially be a simple substitution cipher with the encryption alphabet depicted in Figure 3. (Hurlbut, 2018)



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

Figure 2- Plugboard Encryption (Hurlbut, 2018)

Some of the letters —in this case I, O, R, U, V, and X—are encrypted to themselves. The other 20 letters in the alphabet are swapped with another letter.

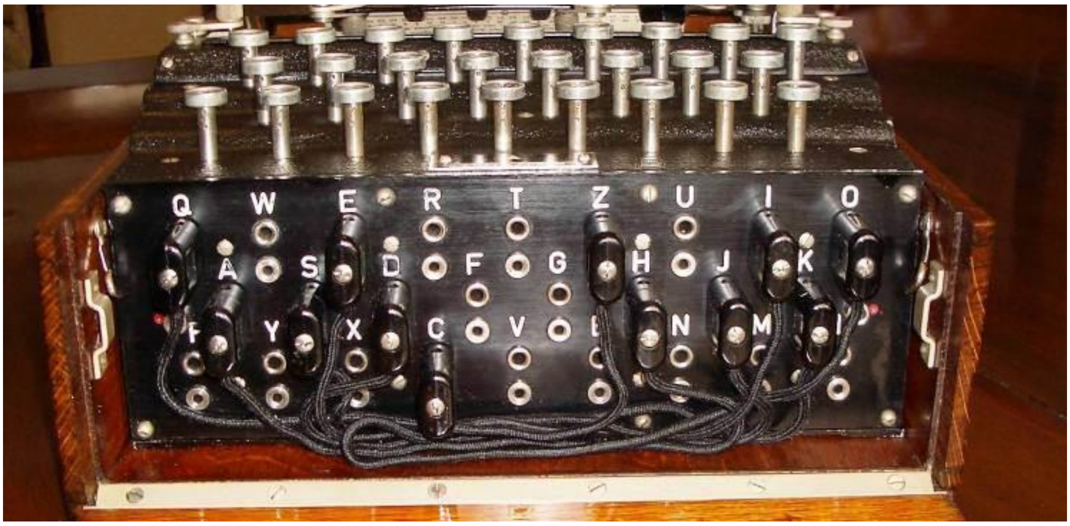


Figure 3- Enigma Machine Plugboard

Next, we have the 3 rotors, each one will display a number or a letter, and when the rotors turn, a new set of 3 numbers/letters appears. Each rotor has 26 numbers/letters on it. Since this machine takes the 3 rotors at the same time, the Germans could interchange rotor, choosing from a set of 5. (Brilliant.org, 2022)

There are 26 starting positions for each rotor, so there are:

$$26 \times 26 \times 26 = 17{,}576$$

choices for initial configurations of the rotors.

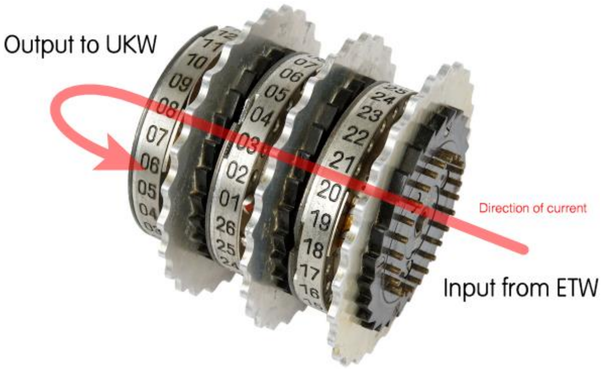
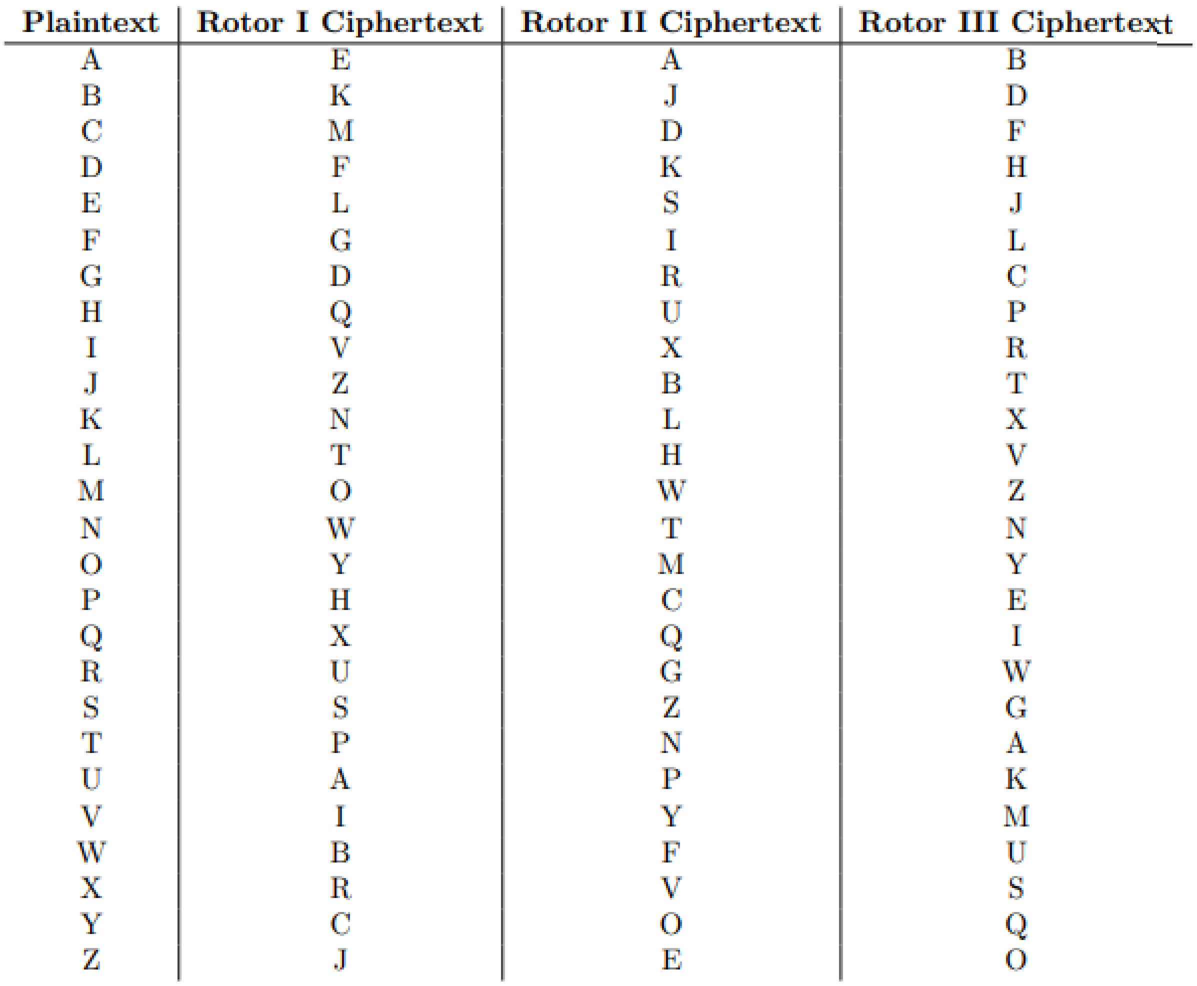


Figure 4- Rotors of the Enigma Machine

This ability to change the mapping is important because once someone deduces that G is A, they'll know that's true for every G in the ciphertext.



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

Figure 5- Encryption by the 3 rotors (Hurlbut, 2018)

Succeeding, we have the *reflector*, that performs a symmetrical encryption, meaning that the process of decryption is the same, and then sends the electrical signal back through the machine.

Finally, the signal makes it back to the *lampboard*, the final component. The *lampboard* is arranged like a keyboard, and each letter has a small light bulb beneath it. When the electrical current reaches a letter, the corresponding bulb flashes on, indicating that this is the encrypted letter.

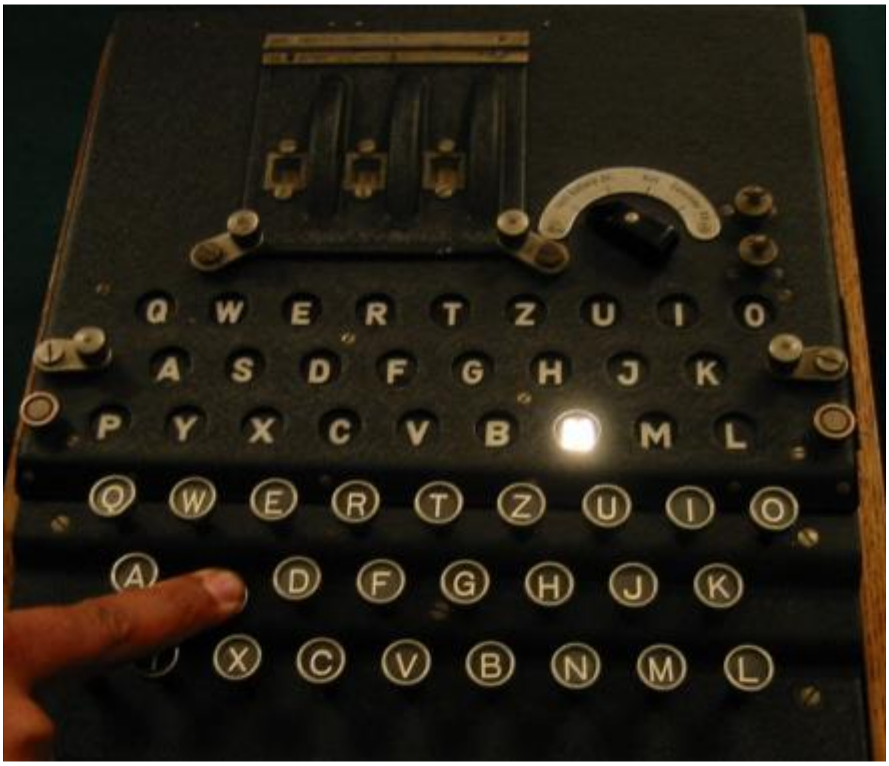


Figure 6- Lampboard of the machine

Decryption

In 1933, three Polish mathematicians were able to develop an electromechanical machine, called Bomba, which could eliminate impossible settings from the onset and run through potential settings.

Later, the German army had improved the security by changing the cipher system daily. The famous Alan Turing and his colleague Gordon Welchman, working at Bletchley Park, developed a machine known as the Bombe which used electric circuits to solve an Enigma encoded message in under 20 minutes.

The Bombe

The British Bombe machine was essentially 36 Enigma machines wired together, this way, the Bombe machine would simulate several Enigma machines at once. Each of this Enigma simulators in the Bombe had three drums, one for each rotor.

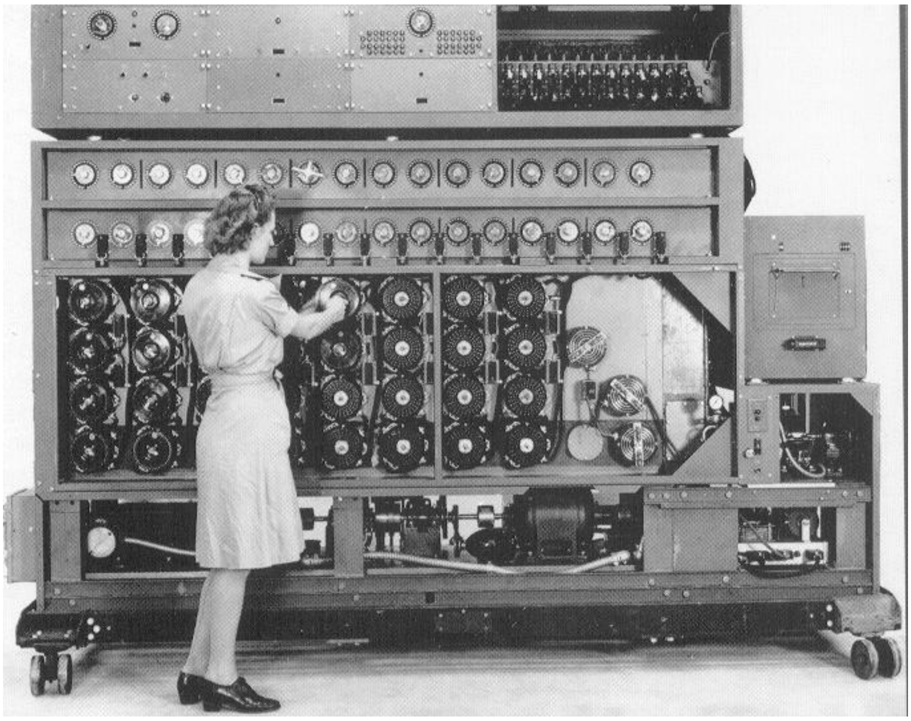
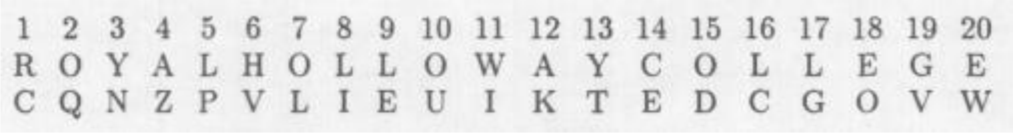


Figure 7- The Bombe

For each full rotation of the top drums, the middle drums were incremented by one position, and likewise for the middle and bottom drums, giving the total of 26 × 26 × 26 = 17,576 positions of the 3-rotor Enigma scrambler. (Brilliant.org, 2022)

Turing’s machine used assumptions about known plaintext within the message, called a crib. The process of finding cribs is greatly aided by the fact that a letter is never encrypted to itself. (Hurlbut, 2018)



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
R	O	Y	A	L	H	O	L	L	O	W	A	Y	C	O	L	L	E	G	E
C	Q	N	Z	P	V	L	I	E	U	I	K	T	E	D	C	G	O	V	W

Figure 8- A message and its ciphertext equivalent

In Figure 9, a line connecting two letters indicates that Enigma encrypts one letter to the other at the indicated position.

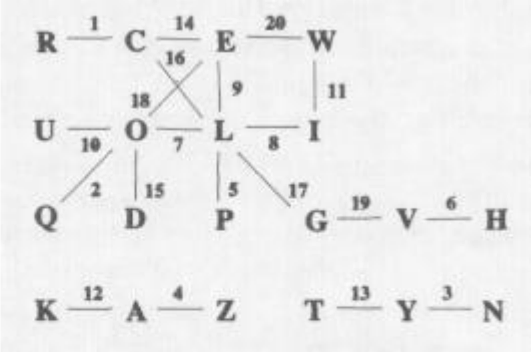


Figure 9- Crib-Ciphertext pairing

An operator would set up the Bombe using a similar diagram. The machine would then run through and eliminate candidate settings that were incompatible with the given menu. (Hurlbut, 2018)

Examples of Use

This machine was used to encrypt and decrypt messages by the Nazis during the WW2 and the settings would be changed daily to enforce security. They exchanged confidential information through this machine such as strategies, commercial and military information.

Therefore, this was such a big deal for the Allies to be able to decipher the encoded text that the germans were exchanging.

Figure 10- Germans using Enigma Machine during WW2

Strengths and Weaknesses

Strengths

By that time, the enigma machine was considered the most advanced cryptosystem. Other than this, it was flexible, portable, reasonably rapid, and easy to use. It could be easily carried by one person, it didn’t require any mathematics and, once the daily settings were in place it was considered as easy as using a standard typewriter.

It was safe against frequency analysis, against the Kasiski and Index of Coincidence methods, because of the key length, it was secure against brute-force because there are 15,000,000,000,000,000,000 possible settings.

Another strength was that it allowed extensive exploitation of radio, allowing Germans to capitalize radio technology

Weaknesses

The biggest vulnerability in this machine is its symmetry, meaning that the process of encryption/decryption is the same, due to the *reflector.*

Though, the biggest weaknesses on this Enigma were related to military practices and human errors. German intel had rules that decreased the key space of Enigma, regarding the plugboard, the settings always used exactly 10 wires, and connecting sequential letters on the plugboard was not allowed. This way, the number of possible settings was reduced from

3 × 10^114 to 1 × 10^23

Even though the Germans did implement some security improvements, these modifications were always implemented one at a time, giving the time for the cryptanalysts to understand and adjust the settings. If they had implemented multiple new settings at a time, it would’ve been harder to crack.

References

Brilliant.org. (2022, November 19). *Enigma Machine*. Retrieved from Brilliant: https://brilliant.org/wiki/enigma-machine/

Hurlbut, A. (2018, 11 27). The Enigma Cipher Machine. pp. 1-24.

Jiaxin Guo, Y. H. (2022, April 20). 2022 International Conference on Big Data, Information and Computer Network (BDICN). *Analysis and Illustration of the Enigma Machine*, pp. 1-13.

Wikipedia. (2022). *Enigma machine*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Enigma_machine