Cryptology project

Introduction to Cryptography

Dreyer Mathieu, Jacque Antoine

Academic Year 2019–2020

Academic supervisor: Gabrielle De Micheli

Contents

1 Introduction

This report will deal with the Enigma machine. The Enigma machine is known for its use during World War II. This report will first focus on the usefulness of the machine, with a description of the machine, its use in history, from its manufacture to its privatized use for the army, and its cost of deployment. We will also see if it is still topical. Then a more detailed analysis will be made in a second time, with at beginning an analysis of its cryptographic system, and How it work. Afterward the analysis will be focused on how to use the machine, its possible advantages and disadvantages. Lastly an analysis on the possible attacks will be made.

2 Some history points

2.1 Machine purpose

Enigma encrypts information by passing an electric power through a series of components. This current is transmitted by pressing a letter on the keyboard; it goes through a complex network of wires and then lights a lamp that indicates the encrypted letter. The first component of the network is a series of 3 adjacent wheels, called "rotors", which contain the electrical wires used to encrypt the message. Each rotors rotate, changing the complex configuration of the network each time a letter is typed. Enigma usually uses another wheel, called a "reflector", and a component called a "switchboard".
To make things even more difficult, different parts of the machine could be set up in different ways, with each setting producing a unique stream of enciphered letters. Unless you knew the exact settings of the machine, you couldn't decipher the messages.

The Enigma machine reproduces a polyalphabetic substitution cipher rendered complex to avoid decryption. We will proceed to explain the system electro-mechanics of a standard Enigma, the one used in the Wehrmacht. It consists of three elements connected by electrical cables :

- - A keyboard for entering plain text.
- - The encryption device that replaces each letter of the plain text with a letter encrypted.
- - A luminous board that displays the numbered letter. Thus, when a key on the keyboard is pressed, an electric current from the keyboard goes through the encryption device and turn on a diode in the light panel that corresponds one-letter code

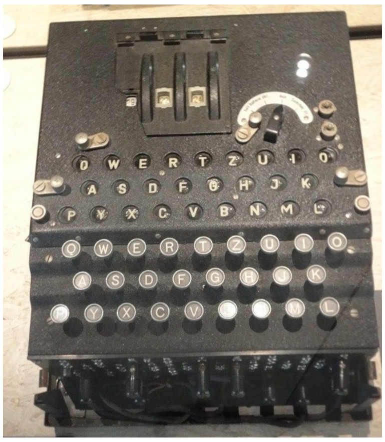


Figure 2.1: Picture of Enigma

2.2 Historical use

Considering the difficulty they face in ensuring the security of communications at the beginning of the 20th century, cryptologists are adapting to new techniques, and devise automatic devices to enable encryption by substitution polyalphabetic that would otherwise be tedious. Almost simultaneously, four inventors from different countries invented electro-mechanical encryption machines, based on the principle of generating numerous ciphered alphabets by means of cylinders that electrical circuits pass through: the American Edward Hugh Hebern marketed his machine in 1917, intended for the military, but filed for bankruptcy a few years later. If the machine was a fiasco in its civilian version, it was going to get its renowned for its use by the military.

In the 1920s, the German army was forced to recognize the poor security of its troops. offered by its ADFGVX encryption system. This change of mindset was made following the publication of two books, one by English Admiral John Fisher, the other entitled The world crisis written by Winston Churchill who was then head of the British Navy. These two books highlighted the decisive advantage of Great Britain in the First World War thanks to the successes of British cryptanalysts on the German messages.
The German army, faced with a fait accompli, carried out an investigation and concluded to the need to equip yourself with Enigma. It was first of all the new German navy, the Reischmarine, in 1926; then the regular army, the Reichswehr, in 1928; and finally the army of air, the Luftwaffe, in 1935. But it wasn't until Hitler's accession to power in 1933. for the German army to equip itself massively with Enigma. That's almost 200,000 machines which were built until 1945, this production having been delegated to several German firms.

According to the key card, before 1940, the Germans used the daily key and starting position. The operator selected a random message key. This message key has been encoded twice to eliminate errors. For example, a word is encoded twice, using 2 different codes, because it is known that the key contains 3 characters. Then, the operator moves the rotor to the information key and encodes the information.
The two letter words that make up the encoded message key are sent with the message. The receiver places its machine in the starting position described in the code book, and then decodes the triplet to put it back into the message key.
He then placed the message key at the beginning of the computer to continue decoding the rest of the message. However, this process is actually a security hole.
we will detail this process in the rest of this report.
This security issue allowed the Polish Encryption Agency to crack pre-war Enigma messages.

The German army used Enigma throughout the war until its defeat.
Such use was necessary because of the new way of waging war. that appeared with the Second World War. This section allows you to get a picture of Enigma's use in the war.
The Blitzkrieg implemented by the Germans during World War II was a strategic innovation, enabled by new inventions in the and communications since the beginning of the First World War.

The Royal Navy is organizing several raids against armed trawlers and weather ships. Catch teams board U-boats abandoned by their crews. Each time, manuals and documents are captured, like bigram tables, the manual used to encrypt weather reports and the manual used to encrypt short messages.

The British Typex coding machine and several of the American machines such as SIGABA, the M-134-C or the TSEC/KL-7 known as the ADONIS code, used by NATO forces, operated on similar principles to Enigma, but in a much more secure manner. Edward Hebern's first modern cipher cylinder machine is considered less secure, a fact noted by William F. Friedman when it was acquired by the US government.

2.3 Still relevant or not

The machine is still much talked about today, as much for collectors as for Internet users, who share a lot of information on this machine. [5] There are some sites that allow to simulate the operation of enigma [2]
The mathematical principle of the machine is known, it is not as safe as before but it can be a basis for reflection for other types of machines.

2.4 Cost of deployment

The first commercial version of Enigma was sold in 1923 for the equivalent of €30,000. Currently the price for an Enigma machine varies between $40 000[1] and $250 000. [4]

3 Cryptographics concepts

3.1 Perfect crypto system

The problem with most of the cipher is that a same letter can be regularly encoded in the same scheme. It imply that the attacker can decode the message using a statistic attack. In order to prevent this type of attack and have a perfect crypto machine, we have to change the encoded value of a letter each time we type a letter. The principle is to have a cipher that can encode a letter into different values. This can be achieved in theory by using a secret key encryption. The purpose of this system is to apply a reversible operation between the text we want to encode and the secret key. In that way, the cipher text cannot be decrypted without the secret key. A simple addition can be enough because given C, we can't find A and B like A+B = C. Example :

We can't know A and B in $A + B = 27$ but if we know B, we can calculate A : $A + 5 = 27$ we can calculate $A = 22$

To have a valid encryption process using this kind of encoding, we must have a one-time usage random secret key with a length that match the text we encode. In the real world, we can light-up 2 problems : - The length of the key for a long message - The key have to be known only by encrypter and decrypter A solution to encrypt short messages is to have a long list of secret key defined secretly between both side of the exchange.

3.2 Mechanical configuration

The Enigma machine was trying to imitate the perfect system. Each time a letter is typed, the mechanical parts changed the electrical circuit in order to change the encryption result of the same letter. The starting configuration of the machina can be interpreted as the secret key. Despite the machina use simple components, its cipher is very strong. In this part, we will see how those simple parts can introduce a complex encoding process. Accordint to [3], the enigma machine used during the World War II can contain 3 whells. The army had only 5 different wheels. So placing 3 wheel in the machina can be interpreted by a permutation.

$$\frac{5!]}{(5-3)!} = 5 * 4 * 3 = 60$$

Each wheel have 26 letter that correspond to the 26 distinct starting placement. This configuration implies a lot of possibilities :

$$26 * 26 * 26 = 17576$$

Each time we press a button, the 1st rotor make a 1/26 rotation. But when the rotor reach a definied position, the second rotor make a 1/26 rotation too. Likewise, the second rotor make the third rotate. The point in wich the first and the second rotor entrains the next rotor can be configured too. For each of this wheel, you can choose one of the 26 different position. Because of this new configuration, you can have a lot of different combination :

$$26 * 26 = 676$$

The switchboard 3.1 is the last possible configuration for the machina. This board permit the user to switch the normal way a letter follow. for example, if you put a wire between A an B, B will be encoded as it is A and vice-versa. According to [8] the number of configuration's possibilities is given by "the number of ways of choosing m pairs out of n objects" wich is equivalent to :

$$\frac{n!}{((n-2m)! * m! * 2^m)}$$

In our case, the Enigma machine was used with 10 wires. the number of different possible configuration is :

$$\frac{26!}{((26-2*10)! * 10! * 2^{10})} = 150,738,274,937,250$$

We can now calculate the number of different starting configurations of this system :

$$60 * 17576 * 676 * 150,738,274,937,250 = 1,07 * 10^{23}$$

In that way, in order to decipher the message a german soldier recieved, he only have to type the encoded message to view the real message on its machina. It only works if the reciever have the same initial configuration.
There is also some discuss about the number of possibilities we can configure the system :

- The fact that we can change the time when the 1st rotor make the second move should not really relevant for a crypto system because this is redundant. So, by convention, the 676 factor is not taken in consideration.

- Sometimes, the configuration specify that some switchboard wires have not to be used. This introduce new possibilities.

This large nomber of starting configuration give the enigma a large number of large private keys according to the perfect crypto system. In order to select the correct key, each side of the communication must have a sheet specifying the dayly configuration.

3.3 How to use it

During the World War II, the german army definied a protocol to use this machina. Both of the side of the conversation was given a secret sheet 3.2 each month. This piece of paper contained for each day the precise configuration to encrypt the message. This paper must remains secret because knowing the starting configuration and the protocol is enough to decrypt a ciphered

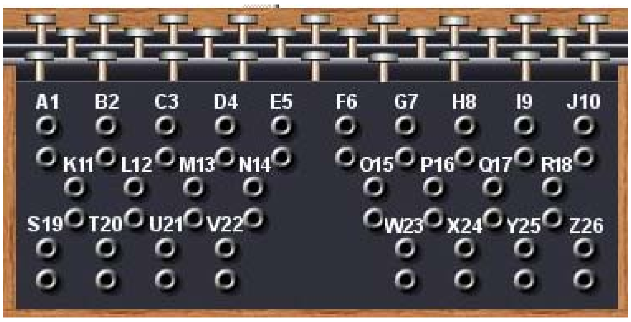
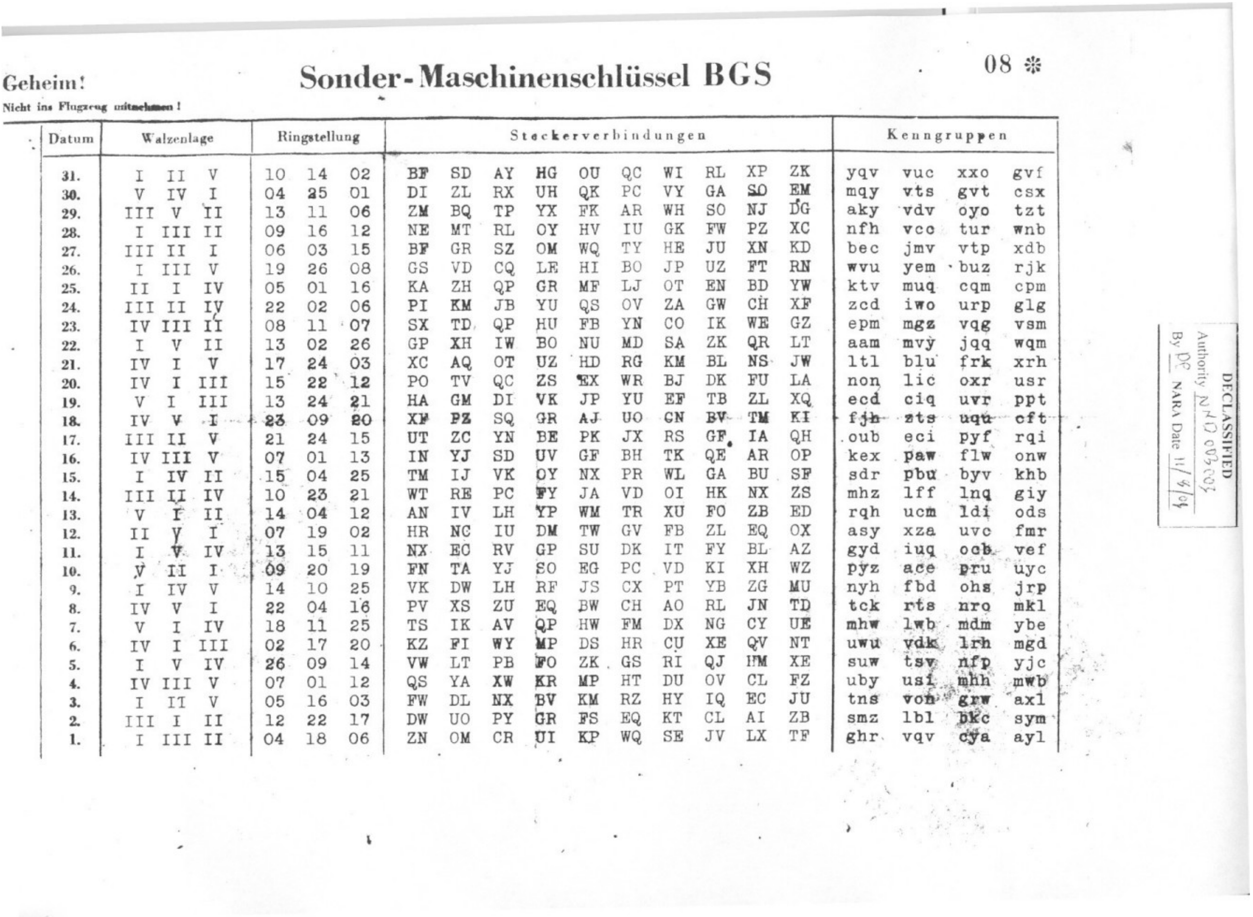


Figure 3.1: Picture of the Enigma's switchboard

message. According to [3], this secret sheet was written with soluble ink in order to destroy the information quickly if an operator was in danger. Even if the enemy got one of this sheet, the decryption of all communication was very limited : there can only decrypt the messages of the service using the obtained sheet and only for a month. Indeed, for each different type of service, a sheet was edited. For example, Uboat had one secret sheet for communication different than the one used in the Luftwaffe in the month.



Geheim!

Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGS

08 ❊

Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
31.	I	II	V	10	14	02	BF	SD	AY	HG	OU	QC	WI	RL	XP	ZK	yqv	vuc	xxo	gvf
30.	V	IV	I	04	25	01	DI	ZL	RX	UH	QK	PC	VY	GA	SO	EM	mqy	vts	gvt	csx
29.	III	V	II	13	11	06	ZM	BQ	TP	YX	FK	AR	WH	SO	NJ	DG	aky	vdv	oyo	tzt
28.	I	III	II	09	16	12	NE	MT	RL	OY	HV	IU	GK	FW	PZ	XC	nfh	vco	tur	wnb
27.	III	II	I	06	03	15	BF	GR	SZ	OM	WQ	TY	HE	JU	XN	KD	bec	jmv	vtp	xdb
26.	I	III	V	19	26	08	GS	VD	CQ	LE	HI	BO	JP	UZ	FT	RN	wvu	yem	buz	rjk
25.	II	I	IV	05	01	16	KA	ZH	QP	GR	MF	LJ	OT	EN	BD	YW	ktv	muq	cqm	cpm
24.	III	II	IV	22	02	06	PI	KM	JB	YU	QS	OV	ZA	GW	CH	XF	zcd	iwo	urp	glg
23.	IV	III	II	08	11	07	SX	TD	QP	HU	FB	YN	CO	IK	WE	GZ	epm	mgz	vqg	vsm
22.	I	V	II	13	02	26	GP	XH	IW	BO	NU	MD	SA	ZK	QR	LT	aam	mvy	jqq	wqm
21.	IV	I	V	17	24	03	XC	AQ	OT	UZ	HD	RG	KM	BL	NS	JW	ltl	blu	frk	xrh
20.	IV	I	III	15	22	12	PO	TV	QC	ZS	EX	WR	BJ	DK	FU	LA	non	lic	oxr	usr
19.	V	I	III	13	24	21	HA	GM	DI	VK	JP	YU	EF	TB	ZL	XQ	ecd	ciq	uvr	ppt
18.	IV	V	I	23	09	20	XF	PZ	SQ	GR	AJ	UO	CN	BV	TM	KI	fjh	zts	uqu	cft
17.	III	II	V	21	24	15	UT	ZC	YN	BE	PK	JX	RS	GF	IA	QH	oub	eci	pyf	rqi
16.	IV	III	V	07	01	13	IN	YJ	SD	UV	GF	BH	TK	QE	AR	OP	kex	paw	flw	onw
15.	I	IV	II	15	04	25	TM	IJ	VK	OY	NX	PR	WL	GA	BU	SF	sdr	pbu	byv	khb
14.	III	II	IV	10	23	21	WT	RE	PC	FY	JA	VD	OI	HK	NX	ZS	mhz	lff	lnq	giy
13.	V	I	II	14	04	12	AN	IV	LH	YP	WM	TR	XU	FO	ZB	ED	rqh	ucm	ldi	ods
12.	II	V	I	07	19	02	HR	NC	IU	DM	TW	GV	FB	ZL	EQ	OX	asy	xza	uvc	fmr
11.	I	V	IV	13	15	11	NX	EC	RV	GP	SU	DK	IT	FY	BL	AZ	gyd	iuq	ocb	vef
10.	V	II	I	09	20	19	FN	TA	YJ	SO	EG	PC	VD	KI	XH	WZ	pyz	ace	pru	uyc
9.	I	IV	V	14	10	25	VK	DW	LH	RF	JS	CX	PT	YB	ZG	MU	nyh	fbd	ohs	jrp
8.	IV	V	I	22	04	16	PV	XS	ZU	EQ	BW	CH	AO	RL	JN	TD	tck	rts	nro	mkl
7.	V	I	IV	18	11	25	TS	IK	AV	QP	HW	FM	DX	NG	CY	UE	mhw	lwb	mdm	ybe
6.	IV	I	III	02	17	20	KZ	FI	WY	MP	DS	HR	CU	XE	QV	NT	uwu	vdk	lrh	mgd
5.	I	V	IV	26	09	14	VW	LT	PB	FO	ZK	GS	RI	QJ	HM	XE	suw	tsv	nfp	yjc
4.	IV	III	V	07	01	12	QS	YA	XW	KR	MP	HT	DU	OV	CL	FZ	uby	usi	mhh	mwb
3.	I	II	V	05	16	03	FW	DL	NX	BV	KM	RZ	HY	IQ	EC	JU	tns	von	grw	axl
2.	III	I	II	12	22	17	DW	UO	PY	GR	FS	EQ	KT	CL	AI	ZB	smz	lbl	bkc	sym
1.	I	III	II	04	18	06	ZN	OM	CR	UI	KP	WQ	SE	JV	LX	TF	ghr	vqv	cya	ayl

DECLASSIFIED
Authority NND 003003
By DC NARA Date 11/4/04

Figure 3.2: One of the secret sheet, source : [7]

Despite of the secret key length, the key had to be changed after each message. Indeed, after typing 26 ∗ 26 ∗ 26 = 17576 letters, the machina return to its starting position. In order to do this, each message is send with the associed starting position called "message key" or "Spruchschlüssel". This key is encrypted using a random choosed start porition "Grundstellung".

In order to verify the date of the message (because sometimes, messages are send with delay),

each message started with a 5 letter code that was not encoded. The 1st two letters are randomly choosen by the sender and the 3 following letters are one of the 4 "Kenngruppen" available each day.
If a message is long, it can be divided into several parts that are encoded using different starting positions.

```
1230 = 3tle = 1tl = 250 = WZA UHL =

FDJKM LDAHH YEOEF PTWYB LENDP
MKOXL DFAMU DWIJD XRJZY DFRIO
MFTEV KTGUY DDZED TPOQX FDRIU
CCBFM MQWYE FIPUL WSXHG YHJZE
AOFDU FUTEC VVBDP OLZLG DEJTI
HGYER DCXCV BHSEE TTKJK XAAQU
GTTUO FCXZH IDREF TGHSZ DERFG
EDZZS ERDET RFGTT RREOM MJMED
EDDER FTGRE UUHKD DLEFG FGREZ
ZZSEU YYRGD EDFED HJUIK FXNVB
```

Listing 3.1: Encrypted message example, source : [7]

If we analyse this message, we can see on the 1st line ordered : the hour of the message $1230- > 12h30$, the number of parts in the message $3tle- > 3teile- > 3parts$, the number of the current part $1tl- > ersteteil- > 1stpart$, the length of the part 250, the "Grundstellung" WZA and the message key encoded using WZA as starting position UHL.
The message itself starts with the "Buchstabenkenngruppe" (first 5 letters) $FDJKM$ composed by a random couple of letter FD and the choosen "Kenngruppe" identifying the day the message was sent JKM.

In order to decrypt the message, the operator have to set up the machine configuration as the sender according to the configuration sheet. After decrypting the message key and setting up the starting position as the message key recieved, the decryption process was very simple. Indeed, because of the reflector (the last part of the electrical circuit), an encrypted letter typed on a enigma configured similarly will be reencrypted in its original form. A modelisation of the reflector can be 3.3 for 6 letters.

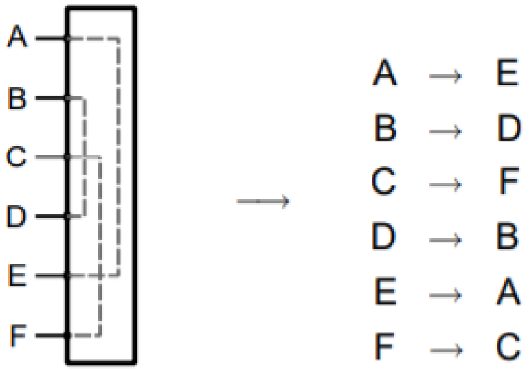


Figure 3.3: Reflector modelisation, source : [6]

This can also be modelized by an involution function. It seems that the permutation function and its inverse are identical :

$$(f(A) = E \Leftrightarrow f(E) = A)$$
$$(f(f(A)) = f(E) = A)$$
$$(f^{-1} = f)$$

Moreover, because the reflector's aim is to close the electrical circuit, a letter cannot be permutted with itself. We can infer that the reflector mathematical model have no fixed point.

$$f(A) \neq A$$

Because the marine played an important role during this war, their encryption protocol was a bit different and ever more complex.

3.4 Advantages and inconvenients

The principle of the enigma machine is known. What makes it effective is the large number of possible combinations of the machine's initial settings and the selection of the original message key.
With all of this different secret key, it's easy to avoid a key to be reused. And as we saw during the World War II, this amount of secret key can be used to encrypt messages from different services using differents ways. This separation is a real advantage car if a secret sheet was found by the enemy, they were only able to decrypt messages from the sheet's source.

The main problem with the enigma principle is easy to identify : how to transmit the monthly secret paper containing daily configurations to all operators ? During World War II, they were transmitted physically to avoid any leak.

An other problem (and the main key of the decryption process) is that all of the complexity comes from the switchboard. Moreover, the switchboard have a limited effect on the cipher process : 6 letters remains unchanged by it. So if we decrypt the text without taking care of the switchboard we will have a message with 6 types of letter correctly placed. After that, a simple logical analysis is enough by finding each permutation one by one.

3.5 Possible attacks

In order to decrypt a cipher encoded by the Enigma, it's very hard to try a classical statistic attack because of the number of possibles configurations. But because of the cyclic part of the machina, it can be possible to find a mathematical modelization of a part of the machina. The modelization includes every configurations parts except the switchboard. Because of this modelizaton it is possible to brute force the placement of the rotors.

Once this configuration obtained, the last thing left is the switchboard. We can so decode the message partially lefting maximum 10 permutations. In order to finish the decryption, we have to find some recognisable words and logically find the substitutions.

Because the enigma machine worked with permutations, and because its principle is based on a electrical circuit, it is impossible to encode a letter by itself (enigma have'nt any fixed point). This can be helpful in order to discover the association between a latter and its permutation by removing one of the 26 possibilities.

An other possible attack uses the coincidence counting. This is an indicator that provides a measure of how likely it is to draw two matching letters by randomly selecting two letters from a given text. It's usually usefull do decrypt natural-language plaintext.

We know that the IC is approximatively 0.038 for a random text and 0.072 for deutch. We can so try to modelize all enigma encoder without taking care of the switchboard and try to decrypt with each modelization the cipher text. For each partially decoded text (partially because the switchboard permute max 10 letter), we calculate the IC and if it's approximatively 0.038, we can think that the modelization is not correct.
Once the correct modelization of the wheels and the starting position found, like the other method, we can identifiate the 10 lefting permutations by highlighting recognizable words.

4 Conclusion

To conclude, enigma is a machine made up of a battery, 26 lamps corresponding to the 26 letters of the alphabet, 26 keyboard keys also corresponding to the letters, and many cables that connect the different components. Designed by the engineer Arthur Scherbius in 1923, the Enigma machine was marketed to anyone who wanted to keep their communications confidential, for example to industrial companies. After a bitter commercial failure, Scherbius decided in 1926 to sell the machine to the German army, without anticipating that it would be used by the Nazis.

the Enigma's operating principle is both simple and clever. Each time a letter is pressed, an electrical circuit is closed, and a light bulb is lit which corresponds to the coded letter. The circuit that is closed depends on the position of the rotors. Each time a letter is pressed, one or more of the moving rotors rotates, changing the substitution that will be made the next time the key is pressed. Moreover, the ciphering is reversible: if you had typed A you would have coded D, if you had typed D you would have coded A. Thus, if the German command and the submarine have the same starting setting, the submarine operator only has to type the coded message directly to get the clear message. So the Germans had issued code books in their services to update the machines every day at midnight with the initial position of the rotors. These code books were valid for one month.

Breaking the codes is like finding a secret setting consisting of a triplet of letters, denoted R, and 10 pairs of letters, denoted C. The setting changed every 24 hours, giving Polish mathematicians just as much time to find the setting. A complete enumeration is impossible even with a modern computer.

Thanks to information provided by the French secret service in 1931, three Polish mathematicians, Marian Rejewski, Jerzy Różycki and Henryk Zygalski, succeeded in breaking Enigma's codes. Their work was communicated to the English secret service in 1939, in the forest a few days before the Nazi tanks entered the country. The British were thus able to read German communications during the first six months of the war. Based on the work of the Poles, the team of English mathematician Alan Turing managed to break the new versions of Enigma and gave England a considerable advantage.

Bibliography

[1] collection aristophil. Enigma price. http://www.collections-aristophil.com/html/fiche.jsp?id=10036316&np=1&lng=fr&npp=20&ordre=2&aff=1&r=. 5

[2] Dcode. Histoire et principe d'ENIGMA, une machine à chiffrer et à déchiffrer. https://www.dcode.fr/chiffre-machine-enigma. 5

[3] Claire Ellis. Exploring the Enigma. https://plus.maths.org/content/exploring-enigma. 6, 8

[4] Enigmamuseum. Enigma price. https://enigmamuseum.com/for-sale/. 5

[5] Gérard GRANCHER. Histoire et principe d'ENIGMA, une machine à chiffrer et à déchiffrer. https://www.mathrice.fr/rencontres/mars.2002/enigma.pdf. 5

[6] JULIEN MILLI GUILLAUME MUNCH. Enigma et la seconde guerre mondiale. 2004. 9, 14

[7] Dirk Rijmenants. Enigma procedure. http://users.telenet.be/d.rijmenants/en/enigmaproc.htm. 8, 9, 14

[8] Tony Sale. Counting the Possible Plugboard Settings. http://www.codesandciphers.co.uk/enigma/steckercount.htm. 7

List of Figures