II. CLASSICAL ENCRYPTION

- Cryptography **?**, History
- Encryption techniques
  - Substitution
  - Transposition

CRYPTOGRAPHY ?

Cryptography is one of the disciplines aimed at **protecting messages** by ensuring their: **Confidentiality, Authenticity**, and **Integrity**, often relying on **secrets** or **keys**.

The word **cryptography** comes from the ancient Greek words: **kruptos**: "hidden or secret" and **graphein**: "to write"

"**Secret writing**"

HISTORY

- **Artisanal Age (Origins)**

Substitution and Permutation

  - Caesar cipher: letter shifting
  - Codebooks: double-entry dictionaries

- **Technical Age (Machines)**

Substitution and Permutation using electromechanical machines

  - Hagelin. Enigma.

- **Paradoxical Age (Algorithms)**

Asymmetric cryptography (use of public keys) without previously established secret conventions

  - RSA

TERMINOLOGY

Encryption: the transformation using a key of a plaintext message (called plaintext) into an incomprehensible message (called ciphertext).

Cipher: the use of substitution at the letter level for encryption;

Code: the use of substitution at the word or phrase level for encoding;

Encoding: replacing a word or phrase with another word, number, or symbol;

Cryptogram: encrypted message;

Cryptosystem: encryption algorithm;

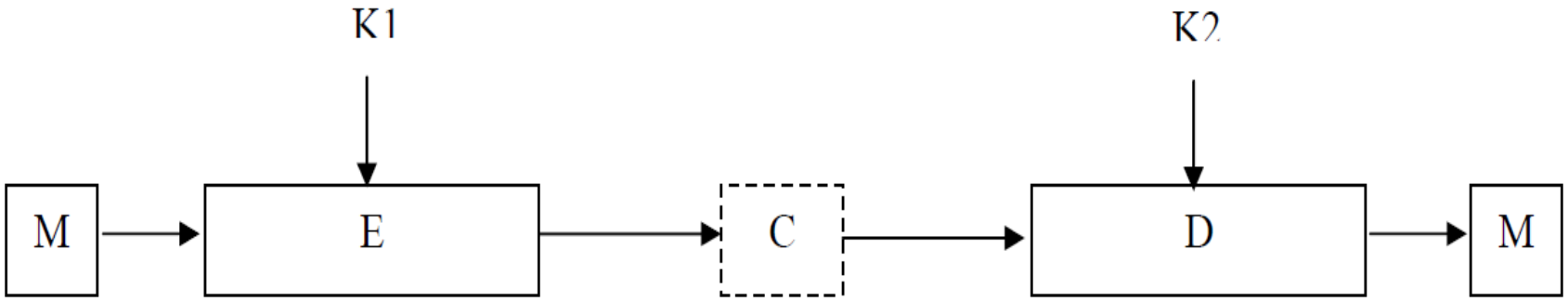
Decrypt: to retrieve the corresponding plaintext message for an encrypted message without possessing the decryption key;

Cryptography: The science aiming to create cryptograms;

Cryptanalysis: science analyzing cryptograms in order to decrypt them;

Cryptology: science encompassing cryptography and cryptanalysis.

FORMULATION



M: Plaintext message,
C: Ciphertext message,
E: Encryption function,
D: Decryption function,
K1: Encryption key,
K2: Decryption key,

E(M)=C (E transform M into C)
D(C)=M (D transform C into M)
D(E(M))=M

CLASSICAL CRYPTOGRAPHY

Classical cryptography manipulates characters

- **Substitution:** to replace characters

Word:	C	H	I	F	F	R	E
Position in the alphabet:	03	08	09	06	06	18	05

- **Transposition:** to Permute characters.

Key:	5	7	2	3	6	1	4			1	2	3	4	5	6	7
Word:	C	H	I	F	F	R	E	=		R	I	F	E	C	F	H

SUBSTITUTION

It consists of substituting in a message each of the letters of the alphabet with another (from the same alphabet or possibly from another alphabet).

TECHNIQUES:

- Simple substitution
- Homophonic substitution
- Polygram substitution
- Polyalphabetic substitution
- Tomographic substitution

SIMPLE SUBSTITUTION

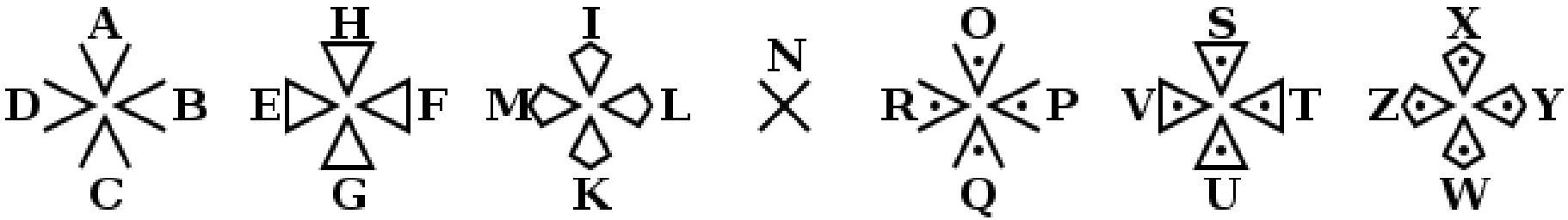
This involves replacing each letter of the plaintext alphabet with a conventional sign: a letter, group of letters, or number, with the same plaintext letter always represented by the same conventional sign

Letter	Replaced by	Or replaced by
D	O	12
I	Y	23
N	V	04
O	M	18
S	D	08
V	B	16

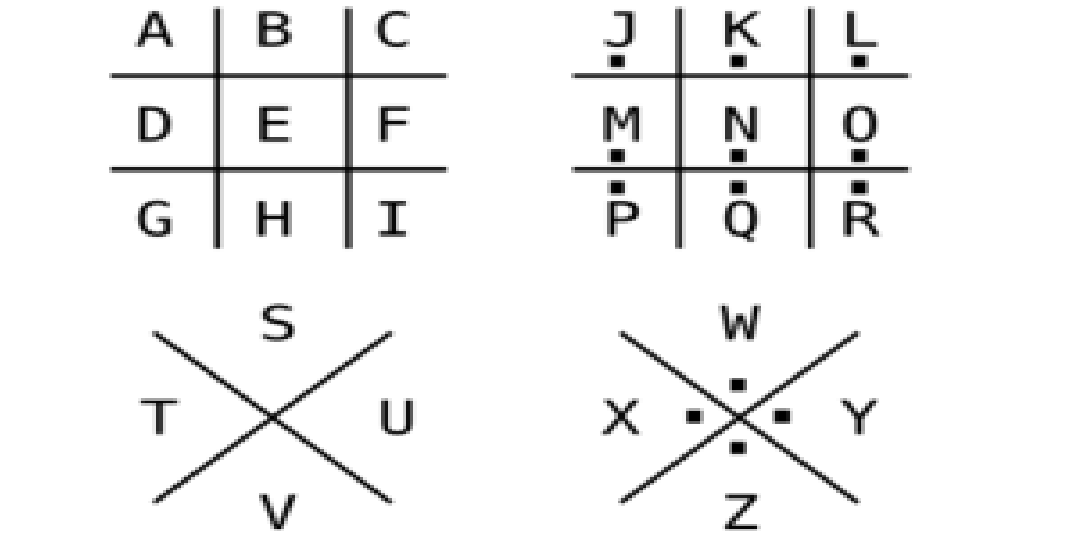
The word **DIVISION** will be ciphered into : **OYBYDYMV**

Examples: Templars, Pigpen, ATBASH, Polybius, Caesar

- **TEMPLARS**



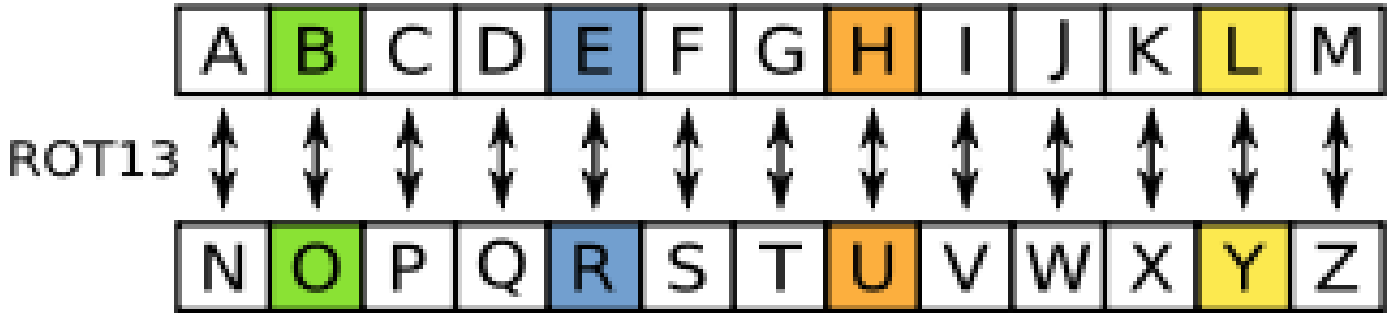
- **Pigpen**

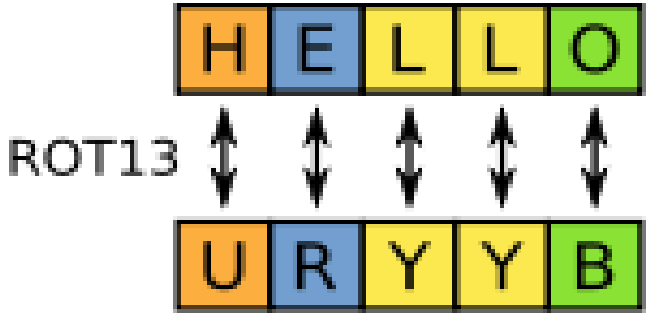


- **ATBASH**

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

- **ROT 13**





POLYBIUS SQUARE

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

HELLO

2315313134

It is possible to fill the table in several different ways, for example, by starting with filling it with a **keyword**, and then in alphabetical order.

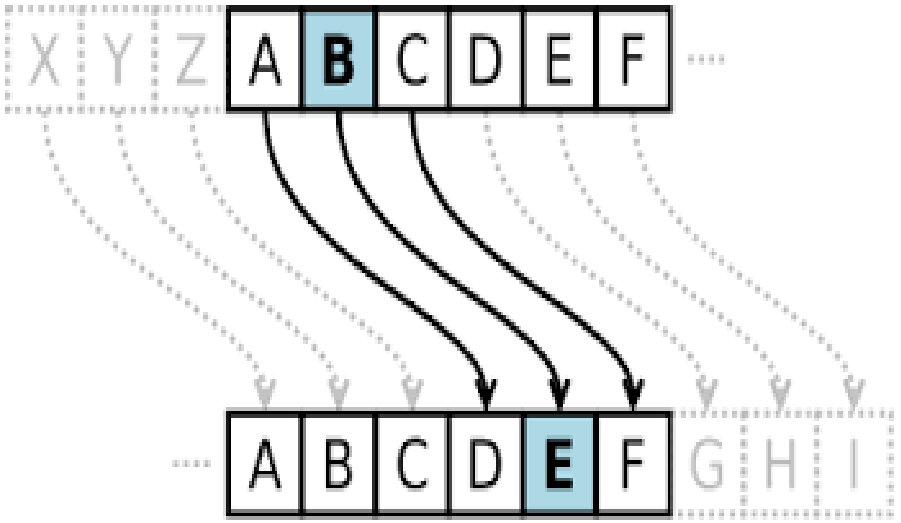
CAESAR Cipher

The Caesar cipher is one of the earliest cryptographic protocols. Indeed, to encrypt messages sent to his army, Caesar proceeded as follows:

- **Encryption:** Each character of the plaintext is replaced by the one found three positions further along in the alphabet. A is encrypted as D, B as E, etc.
- **For decryption,** the process is reversed. D becomes A, E becomes B, and so on.

Example:

Caesar sent the following message to his army:
DOHD MDFWD HVW



The decrypted message is:
ALEA JACTA EST

This means in English: **The die is cast**

- CAESAR Cipher (Formulation)

➢ Encryption:

The principle is to number the letters of the alphabet from 0 to 25 (A=0, B=1, ..., Z=25). Each letter of the alphabet is encrypted by the encryption function **E** which uses a shift **k**. The function **E** is defined as follows:

$$\mathbf{E_k : \{0,1,\ldots,25\} \rightarrow \{0,1,\ldots,25\}}$$

$$\mathbf{i \rightarrow (i+k) \bmod 26}$$

$$\mathbf{E_k(i)=(i+k) \bmod 26 \quad / \quad i \in \{0,1,\ldots,25\}}$$

For example, if we take k=3:

$E_3(0)=(0+3) \bmod 26 = 3 = D$

$E_3(1)=(1+3) \bmod 26 = 4 = E$

Example 1: Let's encrypt the word "**ATTACK**" with **k=3**.

- CAESAR Cipher (Formulation)

➢ Decryption:

The decryption is defined by the function **D**, which uses an inverse shift with the **k** positions defined by the encryption function. The function **D** is defined as follows:

$$D_k : \{0,1,\ldots,25\} \rightarrow \{0,1,\ldots,25\}$$
$$i \rightarrow (i-k) \bmod 26$$

$$D_k(i)=(i-k) \bmod 26 \; / \; i \in \{0,1,\ldots,25\}$$

If 1 was encrypted to 4, then $D_3(4) = 4 - 3 = 1$.

Example 2: Let's decrypt the message "**WURMDQ KRUVH**" with k=3.

Mathematically, we say that D_k is the inverse bijection of E_k: For all $i \in \{0,1,\ldots,25\}$: $D_k(E_k(i)) = i$

HOMOPHONIC SUBSTITUTION

It is like a simple substitution cipher, except that for one character of the plaintext, we do correspond several characters in the ciphertext.
For example, the character '**a**' corresponds to the following characters: **2, 13, 45, or 22**

POLYGRAM SUBSTITUTION

The polygram substitution is a cipher in which characters are encrypted in blocks.
For example, '**aba**' can be encrypted as '**rtq**' while '**abb**' is encrypted as '**sll**'

POLYGRAM SUBSTITUTION

Bigram substitution (groups of 2 characters)
Proceeds from the same principle as simple substitution. But instead of encrypting each letter of the plaintext separately, we do encrypt groups of two letters or bigrams

For example, the plaintext "**Colonne ennemie**" is encrypted into:

Co	lo	nn	ee	nn	em	ie
OP	LN	VK	ST	VK	LI	RE

BIGRAM SUBSTITUTION

a)- Using a table – Playfair Cipher

Introduced in 1854 by the English scholars L. Playfair and C. Wheatstone, it illustrates the concept of polygram ciphering:

- We use the Playfair alphabetical square, which consists of five letters in width and five letters in height.
- The keyword is written horizontally without repeating any letters, and then the remaining letters are written following their alphabetical order.
- Both I and J are treated as a single letter

Playfair Cipher (Example)

If we take the keyword: **SPART**, the alphabetical square is as follows:

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

The letters in each pair can only have three states. They occupy:

1.The same row: Each letter is replaced by the one to its right.
Example: **E D** is replaced by **F E** or **T R** by **S T**

2.The same column: Each letter is replaced by the one below it.
Example: **R Q** is replaced by **E Y** or **Q Y** by **Y R**.

3.Neither of the above: Each letter is replaced by the letter found at the intersection of its row and the column of the other letter, respecting the order of the pairs.
Example: **A H** becomes **P IJ** or **S Z** becomes **T V**.

Since **I** and **J** are considered the same letter, a transformation into **IJ** can be transcribed as either **I** or **J**, at the discretion of the cipherer.

Playfair Cipher (Example)

Example: We want to encrypt the text "**RENDEZ VOUS A PARIS**" with the key **SPART**

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

Playfair Cipher (Example)

Example: We want to encrypt the text "**RENDEZ VOUS A PARIS**" with the key **SPART**

- **Step 1 : RE ND EZ VO US AP AR IS**
- **Step 2 : Encrypt the pairs**

RE = EK

ND = OC

EZ = FY

VO = XM

US = MT

AP = RA

AR = RT

IS = GA

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

Ciphertext: EKOCFYXMMTRARTGA

b)- Using a Mathematical Transformation – Hill Cipher

Encryption:

(1): Replace each letter with its position in the alphabet: **A** becomes **0**, **B** becomes **1**,..., **Z** becomes **25**.

(2): Group the resulting numbers by **m** (let's take **m=2** for example).

(3): For each block of **m** numbers to be encoded ($\mathbf{x_1x_2...x_m}$), we calculate the encoded text by performing linear combinations using an encryption key (which depends on **m**).

(4): To obtain the encrypted letters ($\mathbf{y_1y_2...y_m}$), we calculate the **remainders modulo 26** of the linear combinations using the following formula:

$$\begin{pmatrix} y_i \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_i \\ x_{i+1} \end{pmatrix} \quad mod\ 26$$

For example, for the first two letters $\mathbf{x_1x_2}$, we will have:

$\mathbf{Y_1=(ax_1+bx_2)\ mod\ 26}$

$\mathbf{Y_2=(cx_1+dx_2)\ mod\ 26}$

Note: The choice of the key corresponds to choosing a number **m** and the choice of **linear combinations** to perform.

Example: Encrypt the word **ELECTION** using **Hill**, with **m=2, a=3, b=5, c=1 and d=2**.

Step 1: We divide the word into blocks of 2 letters: **EL | EC | TI | ON**.
Step 2: We replace the letters with their associated order: **4-11 | 4-2 | 19-8 | 14-13.**
Step 3: We perform linear combinations for each block. For example, for the first block, where x_1=4 and x_2=11, we have:

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \ \boldsymbol{mod\ 26} = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 4 \\ 11 \end{pmatrix} \boldsymbol{mod\ 26} \rightarrow \begin{pmatrix} y_1 = 3\times4+5\times11=67 \\ y_2 = 1\times4+2\times11=26 \end{pmatrix} \boldsymbol{mod\ 26} \rightarrow \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 67 \\ 26 \end{pmatrix} \boldsymbol{mod\ 26} \rightarrow \begin{pmatrix} 15 \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} P \\ A \end{pmatrix}$$

With the same way, y_3=22, y_4=8, y_5=97, y_6=35, y_7=107, y_8=40.
Respectively, the modulos are (15, 0, 22, 8, 19, 9, 3, 14).

Etape 4 : We convert back to letters to find **PAWITJDO**.

LETTERS	E	L	E	C	T	I	O	N
X_i positions	4	11	4	2	19	8	14	13
Y_i positions	15	0	22	8	19	9	3	14
Encrypted letters	P	A	W	I	T	J	D	O

Decryption

To decipher, the principle is the same as for encryption: we take the letters two by two, then multiply them by the inverse of the encryption matrix.

$$\begin{pmatrix} x_i \\ x_{i+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} y_i \\ y_{i+1} \end{pmatrix} \quad mod\ 26$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Example : Decrypt the word previously encrypted PAWITDJO.

Step 1 : Divide the word into blocks of 2 letters : PA | WI | TJ | DO.

Step 2 : Replace letters with their associated positions: 15-0 | 22-8 | 19-9 | 3-14.

Step 3 : Calculate the decryption matrix (mod 26)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} mod\ 26 = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}^{-1} mod\ 26 = \frac{1}{3.2 - 5.1}\begin{pmatrix} 2 & -5 \\ -1 & 3 \end{pmatrix} mod\ 26 = \frac{1}{1}\begin{pmatrix} 2 & -5 \\ -1 & 3 \end{pmatrix} mod\ 26$$

Then:

$$\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}^{-1} mod\ 26 = \begin{pmatrix} 2 & -5 \\ -1 & 3 \end{pmatrix} mod\ 26 = \begin{pmatrix} 2 & 21 \\ 25 & 3 \end{pmatrix}$$

Step 4: We perform linear combinations for every block: 15-0 | 22-8 | 19-9 | 3-14

$$x_1 = (2 \times 15 + 21 \times 0) \bmod 26 = 30 \bmod 26 = 4$$
$$x_2 = (25 \times 15 + 3 \times 0) \bmod 26 = 375 \bmod 26 = 11$$

$$x_3 = (2 \times 22 + 21 \times 8) \bmod 26 = 212 \bmod 26 = 4$$
$$x_4 = (25 \times 22 + 3 \times 8) \bmod 26 = 574 \bmod 26 = 2$$

$$x_5 = (2 \times 19 + 21 \times 9) \bmod 26 = 227 \bmod 26 = 19$$
$$x_6 = (25 \times 19 + 3 \times 9) \bmod 26 = 502 \bmod 26 = 8$$

$$x_7 = (2 \times 3 + 21 \times 14) \bmod 26 = 300 \bmod 26 = 14$$
$$x_8 = (25 \times 3 + 3 \times 14) \bmod 26 = 117 \bmod 26 = 13$$

4 11 4 2 19 8 14 13 = ELECTION

POLY-ALPHABETIC SUBSTITUTION

WITH MULTIPLE ALPHABETS

- Using multiple "alphabets," which means that the same letter can be replaced by several symbols

Examples :

Bellaso/Porta,
Alberti’s Disk,
Vigenère,
Beaufort,
Gronsfeld,
Jefferson’s Cylinder,
Enigma.

A – Disk of ALBERTI

Alberti proposes the use of two concentric disks:

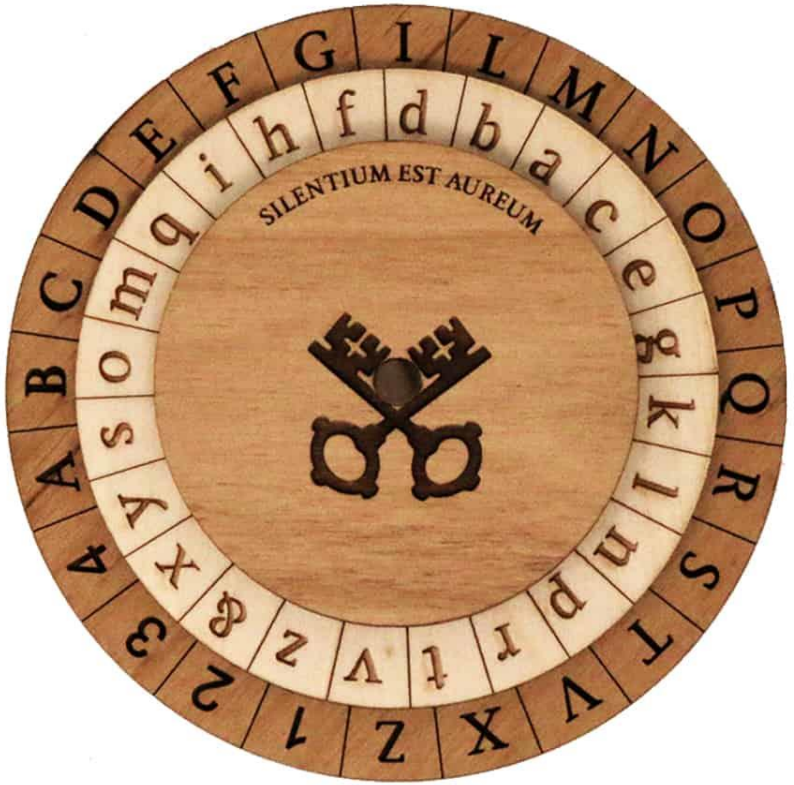
- **A large disk:** fixed, where the alphabet is written in the correct order.
- **A smaller disk:** movable, where the alphabet is written, but in any order.

Principle:

(1) First, you need to start by adjusting the two disks so that the A's coincide.

(1) For each letter of the plaintext message, look for the letter on the large disk; the encrypted letter is the one read opposite it on the small disk.

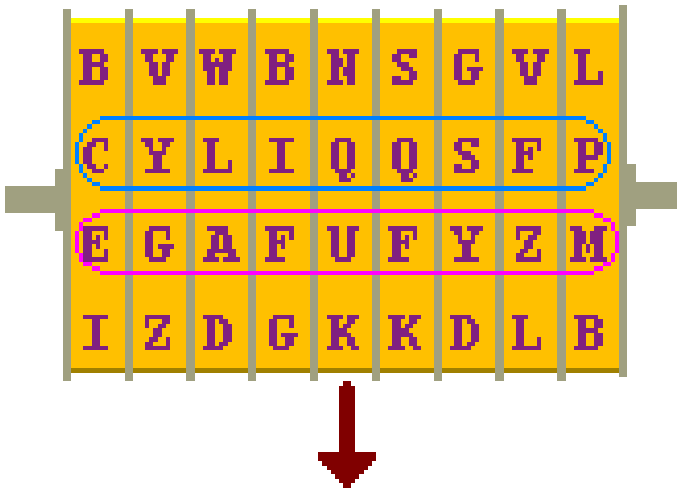
(1) To complicate matters, Alberti suggests periodically rotating (for example, every 4 letters) the small disk by one character.



B - Jefferson Cylinder

The Jefferson Cylinder consists of a series of 25 or 26 wheels, nested along a fixed axis, and able to rotate independently of each other around this axis. On each wheel, one can find the 26 letters of the alphabet, but written in any order.

Principle: to encode the word CYLINDER, we rotate the wheels to display this word on a line in front of our eyes. Then we choose another line, for example, the one just below it, and send the series of letters found there.



We do encrypt the word: **CYLINDER**

We compose it horizontally by rotating the wheels,

The encrypted word is read just below: **EGAF…**

C - Saint-Cyr Slide Rule

A calculating rule, with a fixed part, the stator, and a movable part, the slider. The alphabet is written on the stator, and on the slider, you find the alphabet twice.

To encrypt a letter, one adjusts the slider so that under the **A** on the stator is the letter of the **key**. Beneath the letter of the plaintext message written on the stator, one finds the letter of the encrypted message.

If we want to encrypt the letter **N**, with the key letter being **O**, we align this **O** under the **A**. Beneath the **N**, we read the encrypted letter as **B**.

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

D- BELLASO/PORTA

Introduced by G. D. Porta in 1563 (Origin: BELLASO in 1553)

The **left column** represents the **key letter** used. The **right column** corresponds to the corresponding **substitution alphabet**.

The first letter of the plaintext message is **R**, and the corresponding key letter is **B**. In the line corresponding to the key **B** (the first one), we see that **R** is matched with **E**. Therefore, we replace **R** with **E**.

Example: Plaintext = REVE DE PRINTEMPS Key = BIBMATH

Plaintext	R	E	V	E	D	E	P	R	I	N	T	E	M	P	S
Key	B	I	B	M	A	T	H	B	I	B	M	A	T	H	B
Ciphertext	E	N	I	Y	Q	V	F	E	R	A	M	R	Q	F	F

Ciphertext = ENIYQVFERAMRQFF

Note: if A is encrypted as N, it means that N is encrypted as A. Therefore, the algorithm to decrypt is exactly identical to the algorithm to encrypt

E- Vigenère

- Encryption using a repeated key.
- For each character, we use a letter from the key to perform the substitution.
- The indispensable tool for the Vigenère cipher is the "Vigenère table".

	A	B	C	D	E	etc.
A	a	b	c	d	e	...
B	b	c	d	e	f	...
etc.	c	d	e	f	g	...

Let's encrypt the text: **Keep calm and stay positive**

With the key: **Smart**

Plaintext : `KEEP CALM AND STAY POSITIVE`

Key : `SMAR TSMA RTS MART SMARTSMA`

Ciphertext: `CQEG VSXM RGV ETRR HASZMAHE`

Vigenère Square

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

E- Vigenère

Mathematically,

- Identify the letters of the alphabet with numbers from 0 to 25 (A=0, B=1...).
- The encryption and decryption operations are, for each letter, those of the Caesar cipher. By designating:
- The i^{th} letter of the plaintext as **Text[i]**, The i^{th} letter of the ciphertext as **Cipher[i]**, The i^{th} letter of the key, repeated enough times, as **Key[i]**, It is formalized as:
  - **Cipher[i] = (Text[i] + Key[i]) modulo 26**
  - **Text[i] = (Cipher[i] - Key[i]) modulo 26**

F-Enigma Machine (1919)

Principle: each letter is replaced by another (substitution). The substitution changes from one letter to another.

F-Enigma Machine

- With each character, the rotors rotate incrementally: the 1st rotor turns by one notch with each character (to be encrypted).

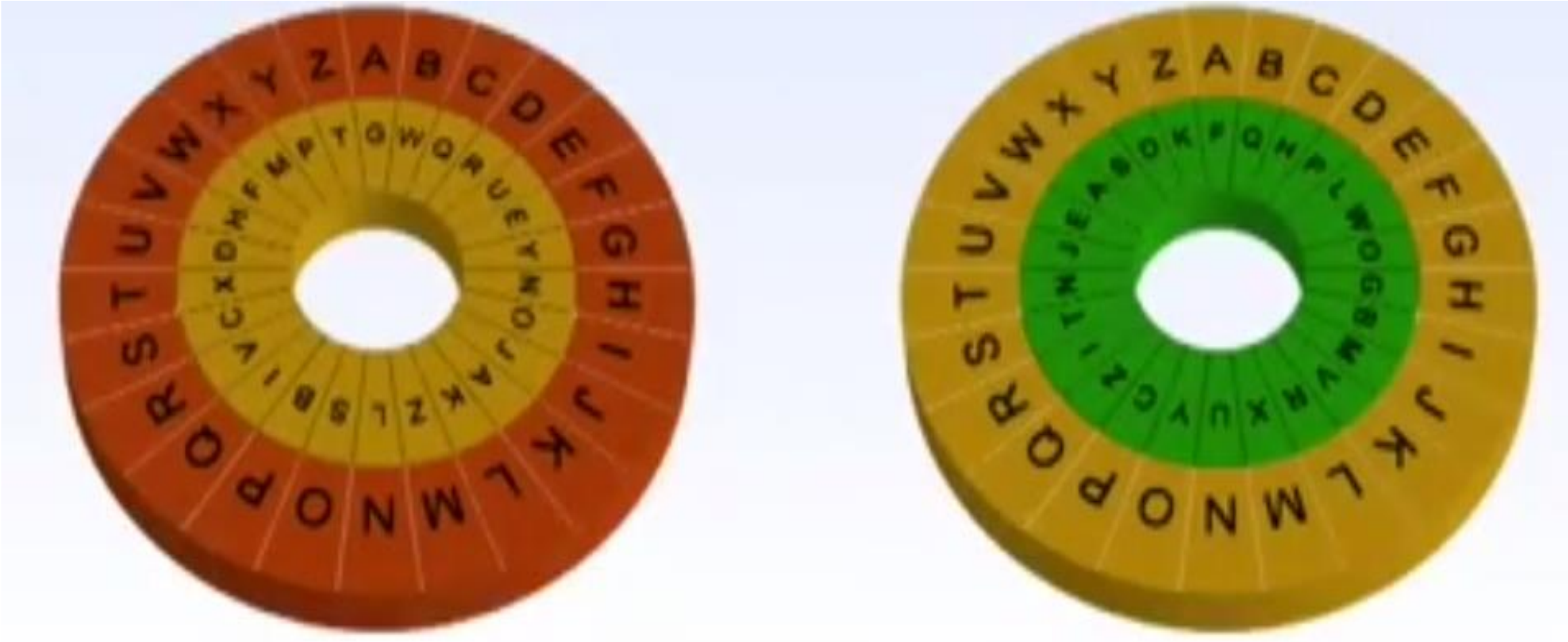
- After encrypting 26 letters, i.e., one full rotation, it advances the 2nd rotor by one notch; then it starts over (26 letters).

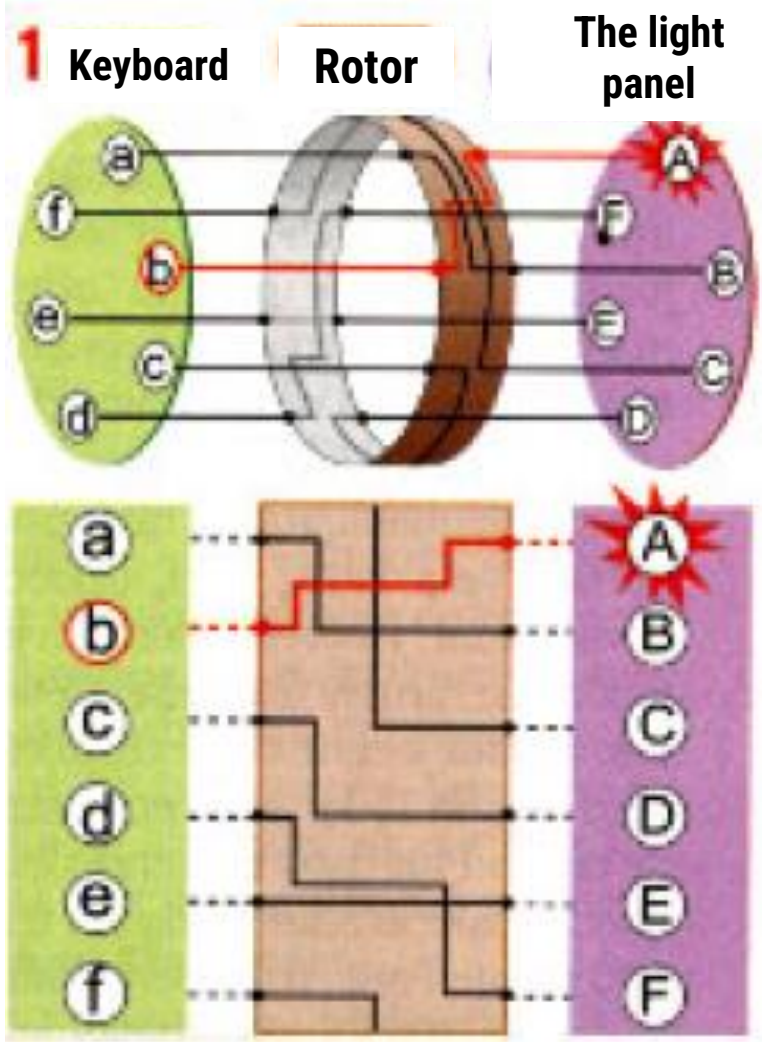
Example : 2 rotors

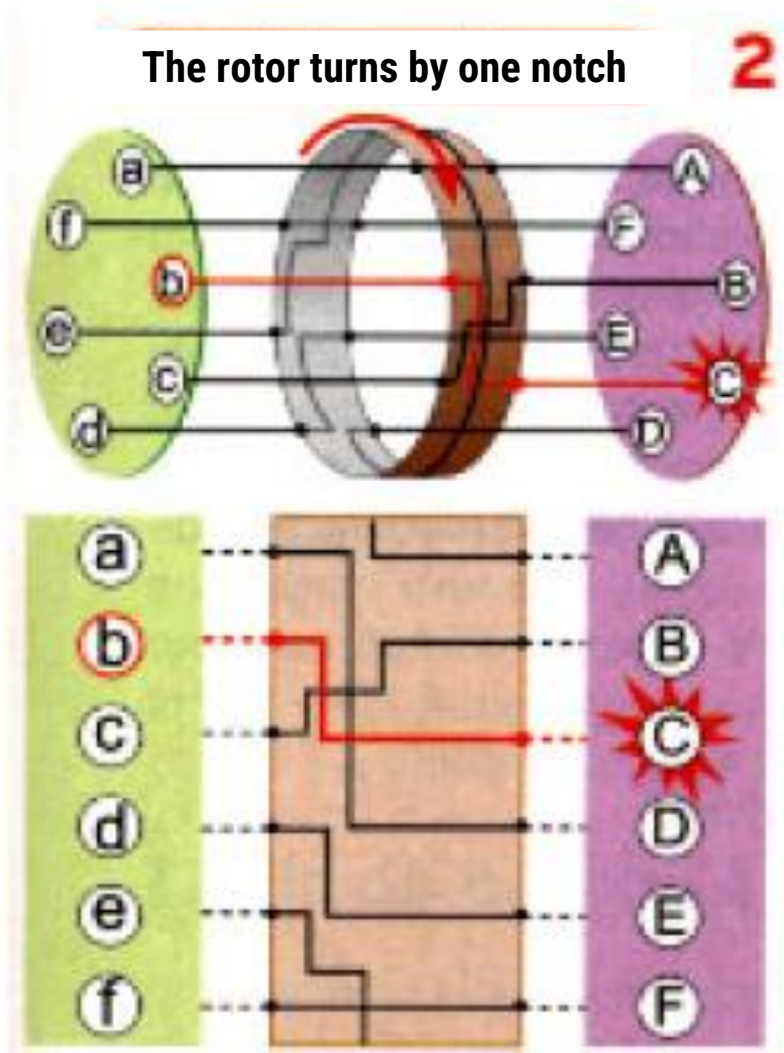
The key is: knowing the chosen rotors (in order), the initial position of each of them, and the configuration of the plugboard connections.

F-Enigma Machine

Example : 3 rotors




1
Keyboard
Rotor
The light panel
a
f
b
e
c
d
A
F
B
E
C
D


The rotor turns by one notch
2
a
f
b
c
c
d
A
F
B
E
C
D

G - Exclusive OR (XORing): This algorithm is extremely simple and is used in a wide range of commercial applications such as Microsoft Word.

- The principle is that the encryption function is identical to the decryption function, using the same key
- (M: the plaintext, C: the encrypted text, K: the key)

$$M \oplus K = C$$

$$C \oplus K = M$$

XOR Table: either one or the other but not both at the same time :

0 (Xor) 0 = 0

0 (Xor) 1 = 1

1 (Xor) 0 = 1

1 (Xor) 1 = 0

G - Exclusive OR (XORing):

Example: $\mathbf{M}$ = 'Le petit prince', $\mathbf{k}$ = 'cS'

$\mathbf{C} = \mathbf{M}$ (Xor) $\mathbf{k}$

$\mathbf{C}$ = 'Le Petit Prince'

(Xor) 'cScScScScScScSc'

$\mathbf{C}$ = '/6C-'-'C-- :-0-'

'L' = $76_{(10)}$ = $0100\ 1100_{(2)}$

'c' = $99_{(10)}$ = $0110\ 0011_{(2)}$

'L' (Xor) 'c' = $0010\ 1111_{(2)} = 47_{(10)}$ = '/'

The time it takes to break this algorithm depends on the ratio:
"size of the message / size of the key": the larger it is, the easier the task will be

TRANSPOSITION

The characters of the plaintext remain unchanged, but their respective positions are modified.

TYPES:

- Simple Transposition
- Zigzag Transposition
- Matrix-based Transposition
- Fixed-width Columnar Transposition
- Grid Transposition ...

SIMPLE TRANSPOSITION

Change the order of the letters by applying a simple permutation between them.

Example: permutation (2, 4, 1, 3) consists of:

(1) swapping the 1st letter with the 2nd, the 2nd with the 4th, the 3rd with the 1st, and the 4th with the 3rd.

(2) repeating the same process with the next groups of four letters.

Plaintext: TRANSPOSITION

Ciphertext: RNTAPSSOTOIIN

ZIGZAG TRANSPOSITION (Rail Fence)

- Write a message on two lines or more depending on the number of levels (one letter on one line and the next on another).
- Then write the different lines obtained one after the other in sequence.

Example: Rail fence of two levels

Plaintext: THE GRASS IS ALWAYS GREENER ON THE OTHER SIDE OF TE FENCE

T E R S I A W Y G E N R N H O H R I E F H F N E
H G A S S L A S R E E O T E T E S D O T E E C

Ciphertext: TERSIAWYGENRNHOHRIEFHFNE HGASSLASREEOTETESDOTEEC

MATRIX-BASED TRANSPOSITION

The key is the matrix: meaning we know the dimension of the matrix (e.g., **matrix (5, 6)**).

Encryption:

(1) The plaintext message is written into a matrix (row-wise);
(2) Read the matrix column by column.

Decryption:

(1) The encrypted message is written into a matrix (column-wise);
(2) Read the matrix row by row.

Example :

Key: matrix(5,6)

M	E	S	S	A	G
E		S	E	C	R
E	T		A		T
R	A	N	S	P	O
S	E	R			

Plaintext: MESSAGE SECRET A TRANSPOSER

Ciphertext: MEERSE TAESS NRSEAS AC P GRTO

GRID TRANSPOSITION

A grid (in the form of a square or a rectangle) divided into a certain number of cells. Some of these cells are called grid **windows**. They are used for writing the plaintext.

Example :
Plaintext: **"MESSAGE URGENT"**

D	M	I	E	O	S	A	W
D	S	P	E	A	S	G	C
M	E	J	U	L	U	R	H
G	A	E	N	F	W	T	N

Ciphertext: **DMIEOSAWDSPEASGCMEJULURHGAENFWTN**

The decryption: involves applying the encrypted text onto a table equal to the grid, and reading the plaintext through the windows.

OVER-ENCRYPTION

Multiple-Encryption

Consists of applying successively two or more encryption algorithms to the plaintext.

- Delastelle
- ADFGVX
- Bazeries
- Nihilistes

DELASTELLE CIPHER

It is a mixture of substitution and transposition encryption:
(1): Group the letters of the message to be encrypted 5/5,
(2): Use the Polybius square and write vertically for each letter the position in the table.

Example:

Plaintext: DELASTELLE

(a) Substitution : Using Polybius square:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

The group of the 5 first letters:

D	E	L	A	S
1	1	3	1	4
4	5	1	1	3

The group of the 5 following letters:

T	E	L	L	E
4	1	3	3	1
4	5	1	1	5

(b)Transposition: Group the numbers two by two, from left to right, and then from top to bottom. :
(First table) 1131445113 (second table) 4133145115
= 1131445113 4133145115

(c) Sometimes reconvert the cryptogram into a message using letters again, by utilizing the Polybius square. : ALTVC QNDVE

ADFGVX

Polybius substitution, followed by a transposition:

A- Substitution: The 26 letters of the alphabet and the 10 digits are arranged in a 6×6 table, with the letters ADFGVX added at the ends.

	A	D	F	G	V	X
A	Q	Y	A	L	S	E
D	Z	C	R	X	H	0
F	F	O	4	M	8	7
G	3	I	T	G	U	K
V	P	D	6	2	N	V
X	1	5	J	9	W	B

Example:

Plaintext: RENFORT COMPIEGNE 16H10

Ciphertext 1: DFAXVVFAFDDFGFDDFDFGVAGDAXGGVVAXXAVFDVXA DX

B-Transposition: Use a 6-letter key and write the intermediate text (Ciphertext 1) under this word, then rearrange the columns in ascending alphabetical order.

Example:

Key = DEMAIN

Ciphertext 1: DFAXVVFAFDDFGFDDFDFGVAGDAXGGVVAXXAVFDVXADX

Then read the table from left to right, and from top to bottom.

Ciphertext 2: XDFVAVDFADFFDGFFDGDVAAGXVGGAVXFXADVVXXA D

D	E	M	A	I	N
D	F	A	X	V	V
F	A	F	D	D	F
G	F	D	D	F	G
V	A	G	D	A	X
G	G	V	V	A	X
X	A	V	F	D	V
X	A	D	X		

A	D	E	I	M	N
X	D	F	V	A	V
D	F	A	D	F	F
D	G	F	F	D	G
D	V	A	A	G	X
V	G	G	A	V	X
F	X	A	D	V	V
X	X	A		D	

BAZERIES

Letter Transposition + Simple substitution:

(1) Choose a number as the keyword (e.g., 3752).
(2) Define a 5x5 encryption grid: write out the keyword in letters.
(3) Define another grid of plaintext letters (alphabetical order from top to bottom and left to right).

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

Plaintext

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

Ciphertext

Encryption:

(1) Divide the plaintext message into pieces of different sizes according to the key (each digit of the key corresponds to the size of the group):

For the key 3752, divide the text into a group of 3, followed by a group of 7, then repeat the process.

(2) Reverse the order of the letters in each group.

(3) Encrypt the letters using the encryption grid.

Example:

Plaintext: "**LE CHIFFRE DE BAZERIES EST UN EXEMPLE DE SURCHIFFREMENT**"
Key: **3752**

Key	3	7	5	2	3	7	5	2	3	7	5
Step 1	LEC	HIFFRED	EBAZE	RI	ESE	STUNEXE	MPLED	ES	URC	HIFFREM	ENTFS
Step 2	CEL	DERFFIH	EZABE	IR	ESE	EXENUTS	DELPM	SE	CRU	MERFFIH	SFTNE
Step 3	NJE	XJARRBQ	JZTMJ	BA	JGJ	JDJFSYG	XJEIU	GJ	NAS	UJARRBQ	GRYFJ

Cryptogram: **NJEXJARRBQJZTMJBAJGJJDJFSYGXJEIUGJNASUJARRBQGRYFJ**

NIHILISTES

It is a slightly complicated Polybius square:

(1) Fill the square with a first keyword and complete it (see Polybius).
(2) Encrypt the message according to the square.
(3) Choose another keyword and encrypt it according to the square.
(4) Add letter by letter the encrypted message and the second keyword.

Example :
Key 1: DIFFICILE
Key 2: EASY
Plaintext: "le coyote hurle"

Example :
Key 1: DIFFICILE
Key 2: EASY (ciphered into 21 22 44 54)
Plaintext: "le coyote hurle"

	1	2	3	4	5
1	d	i	f	c	l
2	e	a	b	g	h
3	j	k	m	n	o
4	p	q	r	s	t
5	u	v	x	y	z

Plaintext	L	E	C	O	Y	O	T	E	H	U	R	L	E
Encrypted letters	15	21	14	35	54	35	45	21	25	51	43	15	21
Repeated key	21	22	44	54	21	22	44	54	21	22	44	54	21
Encrypted text	36	43	58	89	75	57	89	75	46	73	87	69	42

Cryptogram: 36435889755789754673876942