SUBSTITUTION POLY-ALPHABÉTIQUE

A ALPHABETS MULTIPLES

- Utiliser plusieurs "alphabets", ce qui signifie qu'une même lettre peut être remplacée par plusieurs symboles.

Exemples :

Bellaso/Porta,
cadran d'Alberti ,
chiffre de Vigenère,
chiffre de Beaufort,
chiffre de Gronsfeld,
le cylindre de Jefferson,
La machine Enigma.

SUBSTITUTION POLY-ALPHABÉTIQUE

A - Cadran d'Alberti

Alberti propose d'utiliser deux disques concentriques :

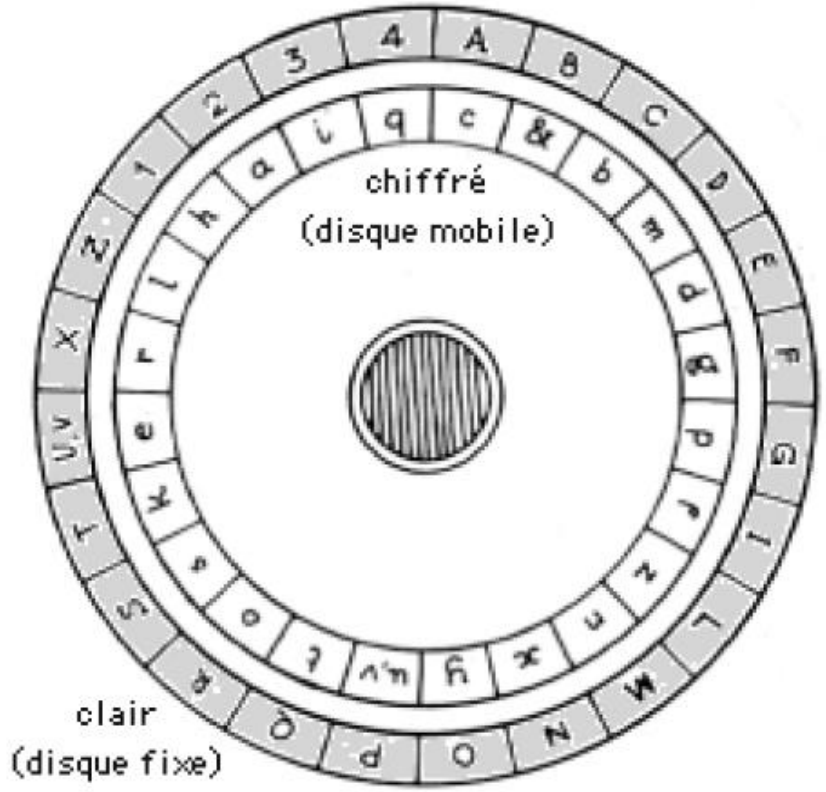
* **un grand disque** : fixe, on écrit l'alphabet dans le bon ordre.
* **un plus petit disque** : mobile, on écrit l'alphabet, mais dans un ordre quelconque.

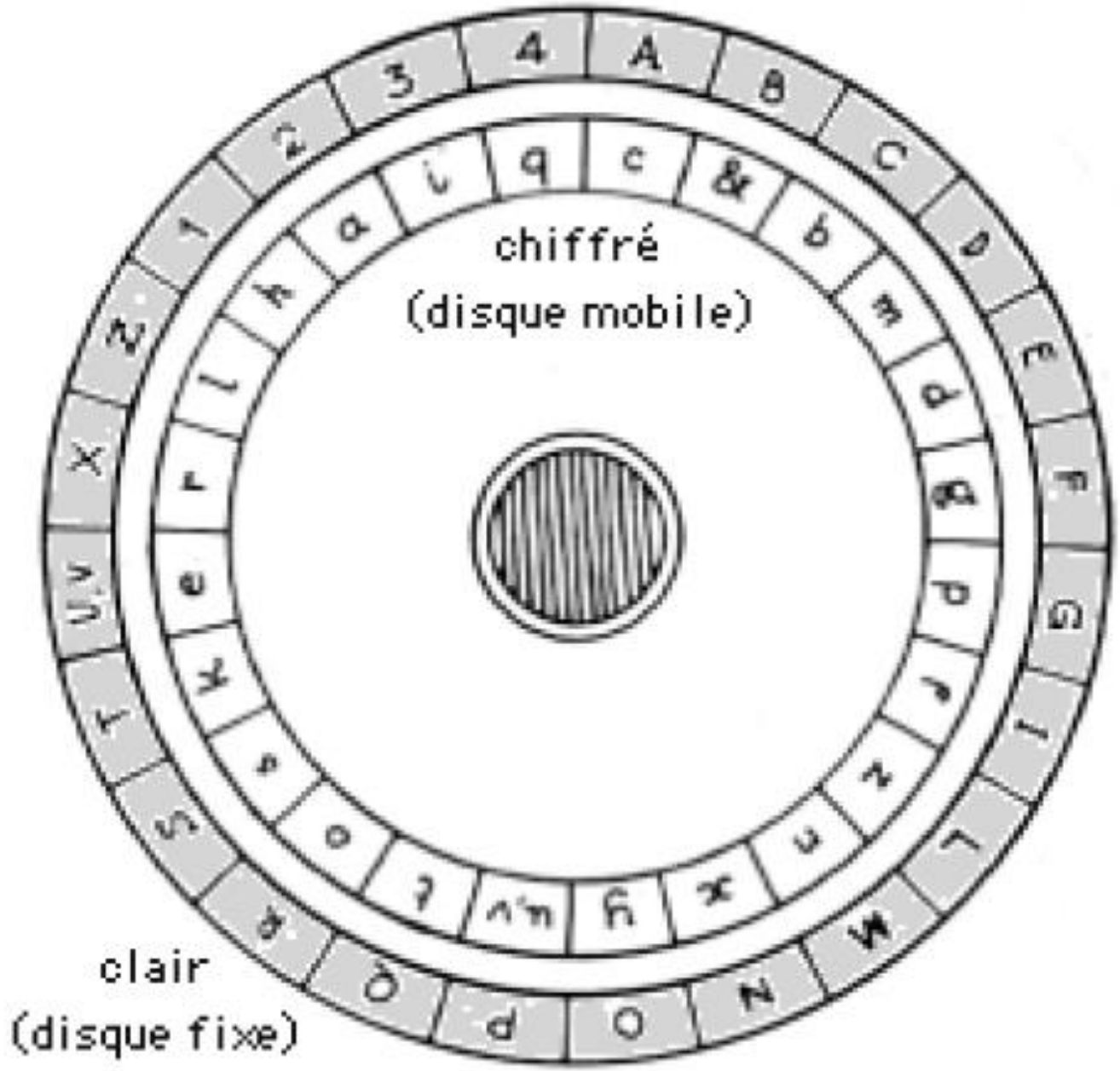
Principe :

(1) : en premier, il faut commencer par ajuster les 2 disques de sorte que les **A** coïncident.

(2) : pour chaque lettre du message clair, chercher la lettre sur le grand disque, la lettre chiffrée est celle qu'on lit en face sur le petit disque.

(3) : pour compliquer les choses, Alberti suggère de tourner périodiquement (par exemple tous les 4 lettres) le petit disque d'un caractère.




chiffré
(disque mobile)
clair
(disque fixe)

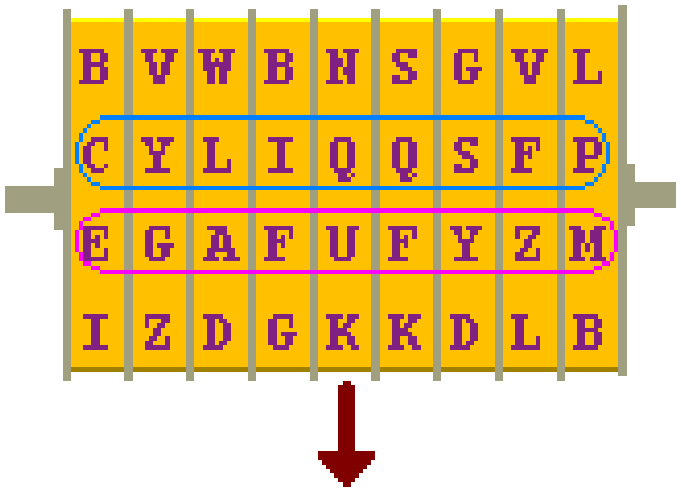
SUBSTITUTION POLY-ALPHABÉTIQUE

B- Cylindre de Jefferson

Le cylindre de Jefferson consiste en une série de 25 ou 26 roues, emboîtées le long d'un axe fixe, et pouvant tourner indépendamment les unes des autres par rapport à cet axe.

Sur chaque roue, on trouve les 26 lettres de l'alphabet, mais écrites dans un ordre quelconque.

- Principe : pour coder le mot CYLINDRE, on fait tourner les roues de sorte de faire apparaître ce mot sur une ligne devant nos yeux. Puis on choisit une autre ligne, par exemple celle juste en dessous, et on envoie la série de lettres qui s'y trouve.

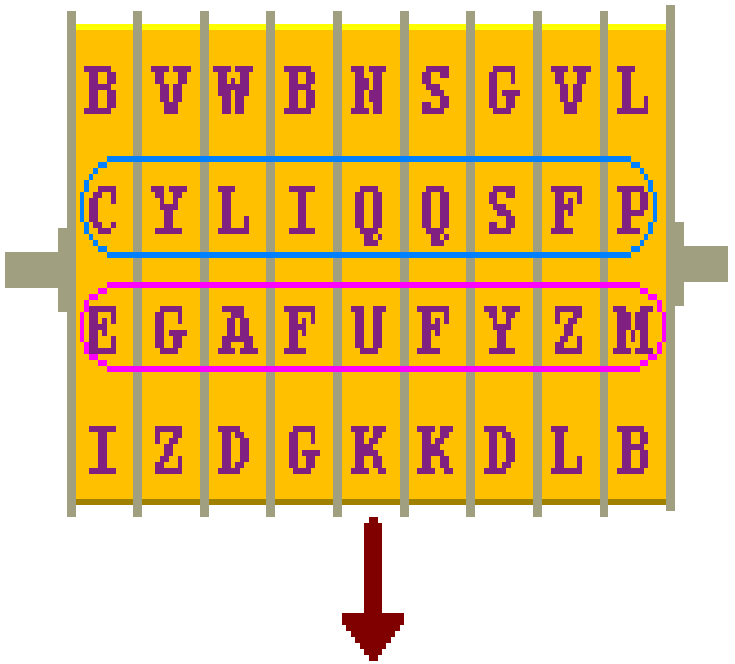


On chiffre le mot : CYLINDRE

On l'écrit sur la colonne entourée de bleu, en faisant tourner les roues.

Le message chiffré se lit juste en-dessous.

Il commence donc par : EGAF…



On chiffre le mot : CYLINDRE

On l'écrit sur la colonne entourée de bleu,

en faisant tourner les roues.

Le message chiffré se lit juste en-dessous.

Il commence donc par : EGAF...

SUBSTITUTION POLY-ALPHABÉTIQUE

C- Chiffre de Vigenère

- Chiffrement par clé répétée.
- A chaque caractère nous utilisons une lettre de la clé pour effectuer la substitution.

L'outil indispensable du chiffrement de Vigenère est la « table de Vigenère ».

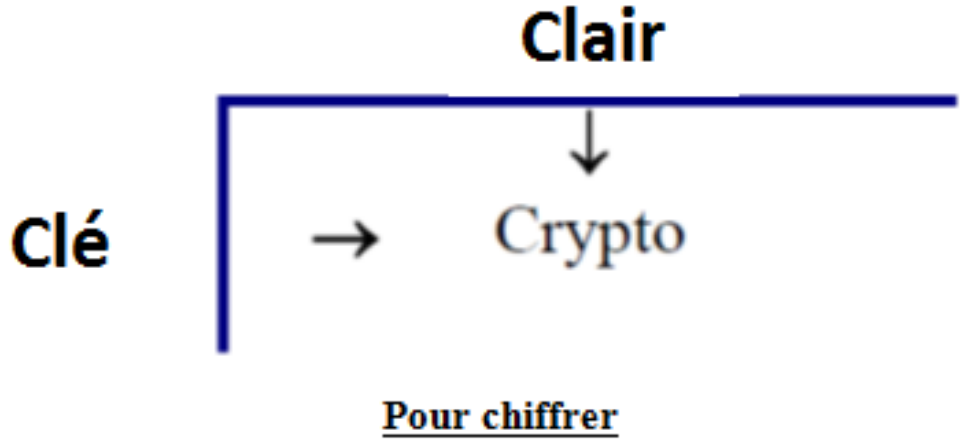
	A	B	C	D	E	etc.
A	a	b	c	d	e	...
B	b	c	d	e	f	...
etc.	c	d	e	f	g	...

		Lettre en clair																								
		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
Clé Utilisée		26 Lettres cryptées																								
	A	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
	B	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
	C	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
	D	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
	E	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
	F	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
	G	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
	H	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
	I	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
	J	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
	K	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
	L	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
	M	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
	N	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
	O	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
	P	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
	Q	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
	R	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
	S	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
	T	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
	U	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
	V	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
	W	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
	X	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
	Y	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
	Z	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

Chiffre de Vigenère

Chiffrement

- On répète la clé en boucle autant que nécessaire (selon le message).
- Pour chaque lettre en clair, on sélectionne la colonne correspondante et pour une lettre de la clé on sélectionne la ligne adéquate, puis au croisement de la ligne et de la colonne on trouve la lettre chiffrée.



Pour chiffrer

Exemple : chiffrer le message RENDEZ VOUS A ALGER avec la clé ORAN

Clair : `RENDEZ VOUS A ALGER`

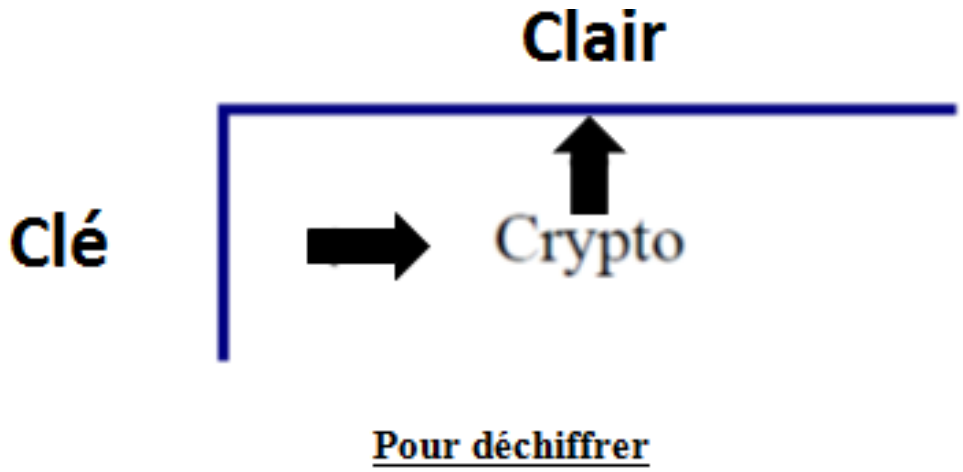
Clé : `ORANOR ANOR A NORAN`

Chiffré: `FVNQSQ VBIJ A NZXEE`

Chiffre de Vigenère

Déchiffrement

- Pour chaque lettre de la clé répétée, chercher la ligne correspondante et on y cherche la lettre chiffrée. La première lettre de la colonne que l'on trouve ainsi est la lettre déchiffrée.



Pour déchiffrer

Exemple : Déchiffrer le message précédemment chiffré

Chiffré: `FVNQSQ VBIJ A NZXEE`

Clé : `ORANOR ANOR A NORAN`

Clair : `RENDEZ VOUS A ALGER`

Chiffre de Vigenère

Mathématiquement,

- Identifier les lettres de l'alphabet aux nombres de 0 à 25 (A=0, B=1...).

Les opérations de chiffrement et de déchiffrement sont, pour chaque lettre, celles du chiffre de César. En désignant :

- La **i^e** lettre du texte clair par **Texte[i]**,
- La **i^e** du chiffré par **Chiffré[i]**,
- La **i^e** lettre de la clé, répétée suffisamment de fois, par **Clé[i]**,

Elle se formalise par :

- Chiffré[i] = (Texte[i] + Clé[i]) modulo 26

- Texte[i] = (Chiffré[i] - Clé[i]) modulo 26

SUBSTITUTION POLY-ALPHABÉTIQUE

D - Réglette de Saint-Cyr

Une règle à calculer, avec une partie fixe, le **stator**, et une partie mobile, le **coulisseau**. Sur le stator est écrit l'alphabet, et sur le coulisseau on trouve deux fois l'alphabet.

Pour chiffrer une lettre, on ajuste le coulisseau pour que sous le A du stator se trouve la lettre de la clé. Sous la lettre du message clair écrite sur le stator, on trouve la lettre du message chiffré.

On veut chiffrer la lettre N, la lettre de la clé étant O.
On aligne ce O sous le A. Sous le N, on lit la lettre chiffrée : B

On veut chiffrer la lettre N, la lettre de la clé étant O.

On aligne ce O sous le A. Sous le N, on lit la lettre chiffrée : B

SUBSTITUTION POLY-ALPHABÉTIQUE

E - OU exclusif (Xoring) : Cet algorithme est de très grande simplicité, il est utilisé dans un grand nombre d'applications commerciales comme Word de Microsoft.
Le principe est que la fonction de chiffrement, est identique à celle de déchiffrement, avec la même clé
(M : le texte en clair, C : le texte chiffré, K : la clé)

$$M \oplus K = C$$

$$C \oplus K = M$$

Table Xor (l'un ou l'autre mais pas les 2 en même temps) :

0 (Xor) 0 = 0

0 (Xor) 1 = 1

1 (Xor) 0 = 1

1 (Xor) 1 = 0

Xoring

Exemple : **M** = 'Le petit prince', **k** = 'cS'

C = **M** (Xor) **k**

C = 'Le Petit Prince'

(Xor) 'cScScScScScScSc'

C = '/6C-'-'C-- :-0-'

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

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

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

❖ Le temps pour casser cet algorithme dépend du rapport :
«taille du message / taille de la clé » : plus, il est grand, plus la tâche est facile

SUBSTITUTION POLY-ALPHABÉTIQUE

F- Machine Enigma (1919)

Le codage est à la fois simple et astucieux.

Principe : chaque lettre est remplacée par une autre (substitution).

La substitution change d'une lettre à l'autre.

SUBSTITUTION POLY-ALPHABÉTIQUE

F- Machine Enigma

- A chaque caractère, les rotors tournent de façon incrémentale : le 1er rotor tourne d'un cran à chaque caractère (à chiffrer).
- Après chiffrement de 26 lettres, c-a-d un tour, Il entraîne le 2ème rotor d'un cran ; puis il recommence (26 lettres)

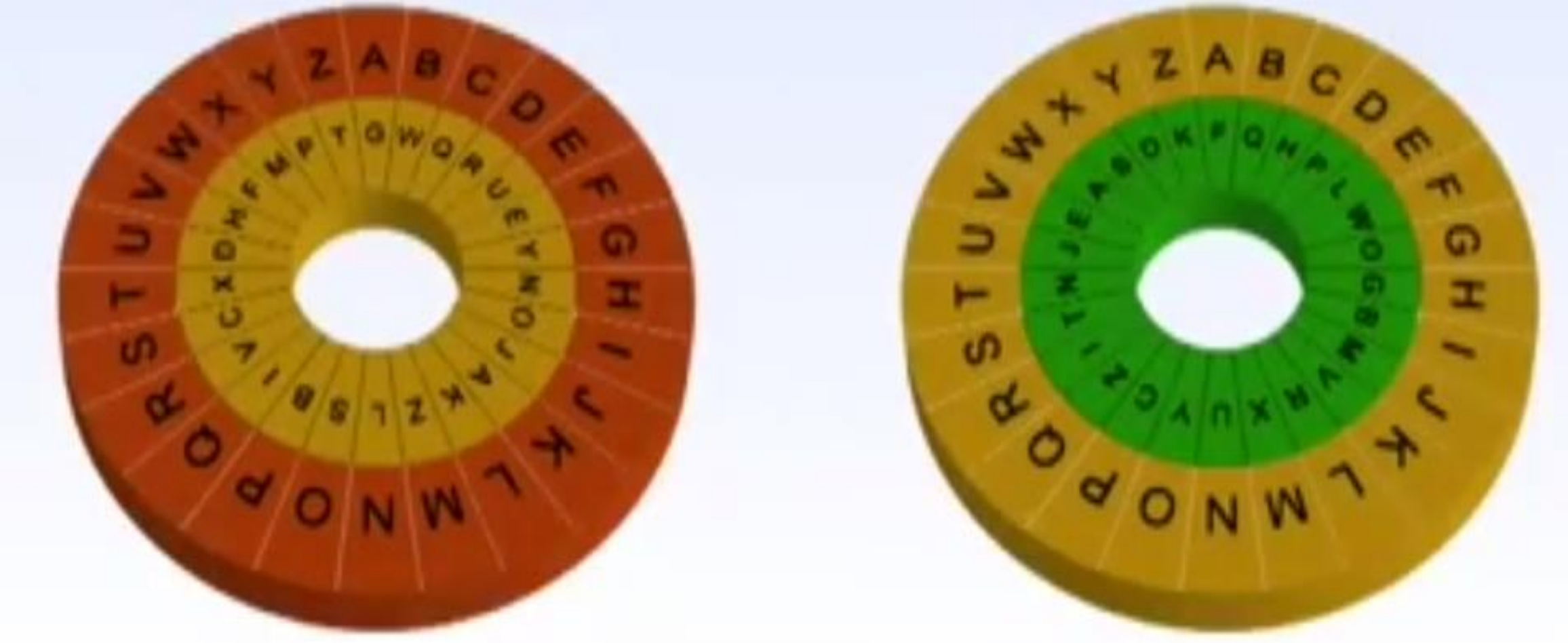
Exemple : 2 anneaux

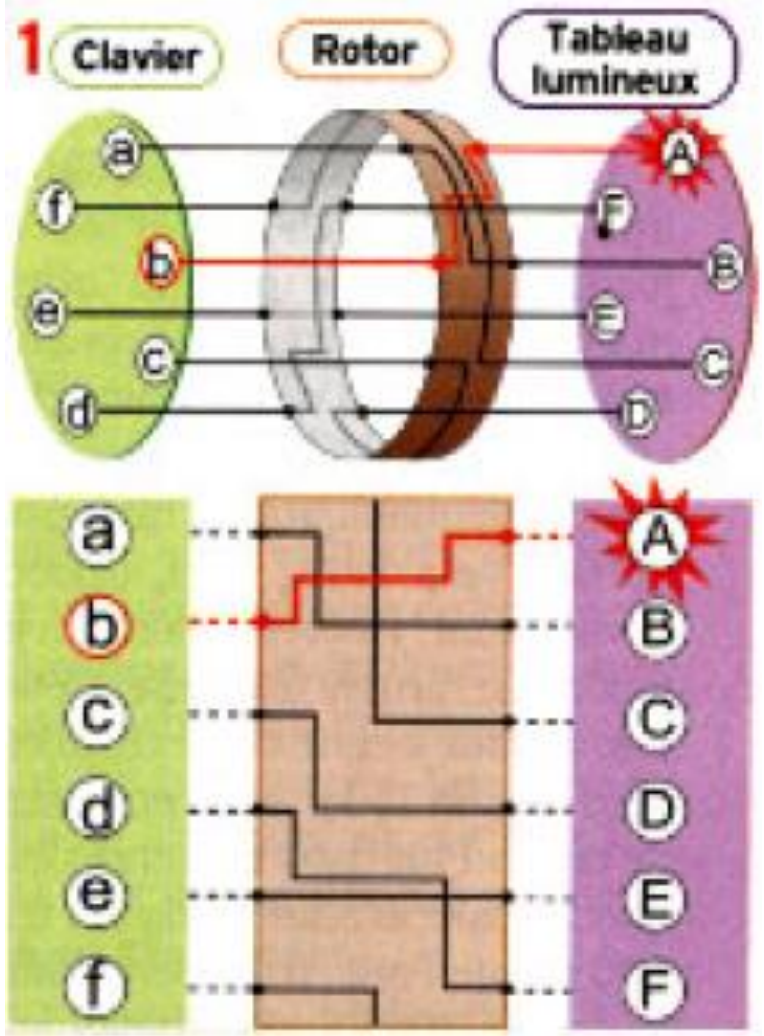
La clé est : la connaissance des rotors choisis (dans l'ordre), de la position initiale de chacun d'eux et de la configuration du tableau de connexions.

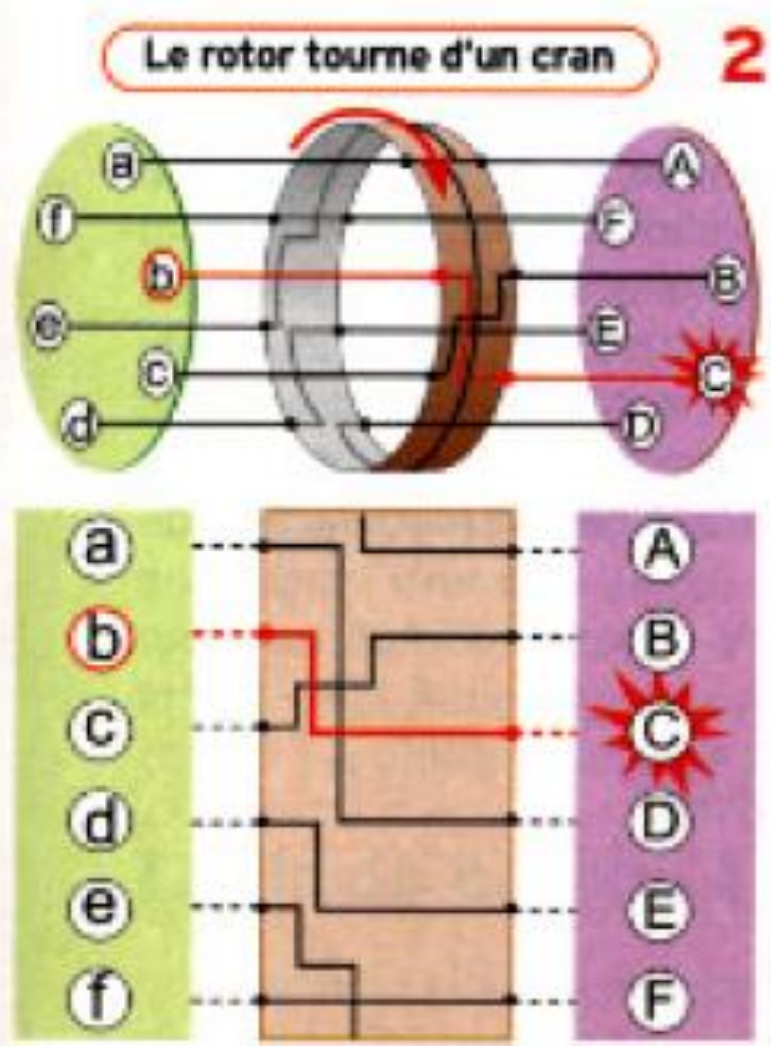
SUBSTITUTION POLY-ALPHABÉTIQUE

F- Machine Enigma

Exemple : 3 anneaux




1
Clavier
Rotor
Tableau lumineux
a
f
b
e
c
d
A
F
B
E
C
D
a
b
c
d
e
f
A
B
C
D
E
F


Le rotor tourne d'un cran
2
a
f
b
c
c
d
A
F
B
E
C
D
a
b
c
d
e
f
A
B
C
D
E
F

TRANSPOSITION

Les caractères du texte en clair sont inchangés mais leur positions respectives sont modifiées

TYPES :

- Transposition simple
- Transposition en zig zag
- Transposition à base matricielle
- Transposition en colonnes à largeurs fixe
- Transposition par grille
- …

TRANSPOSITION SIMPLE

- Changer l'ordre des lettres en décrivant une permutation des lettres simplement.

Exemple : permutation (2, 4, 1, 3) consiste à :
(1) échanger la 1ère lettre avec la 2e, la 2e avec la 4e, la 3e avec la 1ère et la 4e avec la 3e.
(2) refaire le même processus avec les groupes de quatre lettres suivants.

Texte en clair : TRANSPOSITION
Texte chiffré : RNTAPSSOTOIIT

TRANSPOSITION EN ZIG ZAG (Rail Fence)

- Ecrire un message sur deux ou plusieurs lignes selon le nombre de niveaux, une lettre sur une ligne et la suivante sur l'autre.
- Ensuite écrire les différentes lignes obtenues à la suite l'une après l'autre.

Exemple :

Rail Fence à 2 niveaux

Texte en clair : VIENS ME REJOINDRE A CINQ HEURES

V E S E E O N R A I Q E R S
I N M R J I D E C N H U E

Texte chiffré: VESEE ONRAI QERSI NMRJI DECNH UE.

Rail Fence à trois niveaux:

V S E N A Q R
I N M R J I D E C N H U E
E E O R I E S

Texte chiffré: VSENA QRINM RJIDE CNHUE EEORI ES

TRANSPOSITION A BASE MATRICIELLE

La clé est la matrice : c'est-à-dire on connaît la dimension de la matrice (ex : matrice (5, 6)).

Chiffrement :
(1) le message en clair est écrit dans une matrice (en ligne);
(2) lire la matrice en colonne.

Déchiffrement :
(1) le message codé est écrit dans une matrice (en colonne) ;
(2) lire la matrice en ligne.

Exemple :

Clé : matrice (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			

Texte en clair : message secret à transposer

Texte chiffré : meerse taess nrseas ac p grto

TRANSPOSITION PAR GRILLE

Une **grille** (sous forme d'un carré ou d'un rectangle) divisée en un certain nombre de cases. Certaines de ces cases sont appelées **fenêtres** de la grille. Elles servent à l'inscription du clair.

EXEMPLE :
Texte en clair : **"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

Texte chiffré : **DMIEOSAWDSPEASGCMEJULURHGAENFWTN**

- **Le déchiffrement** consiste à appliquer le texte chiffré dans un tableau égal à la grille, et de lire, à travers les fenêtres, le texte clair.

CHIFFRE DE DELASTELLE

Il est un mélange de codage par substitution et par transposition :
(1) : regrouper les lettres du message à chiffrer 5/5,
(2) : utiliser le carré de Polybe et écrire verticalement pour chaque lettre la position dans le tableau.

Exemple : chiffrer le mot : VERONIQUE

(a) Substitution : en utilisant le carré de Polybe :

	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

Le groupe des 5 premières lettres :

V	E	R	O	N
5	1	4	3	3
1	5	2	4	3

Le groupe des 5 suivantes :

I	Q	U	E	
2	4	4	1	0
4	1	5	5	0

Les lettres vides sont remplacées par un double 00.

(b)Transposition : regrouper les chiffres deux par deux, de la gauche vers la droite, puis de haut vers le bas :
(premier tableau)5143315243 (second tableau)2441041550
= 5143315243 2441041550.

(c) Parfois retransformer le code en message avec des lettres en utilisant à nouveau le carré de Polybe.

CHIFFRE ADFGVX

Substitution de type carré de Polybe, suivie d'une transposition :

A- Substitution :

les 26 lettres de l'alphabet et les 10 chiffres sont rangés dans un tableau 6×6, aux extrémités desquelles on a ajouté les lettres ADFGVX

	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

Exemple : texte en clair : RENFORT COMPIEGNE 16H10

DFAXV VFAFD DFGFD DFDFG VAGDA XGGVV AXXAV FDVXA DX

B- Transposition : utiliser une clé de 6 lettres et écrire le texte intermédiaire sous ce mot, puis réordonner les colonnes par ordre alphabétique croissant.

Exemple : Clé = DEMAIN

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		

Ensuite relire le tableau de gauche à droite, et de haut en bas :

XDFVAVDFADFFDGFFDGDVAAGXVGGAVXFXADVVXXA D

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	

SUR-CHIFFREMENT

Consiste à appliquer successivement deux algorithmes de chiffrement (ou plus) au message clair.

- Chiffre de Bazeries
- Chiffre des Nihilistes

CHIFFRE DE BAZERIES

- Transposition des lettres + Substitution simple :

(1) Choisir un nombre comme mot-clé (ex : 3752).
(2) Définir une grille de chiffrement 5x5 : écrire en lettres le mot-clé.
(3) Définir une autre grille de lettres en clair (ordre alphabétique de haut en bas et de gauche à droite).

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

Clair

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

Chiffré

❑ **Chiffrement :**

(1) Découper le message clair en morceaux de différentes tailles selon la clé (chaque chiffre de la clé correspond à la taille du groupe) : Pour la clé 3752, découper le texte en un groupe de 3, suivi d'un groupe de 7, puis recommencer le processus.
(2) Inverser l'ordre des lettres de chaque groupe.
(3) Chiffrer les lettres en utilisant la grille de chiffrement.

Exemple :

Texte en clair : "**LE CHIFFRE DE BAZERIES EST UN EXEMPLE DE SURCHIFFREMENT**"
La clé est **3752**.

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

Cryptogramme final: **NJEXJARRBQJZTMJBAJGJJDJFSYGXJEIUGJNASUJARRBQGRYFJ**

CHIFFRE DES NIHILISTES

- C’est le carré de Polybe légèrement compliqué :

(1) remplir le tableau avec un 1er mot clé et le compléter (voir Polybe).
(2) chiffrer le message selon le carré rempli.
(3) choisir un autre mot clé et le chiffrer selon le tableau.
(4) additionner lettre par lettre le message chiffré et le 2ème mot clé.

Exemple :
Mot clé 1 : DIFFICILE
Mot clé 2 : EASY
Texte en clair : "le coyote hurle"

Exemple :
Mot clé 1 : DIFFICILE
Mot clé 2 : EASY, (chiffré 21 22 44 54).
Texte en clair : "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

Message clair	L	E	C	O	Y	O	T	E	H	U	R	L	E
Lettres chiffrées	15	21	14	35	54	35	45	21	25	51	43	15	21
Mot de passe (répété)	21	22	44	54	21	22	44	54	21	22	44	54	21
Message chiffré final	36	43	58	89	75	57	89	75	46	73	87	69	42

Cryptogramme final: 364358 897557 897546 738769 42