Cryptographie classique

abdelkrimbouadjemi@yahoo.fr

La substitution

La substitution de procédés de chiffrement est un procédé de remplacement qui consiste à remplacer dans un message une ou plusieurs lettres par une ou plusieurs autres, elle se divise en deux parties. La première est la substitution monoalphabétique, la deuxième est la substitution polyalphabétique.

- La **substitution monoalphabétique** consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet.
- La **substitution polyalphabétique** consiste à utiliser une suite de chiffres monoalphabétique réutilisée périodiquement.
- La **substitution homophonique** permet de faire correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères.

Substitution monoalphabétique

- Algorithme de Jules César

Il s'agit du plus simple et plus ancien chiffre classique ayant existé. Son principe est un décalage des lettres de l'alphabet.

Exemple1 : A partir de ce décalage de 3 lettres

Texte 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
Texte codé	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

Le texte que nous souhaitons coder est le suivant : **CE MESSAGE EST BIEN LISIBLE**

Le texte codé sera alors : **FH PHVVDJH HVW ELHQ OLVLEOH**

Substitution polyalphabétique

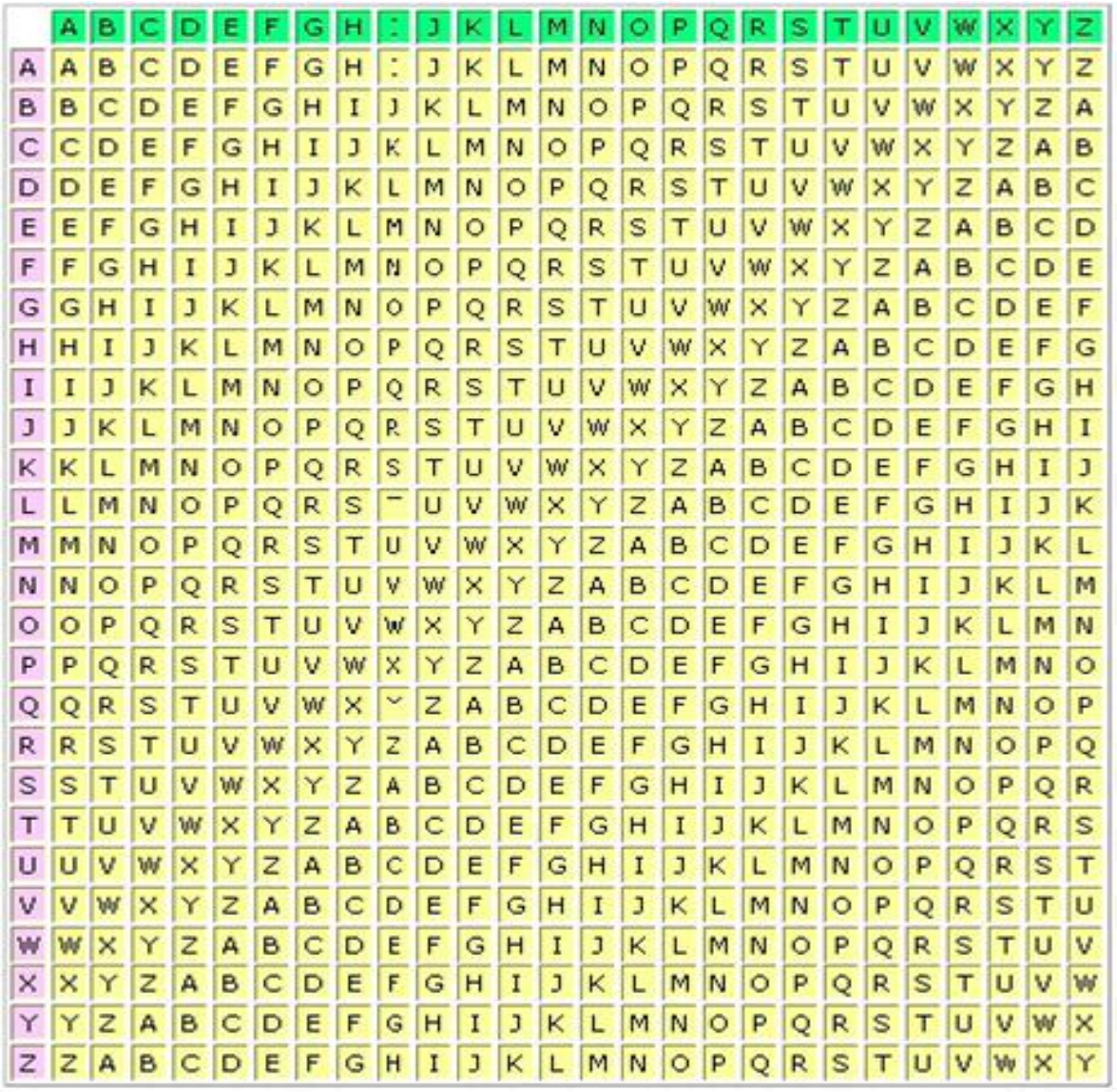
- Algorithme de Vigenère

C‘est une amélioration décisive du chiffre de César. Sa force réside dans l‘utilisation non pas d‘un, mais de 26 alphabets décalés pour chiffrer un message. On parle du **carré de Vigenère**.

Substitution polyalphabétique

Dans l‘exemple suivant on va chiffré le texte "CHIFFRE DE VIGENERE" avec la clé "BACHELIER" (cette clé est éventuellement répétée plusieurs fois pour être aussi longue que le texte clair).

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clé	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I



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

La lettre de la clé est dans la colonne la plus à gauche, la lettre du message clair est dans la ligne tout en haut. La lettre chiffrée est à l‘intersection des deux.

Substitution homophonique

- Algorithme de Polybe

Méthode antérieur à césar , on dispose les lettres dans un tableau 5*5 et on remplace chaque lettre par ces coordonnées.

	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

On remplace alors chaque lettre par ses coordonnées dans le tableau, en écrivant d'abord la ligne, puis la colonne. Par exemple, le A est remplacé par 11, le B est remplace par 12, le F par 21, le M par 32...etc.

Exemple : Si nous codons le texte en clair suivant : **LE CARRE DE POLYBE**
Nous obtenons le texte codé suivant : **3115 1311424215 1415 353431541215**

Transposition

Le chiffrement par transposition est basé sur les permutations des caractères du message en clair. De ce fait, les caractères sont toujours mais dans un Autre ordre pour augmenter les diffusions dans le message en clair. Ce procédé est fondé essentiellement sur des matrices d’ordres nxp.

Transposition simple par colonnes

Dans la matrice, le message en clair est écrit horizontalement et le message chiffré est obtenu en lisant la matrice verticalement. De ce fait, l'ordre de la matrice représente la clé de chiffrement K.

Exemple :

K = 4 x 4

M = INFORMATIQUES

Donc nous avons une matrice de 4 lignes et 4 colonnes.

X est pour compléter la matrice.

Transposition simple par colonnes

1	2	3	4
I	N	F	O
R	M	A	T
I	Q	U	E
S	X	X	X

D’où le message chiffré est
C = IRISNMQXFAUXOTEX

Transposition complexe par colonnes

Dans la transposition complexe par colonnes, le nombre de colonnes (p) de la matrice est fixé par le nombre de caractères d'une clé K (tous les caractères sont différents les uns aux autres), le nombre de ligne (n) dépendra de la longueur du message en clair. Le classement dans l'ordre alphabétique des caractères de la clé permet de fixer le séquencement de la lecture des colonnes de la matrice.

Exemple :

K = GATS, p = 4

M = INFORMATIQUES

Transposition complexe par colonnes

G	A	T	S
I	N	F	O
R	M	A	T
I	Q	U	E
S	X	X	X

Classement par ordre alphabétique des caractères de K

A	G	S	T
N	I	O	F
M	R	T	A
Q	I	E	U
X	S	X	X

Message chiffré est C = NMQX IRIS OTEX FAUX