QUELQUES METHODES DE CHIFFREMENT CLASSIQUES

Le chiffrement de César

- Initialement, le secret échangé était la technique mise en œuvre, ou l'algorithme de chiffrement E. Ainsi le chiffrement de César substituait chaque lettre du message initial M par celle située 3 positions plus loin dans l'alphabet.

- Ensuite, E et D furent paramétrées par une simple clé K, choisie secrètement entre Alice et Bob. D'autres systèmes cryptographiques, plus élaborés virent alors le jour (Chiffrement affine, par substitution etc.…).

Fréquence d'apparition

- Pour ces systèmes dits à substitution mono alphabétique, une cryptanalyse simple consiste à étudier la fréquence d'apparition des lettres au sein du texte chiffré et en déduire la correspondance avec les lettres du texte clair

A	8.11 %	N	7.68 %
B	0.81 %	O	5.20 %
C	3.38 %	P	2.92 %
D	4.28 %	Q	0.83 %
E	17.69 %	R	6.43 %
F	1.13 %	S	8.87 %
G	1.19 %	T	7.44 %
H	0.74 %	U	5.23 %
I	7.24 %	V	1.28 %
J	0.18 %	W	0.06 %
K	0.02 %	X	0.53 %
L	5.99 %	Y	0.26 %
M	2.29 %	Z	0.12 %

la répartition statistique des lettres dans les textes français

Chiffrement Vigenère

Pour contrer cette cryptanalyse, Vigenère mit au point en 1586 un système pour lequel une clef définit le décalage pour chaque lettre du message (A : décalage de 0, B : 1, C : 2, …, Z : 25). Ce chiffrement est illustré dans le tableau 4.2.

Clair	L	A	V	I	E	E	S	T	B	E	L	L	E
Clef	B	O	N	J	O	U	R	B	O	N	J	O	U
Décalage	1	14	13	9	14	20	17	1	14	13	9	14	20
Chiffré	M	O	I	R	S	Y	J	U	P	R	U	Z	Y

TAB. 4.2 – Chiffrement de Vigenère utilisant la clé BONJOUR

Remarques:

la seule attaque possible est la recherche exhaustive de clé secrète.

Pour qu'un système soit inconditionnellement sûr, il faut donc que la clé secrète soit au moins aussi longue que le texte clair. C'est le principe du système du chiffrement à clé jetable présenté maintenant.

Le carré de Polybe
(Chiffrement monoalphabétique)

Polybe, historien grec (env. 200 - 125 av. J.-C.), est à l'origine du premier procédé de chiffrement par substitution.

C'est un système de transmission basé sur un carré de 25 cases (on peut agrandir ce carré à 36 cases).

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

En français, on supprime le W, qui sera le cas échéant remplacé par V. En anglais, on agrège le I et le J.

Chaque lettre peut être ainsi représentée par un groupe de deux chiffres: celui de sa ligne et celui de sa colonne. Ainsi "e"=15, "u"=51, "n"=34, ...

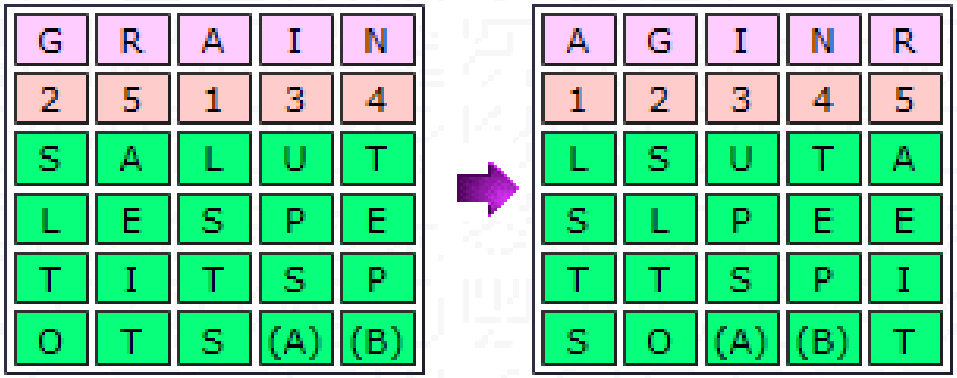
Le carré de Polybe
(Suite)

On peut compliquer ce système de chiffrement avec un mot de passe. Par exemple, si le mot de passe est *DIFFICILE*, on commencera à remplir le carré avec les lettres de ce mot, après avoir supprimé les lettres identiques, puis on complètera le tableau avec les lettres inutilisées (voir les "alphabets désordonnés"). On obtiendra alors:

	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

Transpositions rectangulaires

Une **transposition rectangulaire** consiste à écrire le message dans une grille rectangulaire, puis à arranger les colonnes de cette grille selon un mot de passe donné (le rang des lettres dans l'alphabet donne l'agencement des colonnes). Dans l'exemple ci-dessous, on a choisi comme clef GRAIN pour chiffrer le message SALUT LES PETITS POTS. En remplissant la grille, on constate qu'il reste deux cases vides, que l'on peut remplir avec des nulles ou pas.



G	R	A	I	N
2	5	1	3	4
S	A	L	U	T
L	E	S	P	E
T	I	T	S	P
O	T	S	(A)	(B)

A	G	I	N	R
1	2	3	4	5
L	S	U	T	A
S	L	P	E	E
T	T	S	P	I
S	O	(A)	(B)	T

Carré de Vigenère

(Chiffrement polyalphabétique)

Dans cette table, l'alphabet est répété sur 26 lignes, avec un décalage à gauche de une lettre pour chaque nouvelle rangée.

La lettre de la clef 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 de la ligne de la lettre clef et de la colonne de la lettre claire.

Comment utiliser le carré de Vigenère ?

Trouvez la lettre du message clair dans la colonne la plus à gauche, partez ensuite horizontalement vers la droite jusqu'à la lettre de la clef, puis remontez verticalement pour lire la lettre chiffrée dans la ligne tout en haut.

Carré de Vigenère
(Suite)

Exemple:

clair MONMESSAGE

clef MACLEFMACL

chiffré YOPXIXEAIP

	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
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

Version moderne du carré de Vigenère

Chiffrement à usage unique

Le système à clef jetable (*One time pad*[1]) est un système à clef privée K dans lequel cette clef n'est utilisée qu'une fois. Il repose sur le fait que pour tous messages M et N de même longueur, on a :

$$(M \oplus N) \text{ xor } N = M$$

où $\oplus$ (qu'on note aussi xor) désigne l'opération logique "ou exclusif".

Pour envoyer un message M de n bits, il faut avoir une clef K secrète de n bits. Le message chiffré $\tilde{M}$ est donné par $\tilde{M} = M \oplus K$. Pour déchiffrer, il suffit de calculer $\tilde{M} \oplus K$.

Chiffre de Hill

Le chiffre de Hill substitue m caractères X1, ..., Xm du texte clair par m caractères C1,..,Cm, selon le système d'équations linéaires suivant:

C1=K11 X1 +...+ K1m Xm mod 26

C2=K21 X1 +...+ K2m Xm mod 26

.....

Cm=Km1X1 +...+ Kmm Xm mod 26

ou encore, sous forme matricielle: $C = K X$

Chiffrement de Hill: Clé K

- La matrice K constitue la clé de chiffrement.

  Elle doit évidemment être inversible pour que le déchiffrement soit possible.

  L'algorithme de déchiffrement est alors le même que l'algorithme de chiffrement, en remplaçant simplement K par K^{-1} .

  On voit que, si p<m , alors deux occurrences d'une même chaîne X1...Xp de p caractères ne seront en général pas chiffrées de la même manière.

Méthode de Hill

L’idée de HILL Lester n'est plus de coder lettres par lettres, mais de coder simultanément des groupes de m lettres! Bien sûr, plus m est grand, plus les analyses statistiques deviennent difficiles!

D'abord, nous remplaçons chaque lettre par son ordre dans l'alphabet

-1 : A devient 0, B devient 1,..., Z devient 25.

-2 : On groupe les nombres ainsi obtenus par m (prenons par exemple m=2).

-2 : Pour chaque bloc de m nombres à coder x1x2...xm, on calcule le texte codé en effectuant des combinaisons linéaires (ici m=2) :

Suite Méthode de Hill

$y1=ax1+bx2$
$y2=cx1+dx2$

Si a,b,c,d sont des entiers, y1 et y2 seront aussi des entiers. Pourtant, si l'on souhaite les reconvertir en lettres, il faudrait qu'ils soient compris entre 0 et 25 ce dont on ne peut s'assurer.

On les y ramène en prenant leur reste dans la division par 26. Si z1 et z2 sont les restes respectifs de y1 et y2 dans la division par 26, on peut retransformer z1 et z2 en lettres, et obtenir le message codé.

Le choix de la clé correspond ici au choix d'un nombre m, et au choix des combinaisons linéaires à effectuer (ce sont toujours les mêmes de blocs en blocs).

Exemple

Avec la clé $K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

le texte :

PAYMOREMONEY

est chiffré par:

LNSHDLEWMTRW.

Suite1: Exemple Chiffrement HILL

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Exemple. Avec la clé

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

le texte:

P A Y M O R E M O N E Y

15 0 24 12 14 17 4 12 14 13 4 24

Suite 2 Exemple Chiffrement HILL

Exemple. Avec la clé

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

le texte:

P A Y M O R E M O N E Y

15 0 24 12 14 17 4 12 14 13 4 24

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} * \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix}$$

Suite 3 Exemple Chiffrement HILL

Exemple. Avec la clé

$$K=\begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix}$$

le texte:

P A Y M O R E M O N E Y

15 0 24 12 14 17 4 12 14 13 4 24

est chiffré par:

11 13 18 7 3 11 4 22 12 19 17 22

L N S H D L E W M T R W.

$$\begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix}*\begin{pmatrix}15\\ 0\\ 24\end{pmatrix}$$

17*15+5*24=255+120=375
375 mod 26 = 11

21*15+21*24=315+504=819
819 mod 26 = 13

Exemple 2

Clé : $M = \begin{pmatrix} 3 & 21 \\ 5 & 8 \end{pmatrix}$ inversible

Message : RENDEZ VOUS CE SOIR

RE	ND	EZ	VO	US	CE	SO	IR
(17,4)	(13,3)	(4,25)	(21,14)	(20,18)	(2,4)	(18,14)	(8,17)
$\times M$	$\times M$	$\times M$	$\times M$	$\times M$	$\times M$	$\times M$	$\times M$
(19,25)	(2,11)	(7,24)	(3,7)	(20,18)	(0,22)	(20,22)	(5,18)
TZ	CL	HY	DH	US	AW	UW	FS

Déchiffrement de HILL

Pour déchiffrer un message codé connaissant la clé, on procède exactement de la même façon.

- On découpe donc en blocs de m lettres, mais cette fois il faut inverser les relations données par les combinaisons linéaires : si un système donne y1 et y2 en fonction de x1 et x2, il faut pouvoir l'inverser et exprimer x1 et x2 en fonction de y1 et y2. Ce n'est pas toujours possible (inversion de matrice possible).

Attaque à texte clair connu, et chiffrement de Hill

Lorsque l'on cherche à déterminer la clé de chiffrement d'un adversaire, on peut se situer à plusieurs niveaux d'information.

A)On peut n'avoir à sa disposition que le message chiffré.

B)Parfois, et cela apporte beaucoup d'informations, on dispose à la fois du message chiffré et de sa traduction en clair, ou au moins une partie de celle-ci.

Exemple (Déchiffrement Hill)

On suppose qu'on a le texte codé suivant : COR ZZETMDW...., qui correspond au début de MON GENERAL...

Un espion dans les bases ennemies nous a permis de savoir que nos adversaires utilisent le chiffre de Hill, avec une longueur de clé égale à 2.

On note A la matrice 2×2 de chiffrement à coefficients dans **Z|26Z**.

La première paire CO s'obtient en appliquant la matrice A à partir de la paire MO,

la seconde paire RZ s'obtient en appliquant la matrice A à partir de la paire NG.

Déchiffrement Hill suite

Cela se traduit par la relation matricielle:

$$\begin{pmatrix} 2 & 17 \\ 14 & 25 \end{pmatrix} = A \begin{pmatrix} 12 & 13 \\ 14 & 6 \end{pmatrix}$$

que nous écrivons sous la forme B=AC. Si la matrice C est inversible dans **Z|26Z**, on obtient en multipliant à droite $A=BC^{-1}$.

On s'empresse de calculer le déterminant de C : il vaut 110, qui n'est pas premier avec 26. C n'est pas inversible dans **Z|26Z**. C'est raté! On recommence avec les deuxième et troisième paires :

$$\begin{pmatrix} 17 & 25 \\ 25 & 4 \end{pmatrix} = A \begin{pmatrix} 13 & 4 \\ 6 & 13 \end{pmatrix}$$

qu'on écrit en D=AE. Le déterminant de E vaut 145, il est premier avec 26, et E est inversible dans **Z|26Z**. On obtient alors :

$$E^{-1} = \begin{pmatrix} 13 & 24 \\ 10 & 13 \end{pmatrix} \text{ et } A = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}.$$

On peut vérifier la matrice de chiffrement sur les autres paires.

Chiffrement de XOR (ou exclusif)

Chiffre XOR

- Le chiffre XOR manipule les bits et non plus les caractères.
- Il est basé sur l'opération *ou exclusif bit à bit* (XOR, noté encore $\oplus$).
- On utilise comme clé une chaîne de bits K de longueur donnée L.
- On chiffre en effectuant le ou exclusif bit à bit de la clé K avec le texte clair, découpé en blocs M de longueur L.

Chiffrement ou exclusif

Chiffre XOR

- **Exemple.** Avec la clé K=0101 le texte clair 11110000 sera chiffré ainsi:

11110000 $\oplus$ texte clair

01010101 $\oplus$ clef

10100101 $\oplus$ texte codé

- Rappelons que le ou exclusif est associatif, commutatif, qu'il possède un élément neutre 0, et que toute chaîne K est son propre inverse: $K \oplus K = 0$
- Ainsi, on voit que l'algorithme de déchiffrement est identique au chiffrement, avec la même clé :

$$M = (M \oplus K) \oplus K = C \oplus K$$

FIN

RAPPEL

Cryptage classique