2. Chiffre de Hill

Le chiffre de Hill est un chiffre **polygrammique** (les lettres ne sont pas chiffrées séparément mais par groupes). Le **calcul matriciel** est utilisé pour ce codage.

Chiffrement

1. Les lettres sont remplacées par leur rang dans l'alphabet

A	B	C	D	E	...	V	W	X	Y	Z
1	2	3	4	5	...	22	23	24	25	0

   On aurait également pu poser "A"=0, "B"=1,... "Z"=25 ou alors prendre un alphabet désordonné : "A"=15, "B"=6,... on aurait alors un surchiffrement.

2. On choisit une **matrice de chiffrement** $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

   Cette matrice doit être carrée (même nombre de lignes que de colonnes) et doit être connue de celui qui déchiffrera le message. De plus, elle doit respecter ces deux conditions :
   – elle doit avoir des composantes positives
   – $(ad - bc)$ ne doit être multiple ni de 2 ni de 13.

3. Les lettres, si on a une matrice 2×2, sont codées par paires.
   Les lettres P_k et P_{k+1} du texte clair sont chiffrées C_k et C_{k+1} de cette manière :
   $\begin{cases} C_k = aP_k + bP_{k+1} \\ C_{k+1} = cP_k + dP_{k+1} \end{cases}$ ou $\begin{bmatrix} C_k \\ C_{k+1} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} P_k \\ P_{k+1} \end{bmatrix}$

Exemple

Matrice de chiffrement : $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. Texte à coder : "Je vous aime".

Codage de "Je" :

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} \text{"J"} \\ \text{"E"} \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 10 \\ 5 \end{bmatrix} = \begin{bmatrix} 6 \\ 7 \end{bmatrix} = \begin{bmatrix} \text{"F"} \\ \text{"G"} \end{bmatrix}$$

Codage de "Je vous aime" :

lettres	j	e	v	o	u	s	a	i	m	e
rangs	10	5	22	15	21	19	1	9	13	5
rangs chiffrés	6	7	24	7	5	4	19	16	7	22
lettres chiffrées	F	G	X	G	E	D	S	P	G	V

Déchiffrement

Le principe est le même que pour le chiffrement :

$$\begin{bmatrix} P_k \\ P_{k+1} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \begin{bmatrix} C_k \\ C_{k+1} \end{bmatrix} \text{ avec } \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \text{ (modulo 26)}$$

L'inverse modulo n

L'inverse modulo n de b est le nombre entier b^{-1} tel que $b \cdot b^{-1} (\text{mod } n) = 1$. Par exemple, 7 est l'inverse de 4 modulo 9 car $4 \cdot 7 (\text{mod } 9) = 28 (\text{mod } 9) = 1$.

Quand $n = 26$, la méthode "**force brute**" pour trouver $n^{-1} (\text{mod } 26)$ est la manière la plus simple.
– multiplier n par les entiers m de l'ensemble : {1,3,5,7,9,11,15,17,19,21,23}
– stopper quand $n \cdot m (\text{mod } 26) = 1$. Ainsi : $n^{-1} (\text{mod } 26) = m$

Exemple : cherchons l'inverse de 15 (mod 26) :
$15 \cdot 1 (\text{mod } 26) = 15$, $15 \cdot 3 (\text{mod } 26) = 19$, $15 \cdot 5 (\text{mod } 26) = 23$, $15 \cdot 7 (\text{mod } 26) = 1$, donc 7 est l'inverse que l'on cherchait.

Pour ne pas avoir à recalculer les inverses :

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Exemple (suite)

Calcul de la matrice inverse :

$$\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}^{-1} = \frac{1}{43}\begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} \bmod 26 = \frac{1}{17}\begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} \bmod 26 = 23\begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} \bmod 26 = \begin{bmatrix} 161 & -92 \\ -115 & 207 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix}$$

Le déchiffrement se fait ensuite suivant le même principe qu'avant.

Variante

Le chiffre de Hill existe aussi dans une version trigrammique. On a alors une matrice 3×3. On peut en fait grouper les lettres par 2, 3, 4... Plus les polygrammes contiendront de lettres, plus le chiffre sera sûr, mais les calculs seront compliqués.

Décryptement

On peut casser ce chiffre en cherchant un **mot probable**.

Exemple

Décryptons le message CMYPZ GTAYO EQBYQ JLAOW INELN NECNN UESZT YTFRU OWYXH KYADM NJRUK CUFZP YPNNM XWSQQ OJMGO JZQZQ FLVAY XGIPR OPUFJ WTSVA ATQU, sachant qu'il contient le mot GEORGE PAPANDREOU.

"GEORGE PAPANDREOU" contient des répétitions de bigrammes à des intervalles pairs :

1.GEORGEPAPANDREOU

2.GEORGE PAPANDREOU

On est donc sûr de retrouver soit GE...GE et PAPA, soit EO...EO, car soit c'est G qui est de rang impair soit, c'est E.

On remarque dans le cryptogramme le segment ZQZQ qui pourrait correspondre à PAPA ; le premier Z de ce bigramme est la 77ème lettre du cryptogramme.

Essayons cette correspondance :

chiffré	OJ	MG	OJ	ZQ	ZQ	FL	VA	YX
couples chiffrés	(15 ;10)	(13 ;7)	(15 ;10)	(0 ;17)	(0 ;17)	(6 ;12)	(22 ;1)	(25 ;24)
couples clairs	(7 ;5)	(15 ;18)	(7 ;5)	(16 ;1)	(16 ;1)	(14 ;4)	(18 ;5)	(15 ;21)
clair	GE	OR	GE	PA	PA	ND	RE	OU

Il s'agit maintenant de trouver la matrice de déchiffrement (D).

Dans notre tableau, prenons les premiers et les quatrièmes couples chiffrés et formons une matrice (A) en disposant verticalement ces valeurs. Prenons les premiers et les quatrièmes couples clairs de notre tableau pour former une matrice (B). On aurait pu choisir n'importe quel couple de colonnes du tableau pourvu que la matrice A formée soit inversible modulo 26. On obtient l'équation matricielle : $D \cdot A = B$ on a donc $D = B \cdot A^{-1}$

Dans notre exemple, on a :

$$D = B \cdot A^{-1} = \begin{bmatrix} 7 & 16 \\ 5 & 1 \end{bmatrix}\begin{bmatrix} 15 & 0 \\ 10 & 17 \end{bmatrix}^{-1} = \begin{bmatrix} 7 & 16 \\ 5 & 1 \end{bmatrix}\begin{bmatrix} 7 & 0 \\ 2 & 23 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 11 & 23 \end{bmatrix}$$

On obtient alors facilement le message décrypté :

IT IS BELIEVED BY MANY GREEKS THAT THE HEAD OF THE GROUP CALLED THE SHIELD IS THE SON OF GEORGE PAPANDREOU EX PREMIER OF GREECE (T).

Sources

http ://www.apprendre-en-ligne.net/