

Une petite énigme pour découvrir la méthode de codage de Hill avant de travailler avec le tableur

2. Mise en pratique des matrices avec une méthode de décodage à découvrir

(En 1929, Lester S. Hill a conçu, breveté et mis en vente cette méthode de codage, sans grand succès.)

Vous venez de recevoir un courriel. Il contient un message secret à décoder et une pièce jointe qui semble donner des explications pour utiliser sa «clé»... Travailler pour l'instant sans ordinateur, vous aurez la suite du message à décoder sur un tableur.

Début du message secret :

23 5 12 23 30 4 7 18 23 7

En pièce jointe sur le tableur :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	

$$A = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$$

Utiliser la matrice A (qui est la matrice de « déchiffrement ») et les restes de la division par le nombre 31.

2. Mise en pratique des matrices avec une méthode de décodage à découvrir

(En 1929, Lester S. Hill a conçu, breveté et mis en vente cette méthode de codage, sans grand succès.)

Vous venez de recevoir un courriel. Il contient un message secret à décoder et une pièce jointe qui semble donner des explications pour utiliser sa «clé»... Travailler pour l'instant sans ordinateur, vous aurez la suite du message à décoder sur un tableur.

Début du message secret :

23 5 12 23 30 4 7 18 23 7
L A \ M A C H I N E

En pièce jointe sur le tableur :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
P	Q	R	S	T	U	V	W	X	Y	Z	[]	^		

$$A = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$$

Utiliser la matrice A (qui est la matrice de « déchiffrement ») et les restes de la division par le nombre 31.

$$\begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} 23 \\ 5 \end{pmatrix} = \begin{pmatrix} 74 \\ 125 \end{pmatrix}$$

$$\begin{array}{r|l} 74 & 31 \\ \hline 12 & 2 \end{array}$$

$$\begin{array}{r|l} 125 & 31 \\ \hline 1 & 4 \end{array}$$

$$\begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} 12 \\ 23 \end{pmatrix} = \begin{pmatrix} 59 \\ 106 \end{pmatrix}$$

La méthode de HILL Correction avec le tableur

B12 fx Σ = **=MOD(\$B8*B11+\$C8*C11;\$B\$6)**

	A	B	C	D	E	F	G	H	I	J	K	L
1												
2		1	2	3	4	5	6	7	8	9	10	11
3		A	B	C	D	E	F	G	H	I	J	K
4												
5												
6	Nombre :	31										
7												
8	Matrice A :	3	1									
9		5	2									
10												
11	Message :	23	5	12	23	30	4	7	18	23	7	
12	Déchiffrement :	12	1	28	13	1	3	8	9	14	5	28
13	Décodage :	L	A	\	M	A	C	H	I	N	E	\
14												
15												

	A	B	C	D	E	F	G	H	I	J	K
1											
2		1	2	3	4	5	6	7	8	9	10
3		A	B	C	D	E	F	G	H	I	J
4											
5											
6	Nombre :	31									
7											
8	Matrice A :	3	1								
9		5	2								
10											
11	Message :	23	5	12	23	30	4	7	18	23	
12	Déchiffrement :	12	1	28	13	1	3	8	9	14	5
13	Décodage :	L	A	\	M	A	C	H	I	N	E
14											
15											

B13



=

=CAR(64+B12)

