Le chiffrement de Hill

Objectifs:

- utilisation du calcul matriciel
- utilisation des congruences
- utilisation de Xcas pour calculer

Enoncé « élèves »

le principe du chiffrement :

On associe à chaque lettre de l'alphabet un entier entre 0 et 25:

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

Le codage se fait sur une chaîne de caractères ($n \geq 2$) . Chaque lettre est chiffrée en fonction de sa valeur et de sa place dans la chaîne de caractères. Si la chaîne finale est incomplète , on peut la compléter.
On utilise dans cet exercice des chaînes de 2 caractères.

Partie A: le codage

On veut coder le mot MATH
Une chaîne de deux lettres est associée à un couple ($x_1 ; x_2$) et le chiffrement ($y_1 ; y_2$) est donné par

$$\begin{cases} y_1 \equiv 11 x_1 + 3 x_2 (26) \\ y_2 \equiv 7 x_1 + 4 x_2 (26) \end{cases}$$

1° Utiliser les matrices pour traduire le système : $\begin{cases} y'_1 = 11 x_1 + 3 x_2 \\ y'_2 = 7 x_1 + 4 x_2 \end{cases}$

2° Xcas code les lettres majuscules de 65 à 90 avec l'instruction « asc(«lettre ») » .
L'instruction « irem (a, b) » donne le reste de la division euclidienne de a par b.
L'instruction « char(n) » donne la lettre associée à l'entier n
Utiliser le logiciel pour coder MA et TH

Partie B : un décodage problématique

1°En utilisant xcas coder le mot AMER avec la matrice de codage : $N = \begin{pmatrix} 4 & 2 \\ 3 & 8 \end{pmatrix}$

2° Soit $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, $X_1 = \begin{pmatrix} n_1 \\ m_1 \end{pmatrix}$, $X_2 = \begin{pmatrix} n_2 \\ m_2 \end{pmatrix}$ les couples ($n_1 ; m_1$) et ($n_2 ; m_2$) correspondent à la numérisation de deux chaînes de caractères et M est la matrice de codage.
Exprimer $M X_1$ et $M X_2$ puis traduire la situation rencontrée dans le 1° en utilisant les congruences.

En déduire $(ad - bc)(n_1 - n_2) \equiv 0 (26)$

3° Déterminer une condition sur $ad - bc$ pour que le décodage soit possible.

Partie C : Décodage avec xcas

Avec xcas les minuscules sont codées de 97 à 122 et les majuscules de 65 à 90. On choisira l'une ou l'autre des écritures.

La matrice de codage est : $A = \begin{pmatrix} 11 & 3 \\ 7 & 4 \end{pmatrix}$

1° calculer A^{-1} avec xcas
2° déterminer un entier k tel que la matrice $B = k A^{-1}$ ait des coefficients entiers
3° calculer BA . En déduire un procédé de calcul pour décoder JNFC

Chiffrement de Hill : Eléments de correction

Partie A

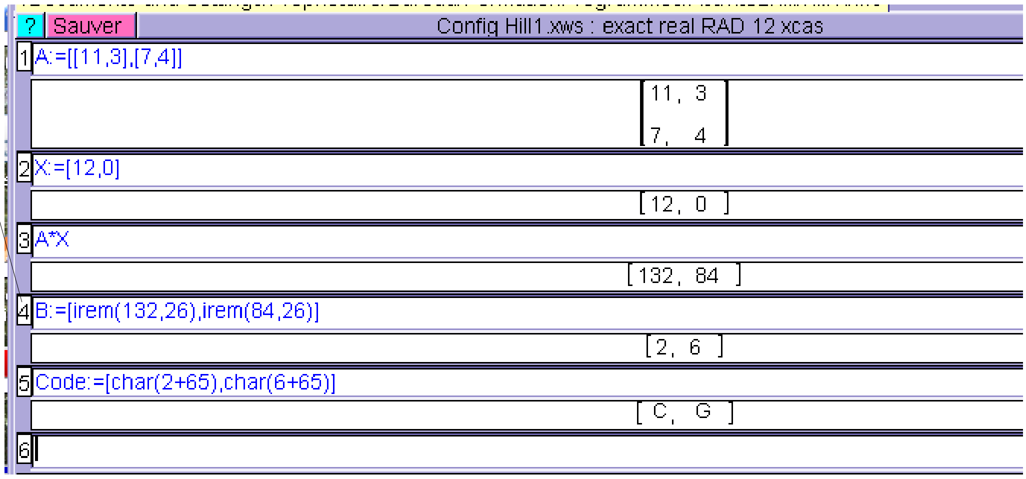
Question 1 : traduction matricielle du système

$A=\begin{pmatrix} 11 & 3 \\ 7 & 4 \end{pmatrix}$ $\quad X=\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ $\quad Y'=\begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix}$ on a $\quad AX=Y'$

Question 2 : Coder « MA » et « TH » avec XCAS:
codage de « MA » numérisé (12 ; 0):

On peut améliorer avec:

B:= irem(A*X , 26)

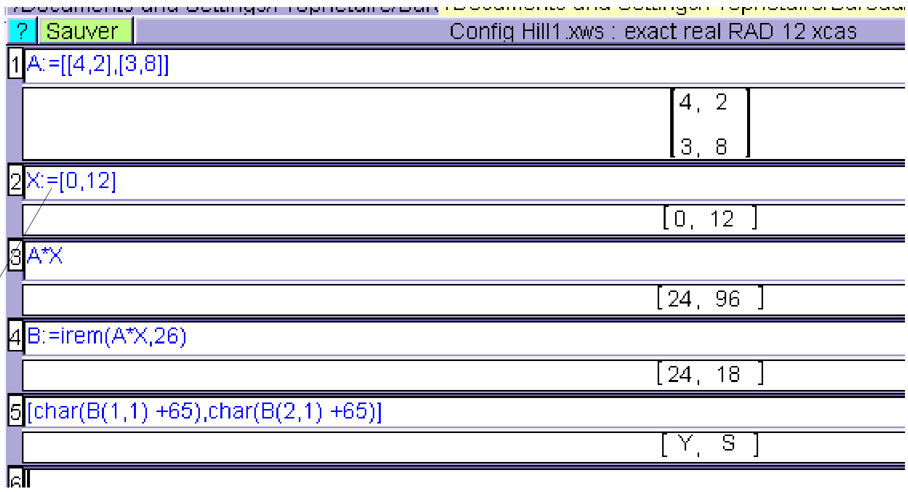


Partie B

Question 1: Codage de AM :

Le vecteur X est une matrice colonne : 2 lignes et 1 colonne

On peut améliorer X par :
X : = [asc(« A »)-65,asc(« M »)-65]



Le codage de ER donne aussi YS . Il y a donc dans ce cas une impossibilité de décodage

Question 2: Travail sur les congruences

$MX_1=\begin{pmatrix} a n_1+c m_1 \\ b n_1+d m_1 \end{pmatrix}$ $\quad MX_2=\begin{pmatrix} a n_2+c m_2 \\ b n_2+d m_2 \end{pmatrix}$ Dans la situation de la question 1 on a :

$\begin{cases} a n_1+c m_1 \equiv a n_2+c m_2 (26) \\ b n_1+d m_1 \equiv b n_2+d m_2 (26) \end{cases}$ donc $\begin{cases} a(n_1-n_2) \equiv c(m_2-m_1)(26) \\ b(n_1-n_2) \equiv d(m_2-m_1)(26) \end{cases}$

d'où $\begin{cases} a d(n_1-n_2) \equiv cd(m_2-m_1)(26) \\ b c(n_1-n_2) \equiv d c(m_2-m_1)(26) \end{cases}$ par soustraction $(ad-bc)(n_1-n_2)\equiv 0(26)$

Question 3: Travail sur la divisibilité

$26|(ad-bc)(n_1-n_2)$, $-26<n_1-n_2<26$ donc 26 ne divise pas n_1-n_2

Deux chaînes différentes aboutissent donc au même code si

- $26|(ad-bc)$
- $13|(ad-bc)$ et $2|n_1-n_2$
- $2|(ad-bc)$ et $13|n_1-n_2$

Conclusion : si 26 et ad – bc sont premiers entre eux , le décodage devient possible.

Partie C *le décodage*

Question 1:

```
? Sauver                                   Config : exact real RAD 12 xcas
1 A:=[[11,3],[7,4]]
                                      [11, 3]
                                      [7,  4]
2 A^-1
                                      [4/23,  -3/23]
                                      [-7/23, 11/23]
3
```

Question 2:

$B=23A^{-1}$ a des coefficients entiers $B=\begin{pmatrix}4 & -3\\ -7 & 11\end{pmatrix}$

Question 3:

$BA=\begin{pmatrix}23 & 0\\ 0 & 23\end{pmatrix}=23I_2$ si on reprend l'écriture matricielle de la partie A 1° on a :

$AX=Y$ équivaut à $BAX=BY$

donc $23X=BY$ on veut des entiers entre 0 et 25 , on note $BY=\begin{pmatrix}b_1\\ b_2\end{pmatrix}$

et on a les relations : $\begin{cases}23x_1\equiv b_1(26)\\ 23x_2\equiv b_2(26)\end{cases}$

Il faut donc trouver *p* tel que $23p\equiv 1(26)$ c 'est à dire tel que *23 p – 26 q = 1*

Avec XCAS :

```
1 bezout_entiers(23,-26)
                                [-9, -8, 1 ]
2
```

p= - 9
q = - 8
Pgcd (23 , -26) = 1

donc $\begin{cases}x_1\equiv -9b_1(26)\\ x_2\equiv -9b_2(26)\end{cases}$

```
/Documents and Settings/Proprietaire/Bureau/FormationProgrammes/Activite2Hill/Hill1PartieC.xws
? Sauver                  Config Hill1PartieC.xws : exact real RAD 12 xcas
1 A:=[[11,3],[7,4]]
                                      [11, 3]
                                      [7,  4]
2 B:=23*A^-1
                                      [4,  -3]
                                      [-7, 11]
3 Y:=[asc("J")-65,asc("N")-65]
                                      [9 ]
                                      [13]
4 BY:=B*Y
                                      [-3]
                                      [80]
5 X:=irem(-9*BY,26)
                                      [1]
                                      [8]
6 decode:=[char(X(1,1)+65),char(X(2,1)+65)]
                                      [ B, I ]
```

Le décodage est: « BIEN »