Voici le principe pour un texte composé uniquement de lettres majuscules:

- on code chaque lettre par son rang dans l'alphabet de 0 pour A jusqu'à 25 pour 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	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

- on regroupe ces nombres par blocs de k caractères pour former des vecteurs lignes x à k colonnes (on prendra ici $k = 2$). S'il manque des nombres pour former le dernier vecteur, on complète arbitrairement ;
- on crypte chaque vecteur X à l'aide d'une matrice de codage A de taille k, modulo 26, et on obtient le vecteur ligne crypté $Y \equiv X\,A\ [26]$;
- le décodage s'effectue en utilisant la matrice inverse de A, modulo 26.

Un mot de 6 lettres a été codé TNLPTM par la méthode du chiffrement de Hill.

La matrice de chiffrement choisie est $A = \begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}$.

a. Montrer que A est une matrice inversible et donner son inverse.

b. Déterminer un entier naturel a tel que la matrice $B = a\,A^{-1}$ soit à coefficients entiers et vérifie : $B\,A \equiv I_2$ [26]

c. Décoder alors le mot TNLPTM.

CORRECTION

a. Une matrice $A\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ est inversible si et seulement si $a\,d - b\,c \neq 0$, ici $3 \times 2 - 1 \times 1 = 5$ donc $3 \times 2 - 1 \times 1 \neq 0$, A et inversible.

$A^{-1} = \frac{1}{5}\begin{bmatrix} 2 & -1 \\ -1 & 3 \end{bmatrix}$

b. $B = a\,A^{-1} = \begin{bmatrix} \frac{2a}{5} & \frac{-a}{5} \\ \frac{-a}{5} & \frac{3a}{5} \end{bmatrix}$

B est à coefficients entiers donc $\frac{a}{5}$ est entier donc il existe un entier naturel k tel que $a = 5k$ donc $B = \begin{bmatrix} 2k & -k \\ -k & 3k \end{bmatrix}$

$B \times A = \begin{bmatrix} 5k & 0 \\ 0 & 5k \end{bmatrix}$

$B \times A \equiv I_2$ [26] $\Leftrightarrow 5k \equiv 1$ [26] $\Leftrightarrow 5 \times 5k \equiv 5$ (26) $\Leftrightarrow k \equiv -5$ (26)

par exemple $k = 26 - 5 = 21$ et $a = 5 \times 21 = 105$ donc si $B = \begin{bmatrix} 42 & -21 \\ -21 & 63 \end{bmatrix}$ alors $B = 105\,A^{-1}$ et $B \times A \equiv I_2$ [26]

c. TN correspond à $\begin{pmatrix} 19 \\ 13 \end{pmatrix}$ est la forme codée de $X\begin{pmatrix} x \\ y \end{pmatrix}$ donc $A\,X = \begin{pmatrix} 19 \\ 13 \end{pmatrix}$

$B \times A\,X = B \times \begin{pmatrix} 19 \\ 13 \end{pmatrix}$ donc $X = B \times \begin{pmatrix} 19 \\ 13 \end{pmatrix} = \begin{pmatrix} 525 \\ 420 \end{pmatrix}$ or $525 \equiv 5$ [26] et $420 \equiv 4$ [26] donc $X \equiv \begin{pmatrix} 5 \\ 4 \end{pmatrix}$ donc TN est décodé par FE

LP correspond à $\begin{pmatrix} 11 \\ 15 \end{pmatrix}$ est la forme codée de $X\begin{pmatrix} x \\ y \end{pmatrix}$ donc $X = B \times \begin{pmatrix} 11 \\ 15 \end{pmatrix} = \begin{pmatrix} 147 \\ 714 \end{pmatrix}$ or $147 \equiv 17$ [26] et $714 \equiv 12$ [26]

donc $X \equiv \begin{pmatrix} 17 \\ 12 \end{pmatrix}$ donc LP est décodé par RM

TM correspond à $\begin{pmatrix} 19 \\ 12 \end{pmatrix}$ est la forme codée de $X\begin{pmatrix} x \\ y \end{pmatrix}$ donc $X = B \times \begin{pmatrix} 19 \\ 12 \end{pmatrix} = \begin{pmatrix} 546 \\ 357 \end{pmatrix}$ or $546 \equiv 0$ [26] et $357 \equiv 19$ [26]

donc $X \equiv \begin{pmatrix} 0 \\ 19 \end{pmatrix}$ donc TM est décodé par AT

TNLPTM est décodé en FERMAT.