Devoir maison 5

Le chiffrement de HILL utilise des matrices et des raisonnements modulo m où m est le nombre de symbole de l'alphabet utilisé.

1. On associe à chaque lettre de notre alphabet un entier de l'ensemble $E = \{0; 2 \ldots; 25\}$ de façon ordonnée. Recopier et compléter le tableau ci-dessous :

Lettre	A	B	...	Z
Nombre	0	1	...	25

2. Dans cette partie, on va chiffrer le message « CLASHOFCLANS » avec la clé de chiffrement :

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

   a. Transformer à l'aide du tableau ci-dessous le message « CLASHOFCLANS » en une suite de nombres.
   b. Regrouper ces nombres deux par deux pour construire 6 matrices colonnes notées de V_1 à V_6.
   c. Déterminer $AV_i\,(26)$ pour i allant de 1 et 6.
   d. Reformer une suite de nombres avec ces six nouvelles matrices colonnes.
   e. Transformer cette nouvelle suite de nombre en mot et vérifier que vous obtenez « HJMCGXULWLMP ».

3. Dans cette partie, on va déchiffrer le message « HJMCGXULWLMP » avec la clé de déchiffrement :

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

   a. Reprendre toute les étapes de la partie précédente en utilisant la matrice B.
   Vérifier que vous obtenez « CLASHOFCLANS ».
   b. Que peut-on dire des matrices A et B ?

4. Dans cette partie, on va déterminer à quelle(s) condition(s) une matrice A est une clé de chiffrement valide.
   a. Coder les message « DA » et « AB » avec la matrice

$$A = \begin{pmatrix} 2 & 6 \\ 1 & 3 \end{pmatrix}$$

   b. Que remarque-t-on ?
   c. Donner une condition nécessaire pour qu'une matrice A soit une clé de chiffrement valide.
   d. On considère à présent la matrice inversible

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

      i. Déterminer son inverse.
      ii. Démontrer qu'il existe $s \in \mathbb{Z}$ tel que $s(ad - bc) \equiv 1\,(26)$ si et seulement si $ad - bc$ est premier avec 26.
      iii. En déduire une clé de déchiffrement associée à A si $ad - bc$ est premier avec 26.

5. Dans cette partie, on va utiliser une matrice de codage d'ordre 3.
   a. Coder le message « CODAGE » avec

$$A = \begin{pmatrix} 1 & 2 & 6 \\ 2 & 5 & 2 \\ 1 & 3 & 7 \end{pmatrix}$$

   .
   b. Décoder le message « XATZOU » avec

$$B = \begin{pmatrix} 5 & 24 & 0 \\ 6 & 19 & 8 \\ 19 & 7 & 19 \end{pmatrix}$$

6. Donner en quelques lignes la biographie de Lester HILL.