CHIFFREMENT DE HILL

Notions réinvesties : théorème de Bézout et théorème de Gauss

Le chiffre de Hill consiste à chiffrer le message en substituant les lettres du message, non plus lettre à lettre, mais par groupes de lettres.
Il permet ainsi de rendre plus difficile le cassage du code par observation des fréquences.
Étudié par Lester Hill[1] (1891-1961), ce système utilise les propriétés de l'arithmétique modulaire et des matrices.

I. Version bigraphique : regroupement par blocs de 2

A. Première clé

On se donne pour clé de chiffrement la matrice $A=\begin{pmatrix}2 & 5\\ 1 & 3\end{pmatrix}$.

Nous allons coder le mot « indice ».
Le texte à coder est découpé en blocs successifs de deux lettres :

$$\begin{pmatrix}I\\N\end{pmatrix},\ \begin{pmatrix}D\\I\end{pmatrix},\ \begin{pmatrix}C\\E\end{pmatrix}$$

soit

$$\begin{pmatrix}8\\13\end{pmatrix},\ \begin{pmatrix}3\\8\end{pmatrix},\ \begin{pmatrix}2\\4\end{pmatrix}.$$

S'il y avait eu un reste, on aurait complété le texte original avec une lettre arbitraire.

a) Coder chaque bloc avec la matrice A, en travaillant « modulo 26 ».

b) En déduire le message chiffré.

c) Déterminer, à la calculatrice, la matrice inverse de A.
Vérifier que cette matrice est une clé de déchiffrement pour le mot codé ci-dessus.

B. Deuxième clé

On se donne maintenant pour clé de chiffrement la matrice $A=\begin{pmatrix}9 & 5\\ 4 & 7\end{pmatrix}$.

En chiffrant le mot « indice » avec cette clé, on obtient « htpqmk ».

Pour chaque bloc X, on a codé en écrivant $AX=Y$.
On a donc envie d'écrire $X=A^{-1}Y$ pour décoder le message crypté Y.

1. a) Montrer que la matrice A est inversible.
Déterminer son inverse sous la forme $\frac{1}{43}B$ où B est une matrice à coefficients entiers.

b) Cette matrice ne permet pas de décoder le message… pourquoi ?

1 Mathématicien, cryptologue et enseignant américain. Il s'est intéressé aux applications des mathématiques dans les communications. Détenteur d'un doctorat de l'université Yale (1926), il a enseigné à l'université du Montana, l'université de Princeton, l'université du Maine, l'université Yale et au Hunter College. Parmi ses principales contributions, il reste le *chiffre de Hill*. Il a aussi développé des méthodes pour détecter des erreurs dans les transmissions télégraphiques.

2. Recherche de l'inverse de 43 modulo 26

On va chercher un entier m tel que $43m \equiv 1$ [26]. C'est ce qu'on appelle ***l'inverse de 43 modulo 26***.

a) Pourquoi cet entier m nous permettra-t-il de décoder Y ?

b) On considère l'équation diophantienne (E) : $43x - 26y = 1$ (x et y entiers relatifs).
Montrer que l'équation (E) admet au moins une solution.

c) En déduire qu'il existe un unique entier m tel que $0 \leqslant m \leqslant 25$ et $43m \equiv 1$ [26].
Puis déterminer cet entier.

d) Décoder le mot « htpqmk ».

C. Cas général : clés possibles

On note $\mathrm{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

1. Condition nécessaire

À un couple Y ne doit correspondre qu'un seul couple X, afin de déchiffrer le message sans ambiguïté.
Or, $\mathrm{AX} = \mathrm{Y}$ admet une unique solution si, et seulement si, A est inversible.
Il est donc nécessaire que la matrice A soit inversible, c'est-à-dire que :

…….

2. Condition suffisante

a) Dans le déchiffrement précédent, quelle condition particulière sur 43 et 26 a permis de répondre à la question B.2.b) ?

b) Pour un chiffrement $\mathrm{Y} \equiv \mathrm{AX}$ [26], l'unicité de la correspondance dans le codage est une conséquence de l'inversibilité de la matrice A modulo 26.
Démontrer que cette condition est vérifiée lorsque $ad - bc$ et 26 sont premiers entre eux.

II. Version trigraphique : regroupement par blocs de 3

On souhaite coder la phrase « codage de hill ».
Le texte à coder est découpé en blocs successifs de trois lettres :

$$\begin{pmatrix} \mathrm{C} \\ \mathrm{O} \\ \mathrm{D} \end{pmatrix}, \begin{pmatrix} \mathrm{A} \\ \mathrm{G} \\ \mathrm{E} \end{pmatrix}, \begin{pmatrix} \mathrm{D} \\ \mathrm{E} \\ \mathrm{H} \end{pmatrix}, \begin{pmatrix} \mathrm{I} \\ \mathrm{L} \\ \mathrm{L} \end{pmatrix} \quad \text{soit} \quad \begin{pmatrix} 2 \\ 14 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 6 \\ 4 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 6 \end{pmatrix}, \begin{pmatrix} 8 \\ 11 \\ 11 \end{pmatrix}.$$

On se donne pour clé de chiffrement la matrice $\mathrm{A} = \begin{pmatrix} 1 & 2 & 3 \\ 9 & 7 & 4 \\ 8 & 6 & 5 \end{pmatrix}$.

1. Coder la phrase avec cette clé.

2. a) Déterminer l'inverse de la matrice A, sous la forme $\frac{1}{21}\mathrm{B}$.

b) Déterminer l'inverse de 21 modulo 26.

c) En déduire la clé de déchiffrement et déchiffrer le message « rcjzjkhftyyg ».