Chiffrement de Hill [1]

Présentation du principe

Le chiffrement de Hill a été publié en 1929. C'est un chiffre polygraphique, c'est à dire qu'on ne chiffre pas les lettres une à une, mais par blocs. Le travail suivant donne un exemple bigraphique où les lettres sont regroupées par deux. On peut augmenter la complexité et donc la force du cryptage en choisissant des blocs plus importants.

Partie A : Chiffrement

On choisit pour clé de chiffrement la matrice $A = \begin{pmatrix} 11 & 3 \\ 7 & 4 \end{pmatrix}$

- On regroupe les lettres par deux et chaque lettre est associée à son rang dans l'alphabet :

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

- On obtient des couples d'entiers $(x_1;x_2)$ où x_1 correspond à la première lettre du bloc et x_2 à la deuxième.
- Chaque couple $(x_1;x_2)$ est transformé en $(y_1;y_2)$ de sorte que y_1 et y_2 sont les restes respectifs de la division euclidienne de $11x_1 + 3x_2$ et $7x_1 + 4x_2$ par 26.

  Autrement dit, $\begin{cases} y_1 \equiv 11x_1 + 3x_2\,[26] & \text{et} \quad 0 \leqslant y_1 \leqslant 25 \\ y_2 \equiv 7x_1 + 4x_2\,[26] & \text{et} \quad 0 \leqslant y_2 \leqslant 25 \end{cases}$.

  Ou encore, $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \equiv A \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} [26]$ avec $0 \leqslant y_1 \leqslant 25$ et $0 \leqslant y_2 \leqslant 25$.
- On identifie alors le bloc de deux lettres obtenu et on l'ajoute au message.

Partie B : Mise en œuvre du chiffrement

1) Vérifier que le bloc TE est transformé en NT.
2) Coder le bloc ST. Que remarquez vous ?
3) Compléter l'algorithme Python suivant permettant de coder un bloc de deux lettres :

```
def hill(lettre1 , lettre2):
    alphabet="ABCDEFGHIJKLMNOPQRSTUVWXYZ"
    x1=alphabet.index(lettre1)
    x2=alphabet.index(lettre2)
    y1=...
    y2=...
    return ...

print(hill('T','E'))
```

4) À l'aide de ce programme chiffrer les mots PALACE et RAPACE. Que remarquez vous ?

Partie C : Déchiffrement

La clé de chiffrement est toujours la matrice A.

1) Montrer que tout couple $(x_1;x_2)$ vérifiant le système $\begin{cases} y_1 \equiv 11x_1 + 3x_2\,[26] \\ y_2 \equiv 7x_1 + 4x_2\,[26] \end{cases}$ vérifie $\begin{cases} 23x_1 \equiv 4y_1 + 23y_2\,[26] \\ 23x_2 \equiv 19y_1 + 11y_2\,[26] \end{cases}$.
2) Déterminer alors un inverse de 23 modulo 26.
3) En déduire la matrice de déchiffrement B telle que $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = B \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$
4) Modifier le programme Python afin de déchiffrer le message PFXXKNESOQPFNTCZFYRSLTNT.

1. Lester S. Hill (18 janvier 1891 - 9 janvier 1961) est un mathématicien, cryptologue et enseignant américain.