TP 3 – Chiffrement de Hill

Le principe du chiffrement de Hill repose sur le choix d'une matrice A vérifiant les conditions suivantes :

- $\det(A) \neq 0$;
- $\det(A)$ est premier avec 26.

On rappelle par ailleurs que pour coder un texte ayant un nombre pair de n lettres, on procède de la manière suivante :

- On associe à chaque lettre de l'alphabet un nombre entre 0 et 25 à l'aide du tableau suivant :

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

- On divise le texte à chiffrer en bloc de deux lettres successives. On obtient ainsi plusieurs blocs de nombres $(x_1; x_2); \ldots; (x_{n-1}; x_n)$.
- On calcule, pour tout $k \in \{0; \ldots; \frac{n-2}{2}\}$, $\begin{pmatrix} y_{2k+1} \\ y_{2k+2} \end{pmatrix} = A \times \begin{pmatrix} x_{2k+1} \\ x_{2k+2} \end{pmatrix}$.
- On réduit modulo 26 chacun des y_k : plus précisément, pour tout $k \in \{1; \ldots; n\}$, on calcule le reste r_k de la division de y_k par 26. On obtient donc une liste de nombres $r_1; \ldots; r_n$.
- On transforme la liste des r_k en un texte en associant chaque nombre r_k à une lettre grâce au tableau précédent.

Sachant que la matrice qui a été utilisée pour le chiffrement est $A = \begin{pmatrix} 7 & 2 \\ 1 & 3 \end{pmatrix}$, écrire un algorithme en langage Python permettant de déchiffrer le texte suivant (disponible en ligne) :

gmroaomfioerqajmvfhtusindfgumgeewfgtubvflswzzkwzkajoaoehcewzmypno
iznqsfuanvduwlfxdpjawromfedaygbnustusqnzxwzetjbwhfjanqrizfjlvstgiuekd
nnrbxdouroiwpyftswbjeuuwlsetrnzfyinyqyzsevswnbuwiouknvmxpjoyvfpxxd
anzjetcdhxedkclfpejbzggktrubkacxkcubvfroowxdmfmgdtbwocxpzxkbftlssgal
mhqneddppjebpyftwvwhdttrubromgcreeedpnevoqcnojxhlxanmrionfixftfjoah
jfjvzedroqzqaftixwvwovscrwookfjpnlvkhlblxmfftgmtryekckaxdvfkcdfojll

Histoire

Lester S. Hill (1891-1961) est un mathématicien américain, spécialiste de cryptographie. Il a notamment mis au point le chiffrement qui porte son nom. Ce procédé peut être vu comme une généralisation du chiffrement affine mais est plus efficace car il ne peut pas être cassé facilement par une analyse des fréquences d'apparition des lettres.

En pratique, on ne regroupe pas les lettres par blocs de deux lettres mais plutôt par blocs de k lettres et la matrice utilisée es donc une matrice de taille $k \times k$. Cela augmente le nombre de possibilités pour coder une même lettre et rend ainsi le chiffrement de Hill plus efficace.

Notons enfin que Lester S. Hill est connu pour avoir conçu une machine permettant de réaliser mécaniquement les calculs du chiffrement.

Lester S. Hill