Contrôle de TP

On ne considérera que les textes composés des 29 symboles suivants :
'a' 'b' 'c' ... 'z' 'la virgule' 'le caractère espace' 'le point'.

Ces symboles seront représentés par des entiers comme suit :
a=0, **b**=1, **...z**=25, **virgule** = 26, **espace**=27, **point**=28.

La matrice de chiffrement est donc composée d'éléments de $\mathbb{Z}/29\mathbb{Z}$ et tous les calculs se font dans le corps fini $(\mathbb{Z}/29\mathbb{Z}, +, \times)$. Pour rappel, dans un corps fini quelconque, l'opération $\frac{a}{b}$ signifie que l'on multiplie a par le symétrique (pour la loi multiplicative) de l'élément b.

Note : Pour effectuer l'inversion (modulaire) de matrice, vous pouvez utiliser l'outil mis à disposition ici : https://www.dcode.fr/inverse-matrice.

Exercice 1 : Cryptanalyse du Chiffre de Hill

On suppose ici que $n = 3$. Vous disposez du texte chiffré ci-dessous, obtenu avec une clé $A \in \mathcal{M}_{3\times 3}(\mathbb{Z}/29\mathbb{Z})$.

**pfjgflgpbvlhxiimynolvztxvsgodmcusqkhuksgumnzktdhuqlqkhmhfujuapdsahth
mmtpjjjgtuoxzuignqecqzunkgaikhxervuksoyxuqlfhgnnljnrjlimelnfsugvuclpldp
roiurmwbbdrmxtoepsgfmhfetoerwqzbbjxjxjiehrhjzzyxvicavizqoyiunkesvakmk
cqqujqkhaozqzbbdrgdznyewkwguzqkhhbgofrtjgsjlhdyzrllzuxiibnegczvbxukssl
aapdgcejgizvggwhobjdcz**

Vous savez que les chaînes "baa", "aba", "aab" sont respectivement chiffrées en "hlt", "gdf", "mcb" avec la matrice A.

1. Déterminer la valeur de la matrice A.
2. Déchiffrer le texte ci-dessus.

Pour la suite, on considérera une variante du Chiffre de Hill où la clé de chiffrement est composée d'une matrice A de taille $n \times n$ (**inversible** dans $\mathcal{M}_n(\mathbb{Z}/29\mathbb{Z})$) et d'un vecteur colonne b **quelconque** de taille n composé d'éléments de $\mathbb{Z}/29\mathbb{Z}$. Cette variante s'appelle le Chiffre de Hill affine.

Exercice 2

Écrire une fonction **gen_cle_hill(n)** qui génère une clé de chiffrement.
Cette clé sera représentée par une liste de $\mathbf{n+1}$ sous-listes de taille n, Les n premières sous-listes représentant la matrice A et la dernière sous-liste, le vecteur colonne b. À titre d'exemple, pour $n = 3$, la clé composée de la matrice :

$$A = \begin{pmatrix} 14 & 17 & 4 \\ 28 & 20 & 10 \\ 19 & 20 & 27 \end{pmatrix}$$

et du vecteur $b = \begin{pmatrix} 10 \\ 18 \\ 6 \end{pmatrix}$
sera représentée en Python par la liste $[[14, 17, 4], [28, 20, 10], [19, 20, 27], [10, 18, 6]]$.

Exercice 3

Pour chiffrer, à partir d'une clé (A, b), un message m composé de n symboles, on calcule $c = Am + b$. C'est à dire que le cryptogramme est le résultat de la multiplication de la matrice A par le vecteur colonne m, résultat auquel on ajoute ensuite le vecteur colonne b ; **toutes ces opérations étant effectuées dans** $\mathbb{Z}/29\mathbb{Z}$.
Écrire la fonction **Hill_affine_chiffre(texte, cle)** qui effectue l'opération de chiffrement selon le principe décrit plus haut. Attention, en appliquant le chiffrement affine de Hill vous allez obtenir des listes de taille n (taille de la matrice) contenant des entiers qui représentent des caractères, ce sont ces caractères qu'il faudra retourner.

Exercice 4

Pour retrouver le message m à partir du cryptogramme c et de la clé (A, b), il faut calculer $A^{-1}(c - b)$.
Écrire la fonction **Hill_affine_dechiffre(texte, cle)** qui déchiffre 'texte' avec 'cle'.

Jusqu'à présent afin de chiffrer un texte de taille quelconque, ce denier est découpé en blocs de taille n. Notons $m^{(1)}, m^{(2)}, \ldots, m^{(t)}$ les blocs correspondants. L'opération de chiffrement consiste à appliquer la transformation de Hill affine à chacun de ces blocs afin d'obtenir les cryptogrammes $c^{(1)}, c^{(2)}, \ldots, c^{(t)}$. Ainsi si 2 blocs de texte $m^{(j)}$ et $m^{(k)}$ sont identiques, cela donnera deux cryptogrammes $c^{(j)}$ et $c^{(k)}$ identiques, ce qui peut être une source d'information pour un éventuel attaquant. On se propose donc de modifier le procédé de chiffrement de plusieurs blocs de taille n, de la façon suivante :

- On tire au hasard un vecteur colonne $c^{(0)}$ de taille n, à éléments dans $\mathbb{Z}/29\mathbb{Z}$.
- Pour chiffrer le bloc $m^{(1)}$, on applique la transformation de Hill affine à $m^{(1)} \oplus c^{(0)}$, ceci donne donc le cryptogramme $c^{(1)}$.
- Pour chiffrer le bloc $m^{(2)}$, on applique la transformation de Hill affine à $m^{(2)} \oplus c^{(1)}$, ceci donne donc le cryptogramme $c^{(2)}$.
- Plus généralement, pour chiffrer le bloc $m^{(i)}$, on applique la transformation de Hill affine à $m^{(i)} \oplus c^{(i-1)}$, ceci donne donc le cryptogramme $c^{(2)}$.
- Le message chiffré est la concaténation des blocs $c^{(0)}$, $c^{(1)}$, $\ldots$, $c^{(t)}$.
- Déchiffrement : pour chaque bloc $c^{(i)}$, avec $i \geqslant 1$, on calcule $m^{(i)} = c^{(i-1)} \oplus D(c^{(i)})$, où D est la fonction de déchiffrement d'un bloc, i.e. $D(c) = A^{-1}(c - b)$.

Exercice 5

Écrire la fonction **Hill_affine_chiffre_en_chaine(texte, cle)** qui réalise l'opération de chiffrement.

Exercice 6

Écrire la fonction **Hill_affine_dechiffre_en_chaine(texte, cle)** qui réalise l'opération inverse.