Cryptographie

Chiffrement de Hill : attaque à clair connu

UNIVERSITÉ de Cergy-Pontoise

Exercice 1 : Décrypter le texte suivant qui a été obtenu en appliquant le chiffrement de Hill sur des blocs de taille 2 sur un mot de la langue française :

`gzatzxjihvbreosu`

sachant que le chiffrement du mot

`chiffrement`

avec la même clé donne le chiffré

`jvfrtqealv`

Exercice 2 : Un chiffrement affine de Hill est le modification suivante d'un chiffrement de Hill : on se donne une matrice A de taille $m \times m$ et un vecteur $\boldsymbol{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$. On chiffre le message par blocs de taille m. Le chiffré de $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in (\mathbb{Z}_{26})^m$ est $\boldsymbol{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} \in (\mathbb{Z}_{26})^m$ défini par $\boldsymbol{y} = A\boldsymbol{x} + \boldsymbol{b}$.
On suppose qu'Eve sait que le texte clair :

`adisplayedequation`

se chiffre en

`dsrmsioplxljbzullm`

De plus, Eve sait que $m = 3$. Déterminer A et $\boldsymbol{b}$ en détaillant tous les calculs.