Fiche de TD n° 1

Exercice n° 1

1) Dans un chiffrement basé sur la transposition par colonnes utilisant une matrice dont la dimension 2x4 (2 lignes et 4 colonnes) et la clé $(4\ 2\ 1\ 3)$, quel est le chiffrement du message "EINSTEIN" ?
2) Quel est le résultat du chiffrement du message "EINSTEIN" si on utilise des transpositions périodiques dont la taille du bloc est 4 et la clé $(4\ 2\ 1\ 3)$?

Exercice n° 2

En utilisant la numérotation des lettres de l'alphabet suivante :

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

1. Coder le message "EINSTEIN" à l'aide du chiffrement par décalage dont la clé $K = 5$.
2. Déchiffrer le message " SJBYTS" sachant qu'il a été créé par un chiffrement par décalage dont la clé K=5.
3. On utilise une substitution affine pour chiffrer un message de la manière suivante :

$$\forall\ \boldsymbol{k} = (\boldsymbol{a}, \boldsymbol{b}) \in \boldsymbol{K}, \boldsymbol{x} \in \boldsymbol{P}$$

$$\boldsymbol{e_k(x)} = (\boldsymbol{ax} + \boldsymbol{b})\ [\mathbf{26}] = \boldsymbol{y}, \quad \boldsymbol{d_k(y)} = \boldsymbol{a^{-1}(y - b)} = \boldsymbol{x}$$

   a. Chiffrer le message de la question 1 en utilisant la clé K=(3,12) ?
   b. Calculer $3^{-1}\ [26]$ en utilisant l'algorithme d'Euclide étendu.
   c. Déchiffrer le message de la question 2 ?

Exercice n° 3

On considère un chiffrement de Hill s'effectuant par bloc de 2 lettres à l'aide d'une clé de chiffrement qui est la matrice carrée d'ordre 2 : $K = \begin{bmatrix} 2 & 5 \\ 1 & 4 \end{bmatrix}$.

On cherche à chiffrer le message : M = "CODAGE" par le chiffrement de HILL**.**

1) A l'aide la grille utilisée dans l'exercice n° 2,
   a. Calculer les matrices $Y_1 = KX_1,\ Y_2 = KX_2\ et\ Y_3 = KX_3$ tel que $M = X_1X_2X_3$
   b. A l'aide du tableau précédent, en associant les éléments des matrices Y_1, Y_2, et Y_3, quel est le résultat de chiffrement du message "CODAGE".
2) Déterminer K^{-1} la matrice inverse de K.
3) Déchiffrer le message "WGGDGW" en utilisant la même clé K pour vérifier que ça redonne le message d'origine.