

Exercice N° 01:

1. Trouver les coefficients u, v et le $PGCD$ des nombres entiers suivants:
 - $(a, b) = (60, 19)$
 - $(a, b) = (280, 11)$
 - $(a, b) = (38, 26)$
2. Calculer l'inverse de :
 - $41^{-1} \text{ mod } 53$.
 - $317^{-1} \text{ mod } 521$

Exercice N° 02: (Chiffrement par décalage)

1. Ecrire un pseudo-code de chiffrement/déchiffrement d'un texte avec César.
2. Prouver que $D_k(E_k(m)) = m$.
3. Chiffrer le texte «CRYPTOGRAPHIE» avec la clé **K**.
4. Déchiffrer le texte « JOPMMYLTUAZFTLAYPXBLJSHZZPXBL » avec la clé **H**.

Exercice N° 03: (Chiffrement Vigenère)

1. Ecrire un pseudo-code de chiffrement/déchiffrement d'un texte avec Vigenère.
2. Chiffrer le texte «CRYPTOGRAPHIE » avec la clé « SECRET ».
3. Déchiffrer le texte «ORABCNDIBDIVD» avec la clé « KEY»:

Exercice N°04: (Chiffrement affine)

Soit $K = (5, 11)$

1. Prouver que $D_k(E_k(m)) = m$
2. Calculer les fonctions de chiffrement et de déchiffrement,
3. Chiffrer le mot suivant: "AFFINE"

Exercice N°05: (Analyse fréquentielle)

Supposons qu'Oscar ait intercepté le message suivant (sans espaces ni signes de ponctuation):

ATKGIZOUTSGRBKORRGZKWAIOIUSVXUSKZRGYKIAOXZKJKYJUTTKKYUAYEYZKSKYJOTLUXSGZOWAK

1. Calculer le nombre d'occurrences de chacune des lettres de l'alphabet dans ce message.
2. Expliquer pourquoi on peut supposer que la lettre K se déchiffre en E.
3. Trouver la clé de déchiffrement et le début du texte en clair.

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