TD3 : Sécurité Informatique

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

Exercice 1 :

Pour crypter des messages on va utiliser le chiffrement affine avec la clé (a=11, b=5).

1. Crypter le message : « MIRO »
2. Décrypter le message : « KADZ »

Exercice 2 :

- En utilisant le chiffre de Vigenère et le mot clé K= « INTERNE» chiffrez le message suivant :« SECURITE INFORMATIQUE »
- En utilisant la même clé déchiffrez le message : « INFORMATION CORRECT »

Exercice 3 :

Soit k la matrice clé de Hill tel que :

$$K=\begin{pmatrix} 11 & 5 & 7 \\ 0 & 2 & 9 \\ 3 & 4 & 0 \end{pmatrix}$$

- Chiffrez le message : « Hello John»

Exercice 4 :

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i /j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Soit le tableau de chiffrement en face :
Le chiffrement avec ce tableau se fait comme suit :
Chaque lettre est codée par le numéro de sa ligne ||numéro de colonne.
Alice et Bob ont utilisé ce tableau, et le résultat du chiffrement de leur conversation était le suivant :

Alice : « 41451531 154344 1315 13232421214215?»
Bob : «13’154344 3115 13232421214215 1415 353431541215»
Alice : «414524 154344 353431541215?»
Bob : «13’154344 4533 232443443442241533 22421513 »
Alice: « 1544 4324 3433 1543431154112444 453315 5111422411334415 11511513 323444 133115 “4315134542244415”»

1- Découvrez la conversation d’Alice et Bob.
2- En utilisant les résultats de la question précédente, chiffrer le message suivant.

M= « Avant de vouloir qu’un logiciel soit réutilisable, il faudrait d’abord qu’il ait été utilisable - Ralph Johnson».