Année : 2022/2023

Université Abdalhafid Boussouf Mila
Institut des sciences et technologies
3ème Année informatique
Module: Sécurité informatique

Série TD N° 03

Exercice 1 :

1. Chiffrez le texte suivant en utilisant le chiffre de César avec la clé **F** :

   Je suis à Mila dans un des rues les plus misérables de la ville

2. Voici un texte chiffré en utilisant le chiffre de César avec la clé **H** :

   TVKBSL ZLJBYPAL PUMVYTHAPXBL

   Retrouvez le texte clair.

Exercice 2 :

1. Chiffrez le texte suivant en utilisant le chiffre de Vigenère avec la clé **MARS** :

   LE SOLEIL A RENDEZ VOUS AVEC LA LUNE

2. Voici un texte chiffré en utilisant le chiffre de Vigenère avec la clé **MUSIQUE** :

   V UVWHY IOIMBUL PM LSLYI XAOLM BU NAOJVUY

- Retrouvez le texte clair.

Exercice 3 :

La cryptographie classique basée sur l'utilisation des lettres de la langue pour le chiffrement des textes, elle est divisée en deux classes.

- Donner ces deux classes.
- À quelle classe appartient la technique assyrienne?
- Chiffrer un message qui contient votre nom et votre prénom par la technique assyrienne avec la matrice M(5,4)

Exercice 4 :

- Soit le texte clair (représenté en Héxadécimal) :

  i = 3243f6a8885a308d313198a2e0370734

  Et la clé (représentée en Héxadécimal) :

  k = 2b7e151628aed2a6abf7158809cf4f3c

- Selon l'algorithme AES-128 :
  1. Donnez les tables d'états du message (texte clair) « i » et de la clé « k ».
  2. Donnez la table d'état courant obtenue après l'application de chacune de ces étapes :

a) L'addition initiale $i \oplus k$ définie par l'opération AddRoundKey.

b) L'opération « SubByte » appliquée sur le résultat de l'addition $i \oplus k$.

c) L'opération « ShiftRow » appliquée sur le résultat de l'opération « SubByte ».

3. Donnez le résultat de l'application de l'opération MixColumn sur la colonne suivante :

$$\begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix}$$

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

- Représentation numérique des lettres de l'alphabet :

- Table de Vigenère

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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