Faculté Des Sciences
Département informatique
Module : Sécurité Informatique **Licence ISIL - 2022/2023**

Série TD 1
Cryptographie classique

Exercice 1 : CESAR
Le système le plus ancien est attribué à Jules César. Il consiste à un décalage de l'alphabet (dans le système original A étais remplacé par C, B par D, C par E, …)
1. voici un texte chiffré obtenu avec la clé H :

SLUUL TPLZA ZBWWV ZLHCV PYAVB
ALXBP WLTLU AZWLJ PHSUL JLZZH
PYLWV BYPUA LYJLW ALYSL ZZPNU
HBEAY HUZTP Z

1- Retrouver le texte clair

Voici un autre texte chiffré ; on ne connaît pas ici la clé utilisée.

FYPYQ LYELO TEUPD LTDOP DAZPX
PDFYP YQLYE LOTEY ZYDLT DOPDA
ZPDTP D

2- Retrouver le texte clair.

Exercice 2. Chiffrement par transposition

Considérons le chiffre par transposition sur l'alphabet latin de 26 lettres (de A à Z) comme l'illustre le tableau suivant.
La taille de la clé = taille du bloc = 6.

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

(a) Alphabet latin avec indices.

1	6	4	3	2	5
M	E	S	S	A	G
E	S	E	C	R	E
T	A	C	H	I	F
F	R	E	R	P	A
R	T	R	A	N	S
P	O	S	I	T	I
O	N				

(b) Matrice de transposition de l'exemple.

Par exemple, en utilisant la clé k = 164325 et le message clair M =« MESSAGE SECRET A CHIFFRER PAR TRANSPOSITION », nous obtenant le cryptogramme C =« METFRPO ARIPNT SCHRAI SECERS GEFASI ESARTON» comme l'illustre la matrice en haut.

1- Combien de clés peuvent être composées de ce cryptosystème ?
2- Quel est le cryptogramme C correspondant au texte clair M = « MATHEMATIQUES ET INFORMATIQUE » et la clé k = « 356124 » ?

3- Quel est le texte clair M correspondant au cryptogramme C = « USCCLSETFEIESTCSEADEXCENA » et la clé k = « 356124 » ?

Exercice 3. Chiffrement de Vigenère

1. Chiffrer le texte clair "thissystemisnotsecure", on donne m= 6 avec le mot-clé, CIPHER.
2. Ce cryptogramme a été obtenu par chiffrement de vigenère avec la clé « COPIE».

TWTVR GGTZX FSRWY TWGQP HOJBT
CFIQV CZWMY TS

1- Retrouver le texte clair.

Exercice 4. Chiffrement de Vigenère

Un message m est chiffré par le chiffrement de Vigenère avec une clé K_0

Cette clé est à son tour chiffrée par Vigenère avec la clé K_1: **OR**

On donne le chiffré de m : **KOADOLP** et le chiffré de la clé K_0 : **XRBLOIM**

1- Déchiffrer m.

	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	D
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	C
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	B
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