Université de Tlemcen Année Universitaire 2020-2021 Faculté des Sciences Département Informatique	Module Sécurité Informatique L3

Cryptographie classique

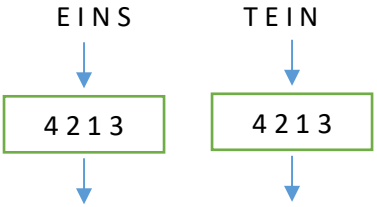
Exercice n° 1

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" ?

1	2	3	4
E	I	N	S
T	E	I	N

Le message chiffré : SNIEETNI

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) ?



Le chiffré : SIENNETI

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.

C=(M+K) mod 26
C1=(E+5)mod26= (4+5)mod26=9=J
C2=(I+5) mod 26=(8+5)mod 26=13=N
C3=(N+5)mod26=(13+5)mod26=18=S
C4=(S+5)mod26=(18+5)mod26=23=X
C5=(T+5)mod26=(19+5)mod26=24 =Y

C6=(E+5)mod26= J
C7=(I+5)mod26=N
C8=(N+5)mod26= S
EINSTEIN--------→ JNSXYJNS

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

2. Déchiffrer le message " SJBYTS" sachant qu'il a été créé par un chiffrement par décalage dont la clé K=5.

M=m1m2m3m4m5m6m7m8

C=c1c2c3c4c5c6c7c8

C=(M+k) mod 26 chiffrement

M =(C-K) mod 26 déchiffrement

M1= (S-5) mod 26=(18-5) mod26= 13= N

M2=(J-5)mod 26= (9-5)mod26=4=E
M3=(B-5)mod26=(1-5)mod26= -4 mod26 = (-4+26)mod26=22=W
M4=(Y-5)mod26=(24-5)mod26=19=T
M5=(T-5)mod26=(19-5)mod26=14=O
M6=(S-5)mod26=(18-5)mod26=13=N

SJBYTS--------→ NEWTON

Université de Tlemcen Année Universitaire 2020-2021 Faculté des Sciences Département Informatique	Module Sécurité Informatique L3

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 : $K=\begin{matrix}2 & 5\\ 1 & 4\end{matrix}$

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 $Y_1=K*X_1$, $Y_2=K*X_2$, $Y_3=K*X_3$ 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

Chiffrement : C=K*M

M= m1m2m3m4

C=c1c2c3c4

$\begin{matrix}c1\\ c2\end{matrix}=K*\begin{matrix}m1\\ m2\end{matrix}$ mod26

M=CODAGE

M=X1X2X3

X1=CO, X2=DA, X3=GE

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

$Y1=\begin{matrix}2 & 5\\ 1 & 4\end{matrix} * \begin{matrix}2\\ 14\end{matrix} \text{ mod } 26 = \begin{matrix}22\\ 6\end{matrix} \rightarrow \begin{matrix}W\\ G\end{matrix}$

$Y2=\begin{matrix}2 & 5\\ 1 & 4\end{matrix} * \begin{matrix}3\\ 0\end{matrix} \text{ mod } 26 = \begin{matrix}6\\ 3\end{matrix} \rightarrow \begin{matrix}G\\ D\end{matrix}$

$Y3=\begin{matrix}2 & 5\\ 1 & 4\end{matrix} * \begin{matrix}6\\ 4\end{matrix} \text{ mod } 26 = \begin{matrix}6\\ 22\end{matrix} \rightarrow \begin{matrix}G\\ W\end{matrix}$

Codage -----→WGGDGW

Chiffrement : C= K* M

Déchiffrement : $M=K^{-1}*C$ / K^{-1} est la matrice inverse de K

$K=\begin{matrix}2 & 5\\ 1 & 4\end{matrix}$

K^{-1}= ?

$K=\begin{matrix}a & b\\ c & d\end{matrix}$

K^{-1}= $1/\det(k) * \begin{matrix}d & -b\\ -c & a\end{matrix}$

Det (k)= a*d- b*c= 2*4-1*5=8-5=3

K^{-1}= $1/3 * \begin{matrix}4 & -5\\ -1 & 2\end{matrix}$

K^{-1}= $3^{-1} * \begin{matrix}4 & -5\\ -1 & 2\end{matrix}$

On doit calculer le modulo inverse de 3 mod 26

On suppose **u** est le modulo inverse de 3 mod 26

→U*3= 1 mod26 ⇔ 3u +26 v =1

Pour calculer le modulo inverse d'un nombre on utilise la division euclidienne étendue

D=26

d=3

r !=1

D=d

d=r

D=26,,, d=3

26/3=8 , r= 2 !=1

D=d=3

d=2

26=8*3+ 2 ------→2=26- 3 * 8

3=2*1 + 1 ---→ 1= 3- 2*1

1=3- (26-3*8)*1

1= 3 -26*1 +3*8

1=3*9 – 26*1

1=3*u + 26*v

U=9

L'inverse modulaire de 3 mod 26 =9

K^{-1}= $3^{-1} * \begin{matrix} 4 & -5 \\ -1 & 2 \end{matrix}$ mod26

K^{-1}= $9 * \begin{matrix} 4 & -5 \\ -1 & 2 \end{matrix}$ mod26

K^{-1}= $\begin{matrix} 36 & -45 \\ -9 & 18 \end{matrix}$ mod26

K^{-1}= $\begin{matrix} 10 & 7 \\ 17 & 18 \end{matrix}$

4. Déchiffrer le message 'WGGDGW' en utilisant la même clé K pour vérifier que ça redonne le message d'origine

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

$M1=\begin{matrix}10 & 7\\ 17 & 18\end{matrix} * \begin{matrix}W\\ G\end{matrix} \text{mod} 26 = \begin{matrix}10 & 7\\ 17 & 18\end{matrix} * \begin{matrix}22\\ 6\end{matrix} \text{mod} 26 = \begin{matrix}2\\ 14\end{matrix} \rightarrow \begin{matrix}C\\ O\end{matrix}$

$M2=\begin{matrix}10 & 7\\ 17 & 18\end{matrix} * \begin{matrix}G\\ D\end{matrix} \text{mod} 26 = M2=\begin{matrix}10 & 7\\ 17 & 18\end{matrix} * \begin{matrix}6\\ 3\end{matrix} \text{mod} 26 = \begin{matrix}3\\ 0\end{matrix} \rightarrow \begin{matrix}D\\ A\end{matrix}$

$M3=\begin{matrix}10 & 7\\ 17 & 18\end{matrix} * \begin{matrix}G\\ W\end{matrix} \text{mod} 26 = M2=\begin{matrix}10 & 7\\ 17 & 18\end{matrix} * \begin{matrix}6\\ 22\end{matrix} \text{mod} 26 = \begin{matrix}6\\ 4\end{matrix} \rightarrow \begin{matrix}G\\ E\end{matrix}$

WGGDGW----------→ CODAGE