Série de TD № 1

Exercice n°1 :

Rappelons la correspondance entre l'alphabet classique et les entiers {0,…, 25}:

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) Un cryptosystème basé sur le décalage crypte le mot CAHIER en HFMNJW. De quelle façon sera crypté le mot *livre* ?
2) Soient M = CRYPTOLOGIEMODERNE, le message en clair et K = 3 (chiffre de Jules César) la clé de chiffrement.

a- Chiffrer le message M.
b- Déchiffrer le message chiffré obtenu comme résultat à la question précédente.
c- Quelle remarque peut-on tirer entre le message M et le chiffré correspondant.

3)

a- Chiffrez le texte 'CRYPTHOGRAPHIE' en utilisant la substitution arbitraire 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*
X	R	O	E	B	C	Z	P	M	G	Y	U	L	H	J	Q	D	A	T	S	F	W	I	V	N	K

b- Quelle est la clef de cet algorithme de chiffrement ?
4) Prenons le message M = LECRYPTOGRAPHE.

Q- Trouver le chiffrement de M avec un chiffrement par substitution avec la clé :
SMOIDTGKXYCRHBPLZJQVWNFUAE

Exercice n° 2 :

Soit M = LECRYPTOGRAPHE un message en clair.

1) Trouver le chiffré, C, de M avec un chiffrement de Vigénère en utilisant la clé K = XYZ.
2) A partir de C trouvez le message original correspondant.
3) Que peut-on remarquer ?

Exercice n°3 :

1) Chiffrer avec le chiffre de Vigenère le texte suivant : "textesecretadecoder" en utilisant comme clé k = crypto.
2) Pour le même texte en clair, on obtient le texte chiffré suivant : "brqksmzcspxiqxtcxzr". Quelle est la clé ?
3) Même question si le chiffré est : "aaabbbcccdddeeefffg". Que remarque-t-on ?

Exercice n°4 :

Décoder le message suivant encodé par le protocole de Vigenère avec une clé de longueur 2 :

OSFFBDWCJFDAPSGSYWJSQSUSQSVHSZXGFCQ
GLRHFHRHBRGMCXFVQRAPSXBSFRHRQRZHGXF

(Note : les espaces et signes de ponctuation ont été supprimés.)

Exercice n° 5 :

Un chiffrement par substitution permute les caractères de l'alphabet. Dans un chiffrement par transposition, les symboles du message demeurent inchangés, mais leur ordre est permuté par une permutation des positions d'indice. A la différence de chiffrements par substitution, les chiffrements par transposition sont des chiffrements par blocs.
Considérons le message en clair m = INFORMATIQUE.

1) Trouver le chiffrement de m avec un chiffrement par transposition utilisant la clé k = [3,2,1,4].
2) Soit C un message chiffré

C = AEUFQ RUTRI QSUTX MEANE YNNAU DEESX OAUTX NUTAX

a- Trouvez le message en clair M avec la clé K = 5x8, lecture des colonnes 2-1-8-4-3-7-5-6
b- Chiffrez le message trouvé M avec transposition complexe par colonnes avec la clé K = ECRITURE et selon l'ordre alphabétique des caractères de la clé.

Université de Jijel
Département d'Informatique

M1 : ILM / R&S
Module : Cryptologie I / Cryptographie

Série de TD № 2

Exercice n°1 :

On considère un diagramme de Feistel à deux rondes sur des chaînes de 8 bits avec deux fonctions f_1 et f_2. On pose :

$$f_1(a) := a \oplus 1011 \quad \text{et} \quad f_2(a) := \bar{a} \oplus 0101$$

pour toute chaîne a de 4 bits.

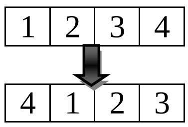
1) Calculer l'image de la chaîne 11010011 par ce diagramme.
2) Déterminer une chaîne de 8 bits dont l'image par le diagramme est elle-même.

Exercice n° 2 :

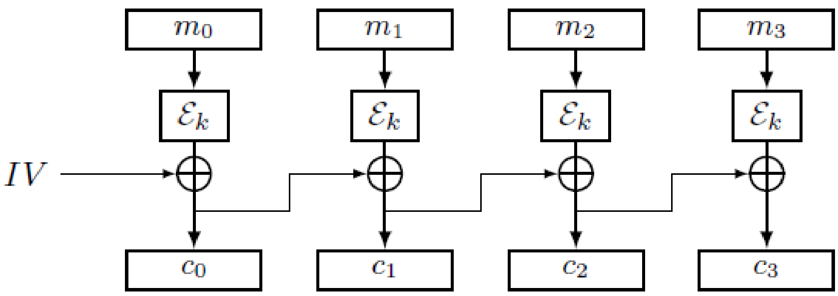
On utilise un schéma de Feistel où la clef de tour est toujours la même et la fonction de codage f_k est le xor avec k.
Quelles sont les faiblesses de ce schéma en fonction du nombre de tours ?

Exercice n° 3 :

1) Soient M = 1110010111001100 message en clair et une clé K = (1 := 4, 2 :=1, 3 :=2, 4 :=3) par permutation. Chiffrez le message M en utilisant le mode ECB.



2) Soit VI = 1110 vecteur d'initialisation. Chiffrez le message M en utilisant le mode CBC puis OFB.
3) Soit le mode de chiffrement illustré par la figure suivante, et soit VI = 1110 le vecteur d'initialisation.



a. Discuter les résultats de chiffrement si m2=m3.
b. Chiffrez le message M en utilisant ce mode.

Exercice n° 4 :

On considère une fonction de chiffrement par bloc de longueur 2 pour des clefs de longueur 2 donnée par :

$$\begin{array}{rcc} E_k : \{0,1\}^2 & \to & \{0,1\}^2 \\ (m_1, m_2) & \mapsto & S_1((m_1 \oplus k_1, m_2 \oplus k_2)) \end{array}$$

où la fonction S1 est décrite ci-dessous.

X	$[0,0]$	$[1,0]$	$[0,1]$	$[1,1]$
$S_1(X)$	$[1,1]$	$[1,0]$	$[0,0]$	$[0,1]$

1) Chiffrer le message M = [0,1,1,1,0,1] avec la clef K = [1,0] et en utilisant :

- **(a)** le mode ECB
- **(b)** le mode OFB

2) Déchiffrer le message C = [0,1,1,1,0,1] dans le cas où il a été chiffré avec la clef K = [1,1] et en utilisant :

- **(a)** le mode CBC,
- **(b)** le mode CFB.

Exercice n° 5 :

Rappelons la correspondance entre l'alphabet classique et les entiers {0,…, 25}:

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

On s'intéresse ici à une utilisation du cryptosystème de Vigénère avec une clé de longueur *m* pour chiffrer un texte de plusieurs blocs de longueur *m* chacun.

Pour chiffrer le premier bloc B_0 du texte on utilise le chiffrement de Vigénère avec la clé privée K. Pour un bloc B_i arrivant à la position i > 0 dans le texte, on utilise le chiffrement de Vigénère en prenant comme clé le chiffré du bloc B_{i-1}.

1) Représenter le chiffrement et le déchiffrement d'un texte de n blocs de longueur m à l'aide de deux schémas.

2) A l'aide de ce cryptosystème, chiffrer le texte INFORMATIQUE avec la clé K = UP.

Université de Jijel
Département d'Informatique

M1 ILM / R&S
Module : Cryptologie I / Cryptographie

Série de TD № 3

Exercice n°1 :

On considère le système RSA avec p = 19 et q = 23.

1) Calculer n et $\varphi(n)$.
2) Déterminer l'exposant a associé à b=9, b=14, puis b=5.
3) Calculer le chiffré associé au message m=42 quand b=5.
4) Déchiffrer le message c=264 avec la clé a correspondante à b=5.

Exercice n°2 :

1) Chiffrer le message "25" avec la clé publique RSA (b=13,n=77). Le calcul peut être facilement fait en remarquant que 25^4 mod 77 = 4.
2) Sachons que n= 11×7= 77, calculer la clé privée associée à la clé publique (b=13,n=77). Le calcul peut se faire facilement en remarquant que : 13×37=481 et 8×60=480.
3) Déchiffrer le message obtenu à la question (1) afin de trouver le message clair.

Exercice n°3 :

Soit à chiffrer le message X = 6882326879666683 en utilisant l'algorithme RSA avec la clé publique (79, 3337). Pour pouvoir le déchiffrer, on procède à une factorisation de n en deux nombres de m chiffres.

1) Quelle est la valeur maximale de m ?
2) Le bloc codé 6325 peut-il résulter d'un codage avec la clé publique ? Même question avec la clé privée.