Université d'Alger1
Faculté Des Sciences
Département informatique
Module : Sécurité des systèmes d'information **Licence ISIL - 2021/2022**

Série TD 2

Cryptographie symétrique

Exercice 1

Exécuter le schéma de Feistel à deux étapes pour le chiffrement des blocs suivants :
1101, 1001, 1110, 0001, 0010

Utilisez les fonctions f1 pour le première étape et f2 pour la deuxième étape.

entrée	f_1	sortie	entrée	f_2	sortie
00	→	01	00	→	11
01	→	11	01	→	00
10	→	10	10	→	00
11	→	01	11	→	01

Exercice 2

Modes opératoires des chiffrements par blocs.
Soit le message clair m=101100010100101. On considère le chiffrement par blocs (de longueur 4) définit par la permutation (qui fait alors à la fois office de clé et de fonction de chiffrement).

b1b2b3b4 -> b2b3b4b1

1- Chiffrer m avec le mode ECB
2- Chiffrer m avec le mode CBC (on prend 1010 comme vecteur d'initialisation).
3- Chiffrer m avec le mode CFB (on prendra des blocs de longueurs r=4 et IV=1010)
4- Chiffrer m avec le mode OFB (on prendra des blocs de longueurs r=4 et IV=1010)
5-

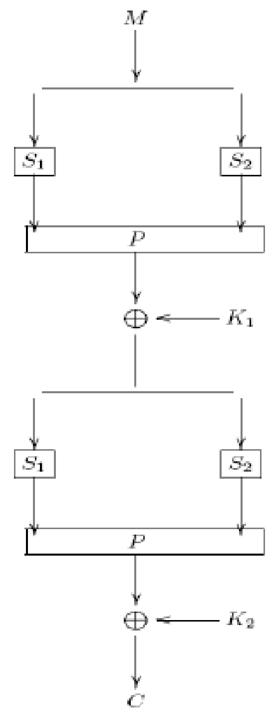
Exercice 3.

Notons m_1, m_2, $\cdots m_n$ les lettre d'un message M. Le message chiffré est donné par les lettres $c_1, c_2, \cdots, c_n$ avec **$c_1=m_1+k \bmod 26$ et pour $i\geq 2$ $c_i=m_i+c_{i-1} \bmod 26$**

k est la clé de chiffrement.
Chiffrer le message « MESSAGE » avec la clé k= C
Trouvez la fonction de déchiffrement.
NB. Les lettres de l'alphabet sont numérotées de 0 à 25 (A=0, B=1 ...)

Exercice 4.

Soit le crypto système suivant :



Sachant que les boites S1 et S2 sont données par

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

Que les clés de ronde se déduisent de la clé de chiffrement K= (k1, k2, k3, k4) par

$$K1= (k1\oplus k2,k2,k3 \oplus k4,k3),K2=(k1 \oplus k2 \oplus k3,k2 \oplus k3,k3 \oplus k4,k4)$$

Et que la permutation P est définit par

$$P(1)=3,\ P(4)=2,\ P(2)=1,\ P(3)=4.$$

Chiffrer le message M=(0,1,1,0) avec K=(1,1,1,1) et déchiffrer le message C = (0,1,0,1) chiffré avec la même clé.

<u>Cryptographie Asymétrique</u>

Exercice 5.

1. Appliquer l'algorithme d'Euclide pour déterminer si les nombres 67 et 60 sont premiers entre eux.
2. Appliquer l'algorithme d'Euclide étendu pour calculer 17^{-1} mod 50
3. Calculer 51447^{21} mod 17

Exercice 6.

On considère un module RSA n =pq, ou p et q sont les inconnus.

1. Montrer simplement comment la connaissance de $\phi(n)$ (la fonction d'Euler) permet de remonter à la factorisation de n.
2. Soit n =pq=84773093 un produit de deux nombres premiers. On sait que $\phi(n)$= 84754668. Retrouver les deux facteurs premiers p et q de n.
3. Soit n =pq=851 un produit de deux nombres premiers. On sait que $\phi(n)$=792. Retrouver les deux facteurs premiers p et q de n.

Exercice 7.

Chiffrer et déchiffrer le message x dans les cas suivants (par l'algorithme de cryptage RSA)

(i) $x = 5234673$ si Bob choisit $p = 2357$, $q = 2551$ et $b = 3674911$.

(ii) $x = 9726$, si $p = 101, q = 113$

Exercice 8. (RSA)

Chiffrer le texte ITS ALL GREEK FOR ME à l'aide de petits nombres par l'algorithme de cryptage RSA. q=59, p=47.

Exercice 9.

Supposant qu'Alice souhaite transmettre le message x= 1299 à Bob par l'algorithme de cryptage El-Gamal.
Sachant que : p=2579, g=2, a=765 et A=949
Décrivez le protocole d'échange en donnant le résultat de calcule de chaque étape.