Université d'Alger1
Faculté Des Sciences
Département Mathématiques – Informatique
Module : Sécurité des systèmes d'information Licence ISIL - 2020/2021

TD2
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
00	→	01
01	→	11
10	→	10
11	→	01

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

Exercice 2

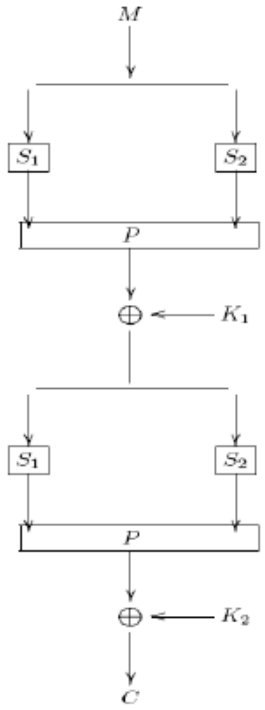
Modes opératoires des chiffrements par blocs.
Soit le message clair m= 101100010100101.On considère le chiffrement par blocs (de longueur 4) définit par la permutation (qui fait alors a la fois office de clé et de fonction de chiffrement).

$$b_1b_2\,b_3b_4 \longrightarrow b_2b_3b_4b_1$$

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

Exercice 3

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⊕ k2,k2,k3 ⊕ k4,k3),K2=(k1 ⊕ k2 ⊕ k3,k2 ⊕ k3,k3 ⊕ 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.