Université de M'sila
Faculté de MI
Département d'informatique

TD N° 03

Niveau: 3ème année Licence

Module: Sécurité Informatique

Exercice N° 01: *Schéma de Feistel*

1. Ecrire les formules de chiffrement avec le schéma de Feistel selon l'itération *i*,
2. Ecrire les formules de déchiffrement avec ce schéma selon l'itération *i*,
3. Dessiner ce schéma pour le chiffrement
4. Appliquer ce schéma sur:
   - Le bloc: 11010110
   - La clé: 1010
   - F(x,k)= x or k
   - $K_i = k_{i-1}$ xor 1011
   - Nombre d'itérations: 3.

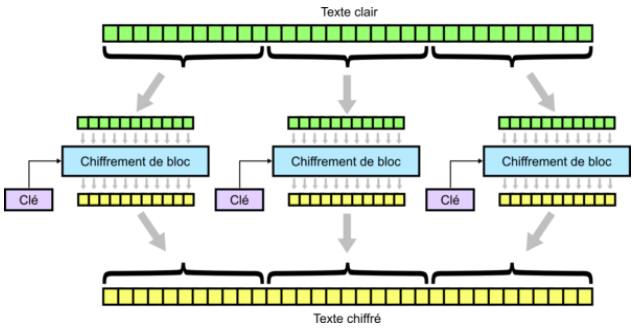
Exercice N° 02: *AES*

1. Définir les quatre transformations de l'AES
2. Appliquer SubBytes à l'octet (01001001).
3. Appliquer ShiftRow au tableau:

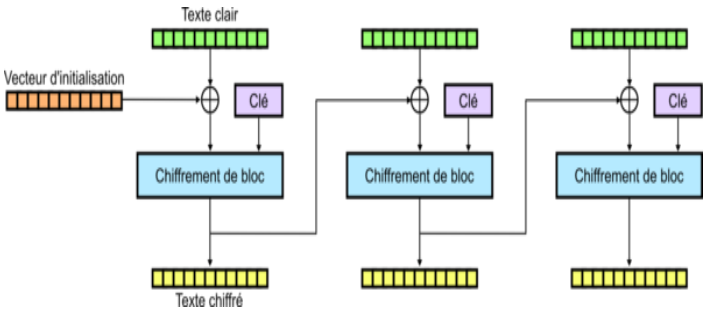
(11000001) (00000111) (00000000) (11111111)
(11000000) (00001000) (00011110) (11111100)
(11000011) (00000100) (00000001) (11100000)
(10001001) (00000110) (11000000) (00010111)

Exercice N° 03: *Modes d'opération*

Soient les schémas des modes d'opération de chiffrement symétrique :



(1) ECB



(2) CBC

1. Le mode **ECB** :
   - Dessiner le schéma de déchiffrement.
   - Déduire les fonctions de chiffrement / déchiffrement.
   - Quel est le problème de ce mode ?
   - Soient le message en clair M = 101100011011101 et la clé K = (f(4)=1, f(3)=4, f(2)= 3, f(1)=2) est correspondance un décalage à gauche de 1 bit. Chiffrez le message M.
2. Le mode **CBC** :
   - Dessiner le schéma de déchiffrement.
   - Déduire les fonctions de chiffrement / déchiffrement.
   - Soient le vecteur d'initialisation VI = 1010, le message en clair M = 101100011011101, et la clé K = (f(4)=1, f(3)=4, f(2)= 3, f(1)=2) est correspondance une décalage à gauche de 1 bit. Chiffrez le message M.