University of M'sila
Faculty of MI
Department of Computer Science

TD N° 03

Level: 3rd year Bachelor's degree

Course: Computer Security

Exercise N° 01: *Diagram of Feistel*

1. Write the encryption formulas with the Feistel scheme according to iteration *i*,
2. Write the decryption formulas with this scheme according to iteration *i*,
3. Draw this scheme for encryption
4. Apply this scheme for:
   - The block: 11010110
   - The key (K_0): 1010
   - F(x,k)= x or k
   - $K_i = k_{i-1}$ xor 1011
   - Number of iterations: 3.

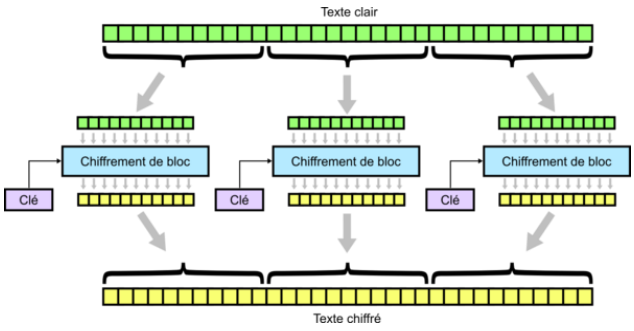
Exercise N° 02: *AES*

1. Define the four transformations of the AES
2. Apply SubBytes to byte (9c).
3. Apply ShiftRow to the table:

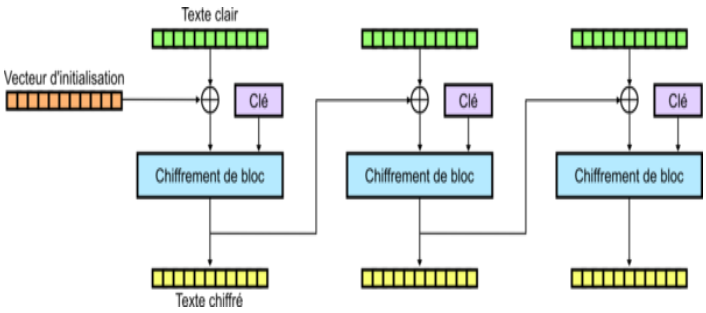
34	9a	aa	01
f4	00	0e	67
89	ff	fb	5th
00	e4	cc	c5

Exercise N° 03: *Modes of operation*

Be the schemas of symmetric encryption operation modes:



(1) ECB



(2) CBC

1. The ECB mode:

- Draw the decryption diagram.
- Deduce the encryption/decryption functions.
- Let the plaintext message M = 101100011011101 and the key K = (f(4)=1, f(3)=4, f(2)= 3, f(1)=2) be a left shift by one position. Encrypt the message M.
- What is the problem with this mode?

2. The CBC mode:

- Draw the decryption diagram.
- Deduce the encryption/decryption functions.
- Let the initialization vector VI = 1010, the plaintext message M = 101100011011101, and the key K = (f(4)=1, f(3)=4, f(2)= 3, f(1)=2) be a left shift by one position. Encrypt the message M.