MODES DE CRYPTAGE PAR BLOCS

Exercice 1 : ECB

On considère un cryptosystème de bloc qui applique une permutation à des vecteurs binaires de taille 4 en mode ECB.

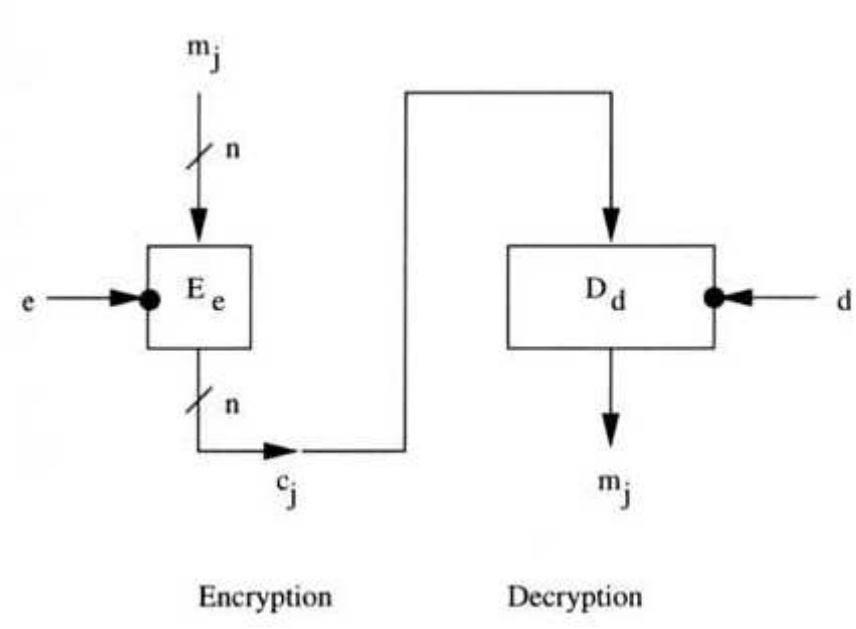


Fig : ECB mode

La fonction de permutation π est defini comme suit :

$b_1 b_2 b_3 b_4 \rightarrow b_{\pi(1)} b_{\pi(2)} b_{\pi(3)} b_{\pi(4)}$

On donne l'operation de permutation :

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Soit le plaintext m :

m = 101100010100101

1) Decrire mathematiquement ou avec un pseudo-code le fonctionnement de ECB.
2) decomposer le plaintext en bloc de taille approprié. Faire du bourrage avec des zeros pour avoir des bloc de meme taille
3) Appliquer le mode ECB lors du chiffrement des blocs du plaintext
4) Donner le ciphertext final
5) Appliquer le dechiffrement et verifier avec le message original
6) Considerer un plaintext formé par les memes blocs 1010, cette redondance est-elle propagé dans le ciphertext ?
7) Si l'ordre des blocs des ciphertexts est modifié ? le décryptage de chaque bloc est il possible ?
8) Que pensiez vous de la securité de ECB et dans quel application est il approprié ?

Exercice 2: CBC

On utilise ma meme clé, le meme plaintext, la meme opération mais en mode CBC. On donne IV=1010

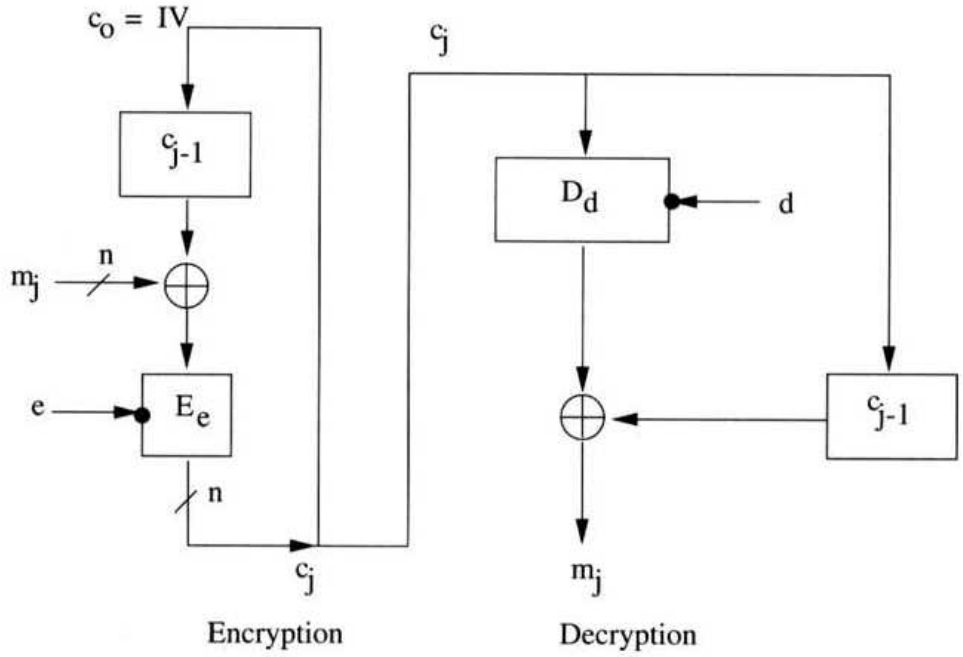
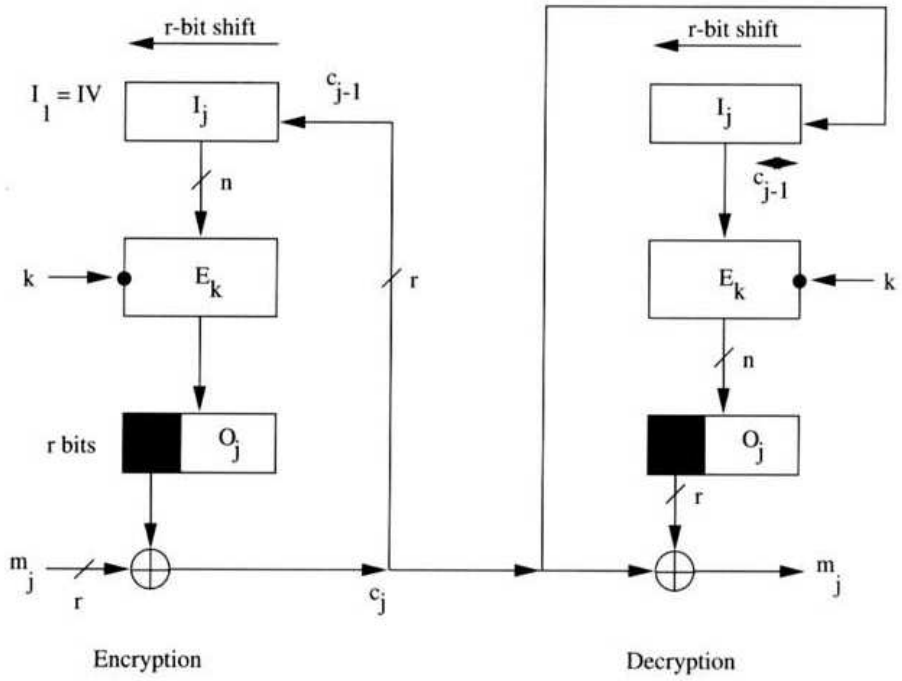


Fig : CBC mode

1) Decrire mathematiquement ou avec un pseudo-code le fonctionnement de CBC.
2) decomposer le plaintext en bloc de taille approprié. Faire du bourrage avec des zeros pour avoir des bloc de meme taille
3) Appliquer le mode ECB lors du chiffrement des blocs du plaintext
4) Donner le ciphertext final
5) Appliquer le dechiffrement et verfier avec le message original
6) Considerer un plaintext formé par les memes blocs 1011, cette redondance est-elle propagé dans le ciphertext ?
7) Si l'ordre des blocs des ciphertexts est modifié ? le décryptage de chaque bloc est il possible ?
8) Que pensiez vous de la securité de CBC et dans quel application est il approprié ?
9) Si une erreur se passe dans le premier bloc du ciphertext. Etudier la propagation d'erreur sur le décryptage (dire quels sont les blocs affectés et les blocs intacts du plaintext).
10) Dire quel application CBC est approprié

Exercice 3 : CFB

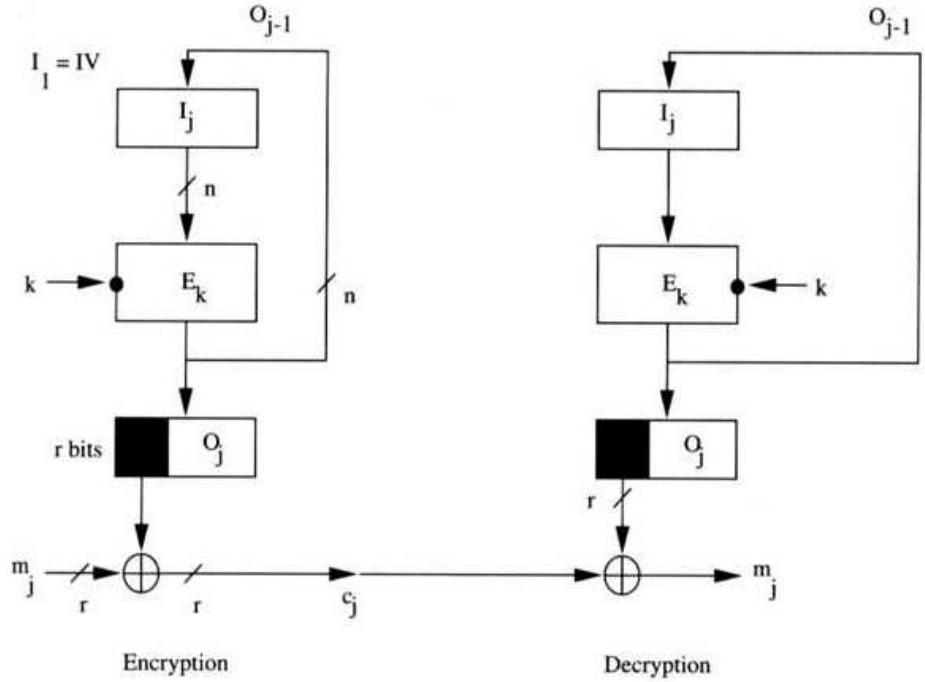
Dans CFB, on a besoin d'un IV et aussi un entier r avec $1 \leq r \leq$ n. le plaintext sera decomposé en blocs de r. Et Initialisation de I_1= IV



Refaire l'exercice avec la meme operation de permutation E, meme plaintext et meme IV, on donne aussi r =3.

Exercice 4 : OFB

OFB est tres similaire à CFB



Refaire l'exercice avec les memes Plaintext, clé, IV, r que CFB. Analyer la propagation d'erreur, la sécurité de OFB et sa rapidité.