Département d'informatique
Sécurité Informatique **2025-2026**
Dr F.Khalifa

TD4

Chiffrement Symétrique
(Chiffrement par blocs et chiffrement par Feistel)

Exercice 1 :

Soit le message en clair m=101100010100101. On considère le chiffrement par blocs de longueur =4, définit par la permutation (qui fait 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 prendra 1010 comme vecteur d'initialisation)
3. Chiffrer m avec le mode CFB

Exercice 2 :

Le mode de chiffrement ECB (Electronic Code Book ou Dictionnaire de code) est le mode de chiffrement le plus simple que l'on puisse imaginer : chaque bloc de données est chiffré indépendamment par la fonction de chiffrement.

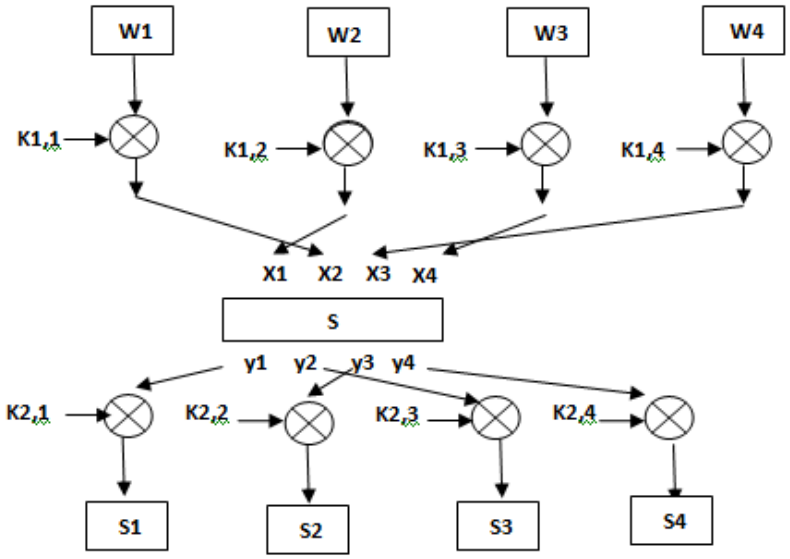
1. Expliquer pourquoi ce mode de chiffrement est déconseillé.
2. youcef, qui gagne 105000 Da par an, a retrouva l'entée chiffrée qui lui correspond dans la base de donnée des salaires de son entreprise :

   Q92DT8FPVXC9IO

   Sachant que la fonction de chiffrement utilisé a des blocs de deux caractères, et que la base de données utilise le nom suivi par deux blancs et par le salaire, le service informatique de son entreprise utilise le mode ECB, retrouver le salaire de Younes la patronne de youcef dans cette base de données :

   TOAV6RFPY5VXC9, YPFGFPDFDFIO, Q9AXU8FPC9IOIO, ACED4TFPVXIOIO, UTJSDGFPRTAVIO.

Exercice 3 : On considère le crypto système E sur 4 bits suivant :



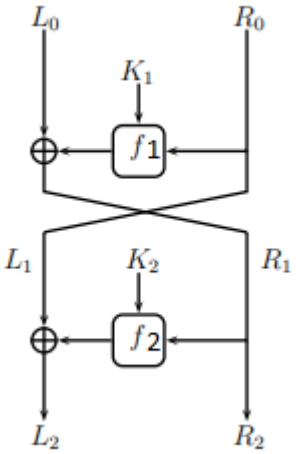
La S-boite est donnée par le tableau suivent (entrée : x1x2x3x4, sortie : y1y2y3y4)

1. Calculer l'image du mot 1011 par le crypto système E ; k1=0110 et k2= 1110

x1x2x3x4	y1y2y3y4	x1x2x3x4	y1y2y3y4	x1x2x3x4	y1y2y3y4	x1x2x3x4	y1y2y3y4
0000	1110	0100	0010	1000	0011	1100	0101
0001	0100	0101	1111	1001	1010	1101	1001
0010	1101	0110	1011	1010	0110	1110	0000
0011	0001	0111	1000	1011	1100	1111	0111

Exercice 4 : Réseau de Feistel

Le réseau de Feistel de la figure suivante travaille sur un tour de 8 bits :



La fonction f prend en entrée une sous clé de 4 bits K_{i+1} et une donnée de 4 bits :

$f: \{0,1\}^4 \times \{0,1\}^4 \rightarrow \{0,1\}^4$

$f(K_{i+1}, R_i) = P\big(S(K_{i+1} \oplus \mathrm{R_i})\big)$

Ou S est une boîte-S donnée par la table suivante :

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S(X)	8	6	7	9	3	12	10	15	13	1	14	4	0	11	5	2

Et $P: \{0,1\}^4 \rightarrow \{0,1\}^4$ est une permutation bit par bit donnée par :

$$p = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \end{pmatrix}$$

1. Chiffrer le message m = 163 avec les sous-clés K1 = 7 est K2 = 12