(Cryptographie Symétrique : DES)

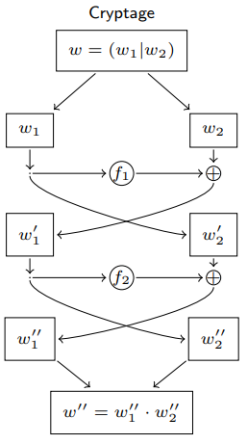
Exercice 1 :

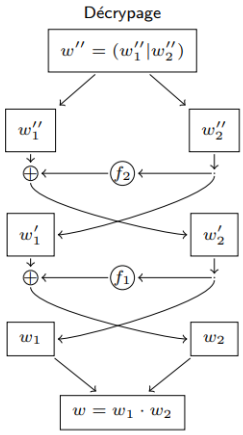
On considère maintenant des chaînes de 8 bits avec deux fonctions f_1 et f_2 définies pour toute chaîne m de 4 bits par les formules suivantes :

$$f_1(m) = m \oplus 1011 \quad et \quad f_2(m) = \bar{m} \oplus 0101,$$

où $\bar{m}$ vérifie la relation $m + \bar{m} = 1111$.

1) Calculer l'image de la chaîne *11010011* par ce diagramme.
2) Peut-on trouvé une chaîne de *8* bits invariante cette fois-ci.

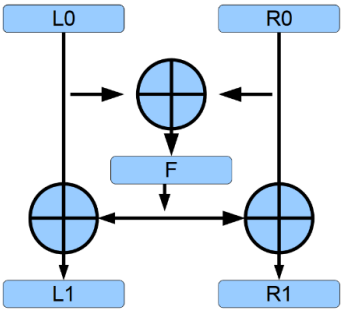




Exercice 2 :

IDEA est un algorithme de chiffrement par blocs. Il utilise des clefs de *128* bits et chiffre des blocs de *64* bits. Il utilise le schéma de Feistel modifié suivant :

1) Comparer la taille des blocs et des clefs entre l'algorithme IDEA et DES?
2) Exprimez L1 et R1 en fonction de L0 et R0 (Chiffrement).
3) Exprimez L0 et R0 en fonction de R1 et de L1(Déchiffrement).



Exercice 3 :

Soit M un message divisé en blocs $\{x_1,x_2,x_3,\ldots x_p\}$chacun de taille n bits et soit K une clé de même taille que les blocs (n bits). Soit $\{c_1,c_2,c_3,\ldots c_p\}$les cryptogrammes des blocs obtenus en appliquant la clé K aux blocs.

Le chiffrement des blocs se fait selon le schéma suivant:

$$C_0 = \text{IV (valeur initiale) ;} \qquad \text{pour j de 1 à p, } C_j = E_K(C_{j-1} \oplus x_j)$$

1) La fonction E_K est inversible et son inverse est D_K. Montrer que l'opération de déchiffrement est
$$x_j = C_{j-1} \oplus D_K(C_j)$$
2) Peut-on chiffrer un bloc quelconque x_j sans chiffrer les blocs qui le précèdent ? Expliquer?
3) Peut-on déchiffrer un bloc quelconque c_j sans déchiffrer les blocs qui le précèdent ? Expliquer ?
4) Peut-on déchiffrer un bloc c_j en l'absence des autres blocs chiffrés ? Expliquer ?

5) Prenons le cas où $E_K(x)=D_K(x) = K \oplus x$. Supposons qu'un attaquant a pu récupérer deux blocs consécutifs (x_{j-1},x_j) ainsi que leurs cryptogrammes correspondants (c_{j-1},c_j). Montrer que cet attaquant peut en déduire la clé de chiffrement K.

Exercice 3

On considère le cryptosystème défini par la Figure 1. Les boites S_1 et S_2 sont données par :

X	$[0,0]$	$[1,0]$	$[0,1]$	$[1,1]$
$S_1(X)$	$[1,1]$	$[1,0]$	$[0,0]$	$[0,1]$
$S_2(X)$	$[1,0]$	$[0,1]$	$[1,1]$	$[0,0]$

Les clefs de ronde se déduisent de la clé de chiffrement $K = [k_1, k_2, k_3, k_4]$ par :

$$K_1 = [k_1 \oplus k_2, k_2, k_3 \oplus k_4, k_3], \quad K_2 = [k_1 \oplus k_2 \oplus k_3, k_2 \oplus k_3, k_3 \oplus k_4, k_4]$$

La permutation P est définie par :

$$P(1) = 3,\ P(4) = 2,\ P(2) = 1,\ P(3) = 4$$

Chiffrer le message $M = [0, 1, 1, 0]$ avec $K = [1, 1, 1, 1]$. Déchiffrer le message $C = [0, 1, 0, 1]$ chiffré avec la même clé.

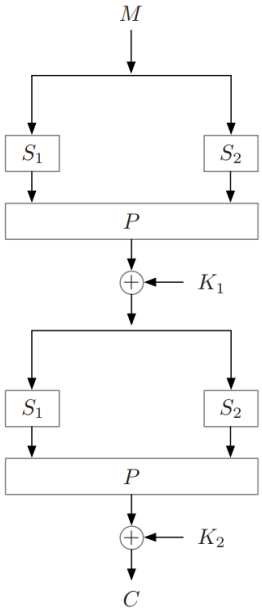


Figure 1: Cryptosystème