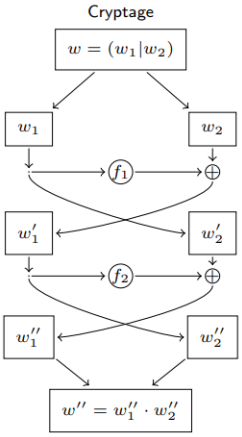
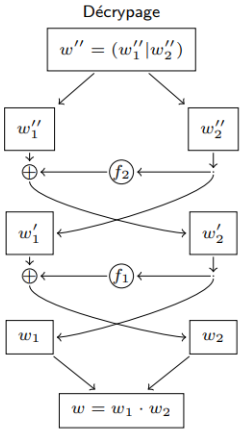
(Cryptographie Symétrique : DES)

Exercice 1 :

On considère un diagramme de Feistel sur des mots binaires de 4 bits à deux rondes où les fonctions f1 et f2 sont les suivantes : on rappel **A⊕B= B⊕A, A⊕0=A, A⊕A=0**

f_1	$00 \mapsto 00,$	$01 \mapsto 10,$	$10 \mapsto 00,$	$11 \mapsto 00$
f_2	$00 \mapsto 11,$	$01 \mapsto 11,$	$10 \mapsto 10,$	$11 \mapsto 11$





1) Donner l'expression de w1 et w2 à la sortie du Diagramme.

2) Crypter le mot 1001 en utilisant ce diagramme.
3) Y a t-ils existent des mots de 4 bits qui sont invariants (Sortie = Entrée) par ce diagramme de Feistel.

Exercice 2 :

On considère le diagramme de Feistel précédent à deux rondes sur des chaînes de 8 bits avec deux fonctions f_1 et f_2 (associées à des clés K_1 et K_2) définies pour toute chaîne a de 4 bits par les formules suivantes :

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

où $\bar{a}$ désigne la négation de a, i.e. $a + \bar{a} = 1111$.

1) Calculer l'image de la chaîne 11010011 par ce diagramme.
2) Déterminer une chaîne de 8 bits dont l'image par le diagramme est elle-même.
3) La propriété précédente, l'existence d'une chaîne invariante par le diagramme de Feistel, est-elle vraie pour toutes les fonctions f_1 et f_2 ?

Exercice 3 :

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) Que pensez-vous de la taille des blocs et des clefs d'IDEA comparés à DES?
2) Chiffrement : Exprimez L1 et R1 en fonction de L0 et R0.
3) Déchiffrement : Exprimez L0 et R0 en fonction de R1 et de L1.