Université Mohammed V-Agdal
Faculté des Sciences de Rabat

Département d'Informatique

Année Universitaire 2021-2022
Master IPS
(Sécurité & Cryptographie)

Série de TD n° 2
Chiffrement de Feistel

Exercice :1

un processus de Feistel permet de chiffrer un message M de 2n bits (on considère en général des messages de 64 ou 128 bits).

- M est découpé en deux parties L_0 et R_0 de longueur n (parties gauche et droite du message)
- A l'aide d'une fonction f_1 de $\{0,1\}^n$ vers $\{0,1\}^n$, les parties L_0 et R_0 sont transformées en
  $L_1 = R_0$ et $R_1 = L_0 \oplus f_1(R_0)$

  1) Montrer que La transformation $(L_0 , R_0) \rightarrow (L_1 , R_1)$ est bijective et déterminer sa réciproque .

  2) En déduire que pour tout entier n>1 le schèma de Feistel à n rondes est une bijection qui associe à chaque (L_0, R_0) un et seul (Ln, Rn)

Exercice :2

On considère le diagramme de Feistel, sur des mots binaires de 4 bits à 2 rondes où les fonctions f_1 et f_2 sont données dans le tableau ci-dessous **:**

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

1. Crypter le mot 1111 en utilisant ce diagramme.
2. Trouver tous les mots de 4 bits qui sont invariants par ce diagramme de Feistel.
3. Encrypter le message binaire suivant par ce diagramme de Feistel en utilisant le mode CBC avec pour IV le mot 0000 :

1000 1101 0011 1110