UNIVERSITÉ LAVAL

Chapitre III : exercices + solutions

MOHAMED MEJRI

Groupe LSFM

Département d'Informatique et de Génie Logiciel

Université LAVAL

Québec, Canada

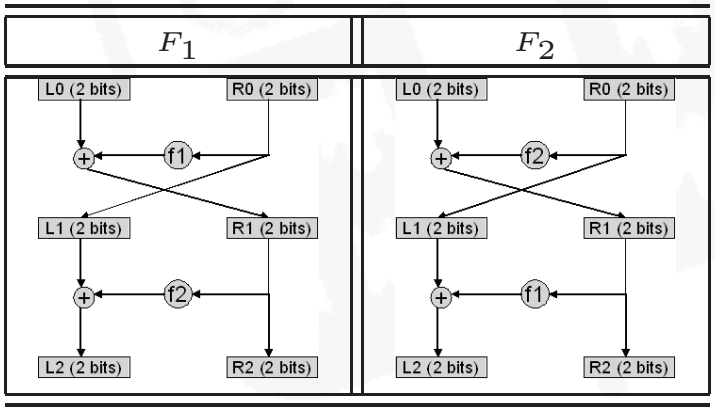
Chiffrement de Feistel

- Soient les deux fonctions f_1 et f_2 suivantes :

Entrée	f_1	Sortie	Entrée	f_2	Sortie
00	$\longrightarrow$	01	00	$\longrightarrow$	11
01	$\longrightarrow$	11	01	$\longrightarrow$	00
10	$\longrightarrow$	10	10	$\longrightarrow$	00
11	$\longrightarrow$	01	11	$\longrightarrow$	01

  - Q1 : Est ce que f_1 et f_2 sont des fonctions inversibles ?

- Soient les deux fonctions F_1 et F_2 suivantes :



  - Q1 : Determiner pour chaque valeur d'entrée la valeur de sortie donnée par F_1 (resp. F_2).
  - Q2 : Est ce que F_1 et F_2 sont des fonctions inversibles ? Dans le cas positif, donner leurs inverses.

Chiffrement de Feistel

Solution :

- $f_1(00) = f_1(11) = 01$ donc f_1 n'est pas inversible. De même, puisque $f_2(01) = f_2(10) = 00$ donc f_2 n'est pas inversible.
- $F_1(L_0, R_0) = L_2, R_2$ avec L_2 et R_2 sont données par le tableau suivant :

	L_0, R_0	$f_1(R_0)$	$L_1 = R_0$	$R_1 = L_0 \oplus f_1(R_0)$	$f_2(R_1)$	$L_2 = L_1 \oplus f_2(R_1)$	$R_2 = R_1$	
0	00, 00	01	00	01	00	00	01	1
1	00, 01	11	01	11	01	00	11	3
2	00, 10	10	10	10	00	10	10	10
3	00, 11	01	11	01	00	11	01	13
4	01, 00	01	00	00	11	11	00	12
5	01, 01	11	01	10	00	01	10	6
6	01, 10	10	10	11	01	11	11	15
7	01, 11	01	11	00	11	00	00	0
8	10, 00	01	00	11	01	01	11	7
9	10, 01	11	01	01	00	01	01	5
10	10, 10	10	10	00	11	01	00	4
11	10, 11	01	11	11	01	10	11	11
12	11, 00	01	00	10	00	00	10	2
13	11, 01	11	01	00	11	10	00	8
14	11, 10	10	10	01	00	10	01	9
15	11, 11	01	11	10	00	11	10	14

Chiffrement de Feistel

– $F_2(L_0, R_0) = L_2, R_2$ avec L_2 et R_2 sont données par le tableau suivant :

	L_0, R_0	$f_2(R_0)$	$L_1 = R_0$	$R_1 = L_0 \oplus f_2(R_0)$	$f_1(R_1)$	$L_2 = L_1 \oplus f_1(R_1)$	$R_2 = R_1$	
0	00, 00	11	00	11	01	01	11	7
1	00, 01	00	01	00	01	00	00	0
2	00, 10	00	10	00	01	11	00	12
3	00, 11	01	11	01	11	00	01	1
4	01, 00	11	00	10	10	10	10	10
5	01, 01	00	01	01	11	10	01	9
6	01, 10	00	10	01	11	01	01	5
7	01, 11	01	11	00	01	10	00	8
8	10, 00	11	00	01	11	11	01	13
9	10, 01	00	01	10	01	11	10	14
10	10, 10	00	10	10	10	00	10	2
11	10, 11	01	11	11	01	10	11	11
12	11, 00	11	00	00	01	01	00	4
13	11, 01	00	01	11	01	00	11	3
14	11, 10	00	10	11	01	11	11	15
15	11, 11	01	11	10	10	01	10	6

– D'après les valeurs de sorties de F_1 et de F_2, on voit bien que ces deux fonctions sont inversibles et que $F_1^{-1} = F_2$ et $F_2^{-1} = F_1$.

DES

- Question : Soit $K = 133457799BBCDFF1$ une clé (en hexadecimal).

  Trouver la clé K_1 générée par DES.

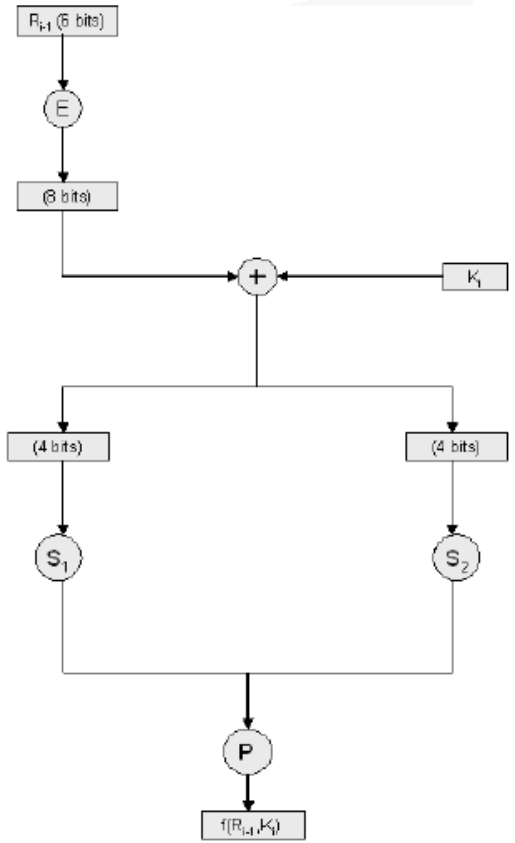
- Solution

  $K = 0001\ 0011\ 0011\ 0100\ 0101\ 0111\ 0111\ 1001$
  $1001\ 1011\ 1011\ 1100\ 1101\ 1111\ 1111\ 0001$

  - $C_0 = 1111\ 0000\ 1100\ 1100\ 1010\ 1010\ 1111$
  - $D_0 = 0101\ 0101\ 0110\ 0110\ 0111\ 1000\ 1111$
  - $C_1 = 1110\ 0001\ 1001\ 1001\ 0101\ 0101\ 1111$
  - $D_1 = 1010\ 1010\ 1100\ 1100\ 1111\ 0001\ 1110$
  - $K_1 = 0001\ 1011\ 0000\ 0010\ 1110\ 1111\ 1111\ 1100\ 0111\ 0000\ 0111\ 0010$

Chiffrement de Feistel : DES simplifié

Supposons que $R_3 = 011\ 100$ et $K = 0100\ 11001$, calculer $f(R_3, K_4)$



$E(b_1b_2b_3b_4b_5b_6)=b_1b_2b_4b_3b_4b_3b_5b_6$

$$K = \underbrace{b_1 b_2 b_3 b_4 b_5 b_6 b_7 b_8 b_9}_{9bits}$$

$$K_i = \underbrace{b_i b_{i+1} \ldots b_1 \ldots}_{8bits}$$

S_1=
100 010 001 110 011 100 111 000
001 100 110 010 000 111 101 011

S_2=
100 000 110 101 111 001 011 010
101 011 000 111 110 010 001 100

$S_i(b_1b_2b_3b_4)=S[b_1,b_2b_4b_3]$

$P(b_1b_2b_3b_4b_5b_6)=b_3b_2b_6b_1b_4b_5$

Solution :

$E(R_3) = 0111\ 1100, K_4 = 0110\ 0101, E(R_3) \oplus K_4 = 0001\ 1001$
$S_1(0001) = S_1[0, 2] = 001, S_2(1001) = S_2[1, 2] = 000$
$P(001000) = 100\ 000 \Longrightarrow f(R_3, K_4) = 100\ 000$