UNIVERSITÉ LAVAL

Chapitre III : exercices

MOHAMED MEJRI

Groupe LSFM

Département d'Informatique et de Génie Logiciel

Université LAVAL

Québec, Canada

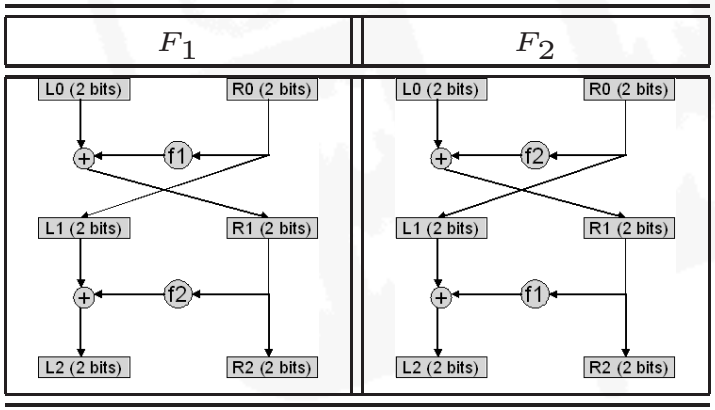
Chiffrement de Feistel

- 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.

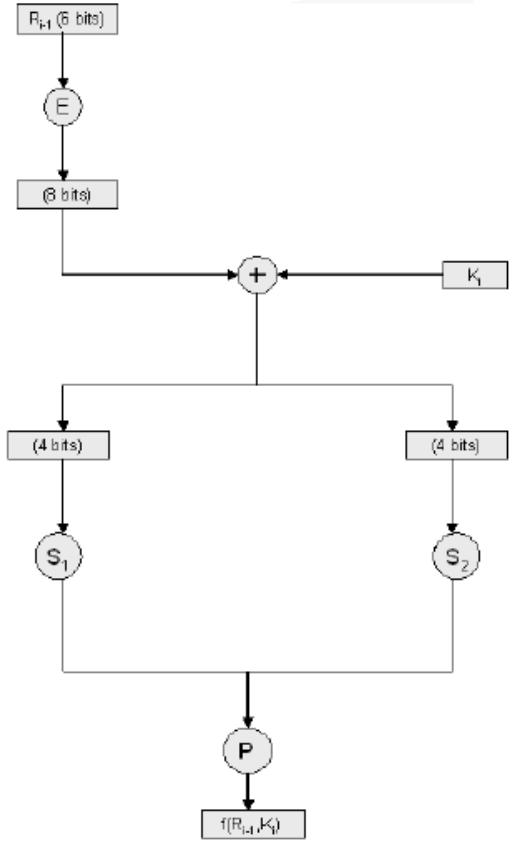
DES

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

  Trouver la clé K_1 générée par DES.

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

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

$P(b_1b_2b_3b_4b_5b_6)=b_3b_2b_6b_1b_4b_5$