Université Abdelhamid Ibn Badis Mostaganem
Faculté des Sciences Exactes et Informatique
Département de mathématiques et informatique

Licence 3 informatique
Matière : Cryptographie
Année universitaire : 2019/2020

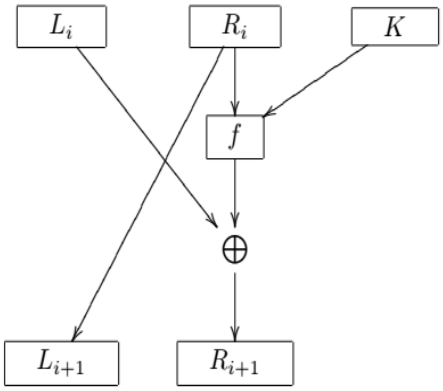
TD N°4

Exercice : Calculer le chiffrement du message $M = A0E0$ après deux rondes du miniDES et la clef $K = 07E$.

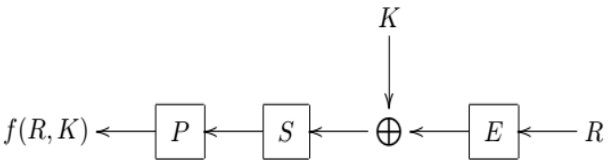
MiniDES

L'algorithme MiniDES est chiffrement à bloc suivant un shéma de Feistel. Il chiffre des messages de 16 bits en un autre bloc de 16 bits avec une clef de longueur 12bits. Il manipule des clés individuelles de ronde 12 bits.

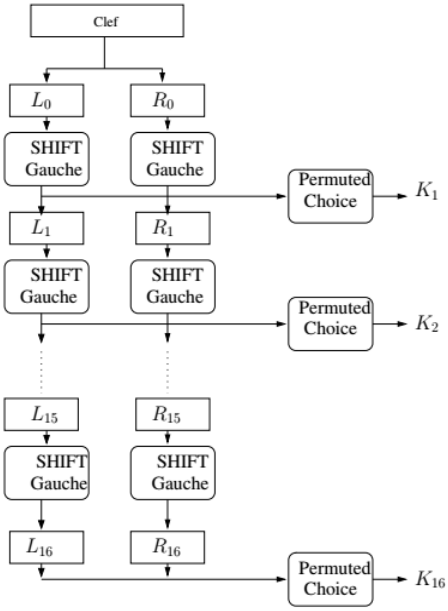
Une ronde



La fonction de ronde



La diversification de la clef de rondes du DES



Permuted Choice (PC)

8	7	1	4	10	5
3	9	2	12	6	11

SHIFT = décalage cyclique de 1 pour les rondes $1, 2, 9, 16$ et décalage de 2 sinon.

La permutation initiale PI

10	12	14	16	9	11	13	15
2	4	6	8	1	3	5	7

La permutation finale PF

13	9	14	10	15	11	16	12
5	1	6	2	7	3	8	4

La fonction d'expansion E

8	1	2	3	4	5
4	5	6	7	8	1

La permutation P

2	8	4	7
6	5	3	1

Les S-boites définissant S

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Corrigé du TD N°4

Remarque: Mini DES est une version miniature du DES (vu au cours) donc au lieu d'avoir 16 rondes (itérations), on va dérouler 2 rondes seulement et de chercher 2 sous-clés.

1) On doit convertir la valeur du message M et la clé principale K en binaire, on aura :

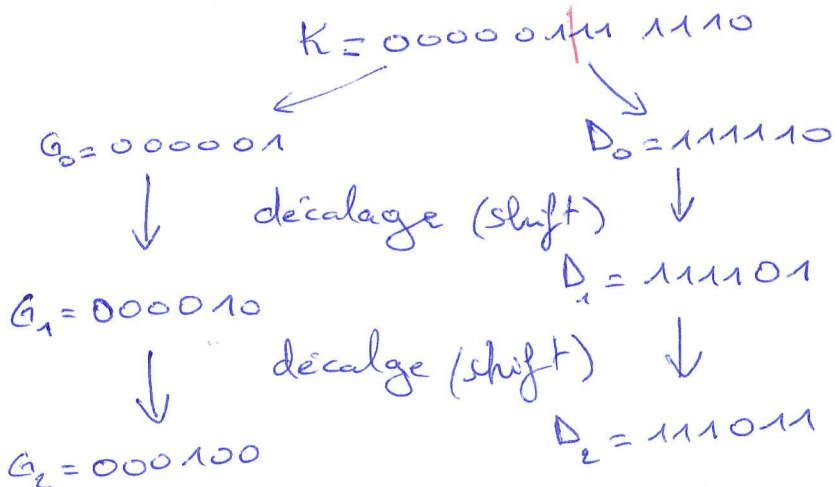
M = 1010 0000 1110 0000 (sur 16 bits)

K = 0000 0111 1110 (sur 12 bits)

2) Générations des sous clés K_1 et K_2.

* Il faut prendre en considération la note donnée en bas de page concernant le décalage cyclique.

* Comme il est indiqué dans le schéma, la clé principale doit être divisé en deux (partie gauche et partie droite).



→ Pour K_1, on prend G_1/D_1 et on lui applique la permutation PC

PC (G_1 000010 D_1 111101) ⇒ K_1 = 110011010100

→ Pour K_2, on prend G_2/D_2 et on lui applique la permutation PC

PC (1 2 3 4 5 6 7 8 9 10 11 12 : 000100 111011) ⇒ 110100010101 = K_2

Remarque: Dans la permutation PC de K_2 par exemple : Dans le 1er bit qui porte N° 8 on va lui permuter par le 8ème bit qui est à 1, ainsi de suite ...

3) Chiffrement :

Suivant le schéma donné au cours le message en clair doit subir en premier une permutation initiale, puis le chiffrement de Feistel. et enfin une permutation finale.

A) Permutation initiale :

On applique sur le message M la permutation PI fournie dans l'exercice présent.

$$M = 1010\,0000\,1110\,0000$$

$$\downarrow PI$$

$$PI(M) = \underbrace{1000\,1100}_{G_0} \,|\, \underbrace{0000\,1100}_{D_0}$$

B) Chiffrement de Feistel :

Comme il est illustré dans la figure d'une ronde, la partie droite va toujours subir une transformation en utilisant la fonction f

E : Expansion de la partie droite

$\oplus$: Xor avec la clé de ronde (K_1 ou K_2)

S : Substition en utilisant S-box.

P : Permutation.

On a : $G_1 = D_0 \Rightarrow \boxed{G_1 = 0000\,1100}$

$D_1 = G_0 \oplus f(D_0, K_1) \Rightarrow$ On doit d'abord calculer $f(D_0, K_1)$ selon les étapes mentionnées ci-dessus.

* Expansion E :

$E(D_0) = 0000\,0101\,1000$

* Xor K_1 :

$E(D_0) \oplus K_1$: $0000\,0101\,1000$

$\oplus 1100\,1101\,0100$

$1100\,1000\,1100$

$B_1 \quad B_2$

* S-boxs

On a $B_1 = \overset{b_1\ b_2\ b_3\ b_4\ b_5\ b_6}{1\ 1\ 0\ 0\ 1\ 0}$

$b_1 b_6 = 10$ en décimal c'est (2)

$b_2 b_3 b_4 b_5 = 1001$ en décimal c'est (9)

On fait l'intersection entre la 2ème ligne et la 9ème colonne de S_1

$\Rightarrow S_1(B_1) = 12$ en binaire c'est 1100

→ On fait la même chose avec B_2 :

On a $B_2 = \overset{b_1\ b_2\ b_3\ b_4\ b_5\ b_6}{0\ 0\ 1\ 1\ 0\ 0}$

$b_1 b_6 = 00$ en décimal (0)

$b_2 b_3 b_4 b_5 = 0110$ en décimal (6)

$\Rightarrow S_2(B_2) = 3$ en binaire 0011

On note $B' = 11000011$ (concaténation entre $S_1(B_1)$ et $S_2(B_2)$)

* Permutation :

$P(B') = 11010001$ ⇒ résultat de $f(D_0, K_1)$

On avait : $D_1 = G_0 \oplus f(D_0, K_1)$

$\Rightarrow D_1 = \begin{cases} 1000\ 1100 \\ \oplus\ 1101\ 0001 \end{cases} \Rightarrow D_1 = 0101\ 1101$

→ Pour la 2ème ronde on va faire la même chose que la première.

On a : $D_1 = G_2 \Rightarrow G_2 = 01011101$

$D_2 = G_1 \oplus f(D_1, K_2)$ donc on va calculer $f(D_1, K_2)$

* Expansion :

$E(D_1) = 10101111 1010$

* Xor K_2 : $\begin{array}{r} 110100010101 \\ \oplus \\ \hline 011111 \mid 101111 \end{array}$

B_1 B_2

* S Box :

On $B_1 = \overset{b_1\ b_2\ b_3\ b_4\ b_5\ b_6}{0\ 1\ 1\ 1\ 1\ 1}$

$b_1 b_6 = 01$ en décimal (1)

$b_2 b_3 b_4 b_5 = 1111$ en décimal (15)

⇒ intersection dans S_1

$S_1(B_1) = 8$ en binaire 1000

On a $B_2 = b_1 b_2 b_3 b_4 b_5 b_6 = 101111$ $\begin{cases} b_1 b_6 = 11 & \text{en décimal } (3) \\ b_2 b_3 b_4 b_5 = 0111 & \text{en décimal } (7) \end{cases}$ → intersection dans S_2

Alors : $S_2(B_2) = 2$ en binaire $\boxed{0010}$

Donc $B' = 10000010$ (concaténer $S_1(B_1)$ et $S_2(B_2)$)

* Permutations ↓

$P(B') = 00010001$ ⇒ résultat de $f(D_1, K_2)$

On avait : $D_2 = G_1 \oplus f(D_1, K_2)$ ⇒ $\begin{cases} 00001100 \\ \oplus\ 00010001 \end{cases}$

$\Rightarrow D_2 = 00011101$

On rassemble maintenant G_2 et D_2 on aura :

$C' = 0101\overset{G_2}{1101}\ \overset{D_2}{00011101}$

c) Permutation finale :

$PF(C') = C = 1010001110110011$ (Message chiffré)