Centre universitaire - Salhi Ahmed - de Naâma

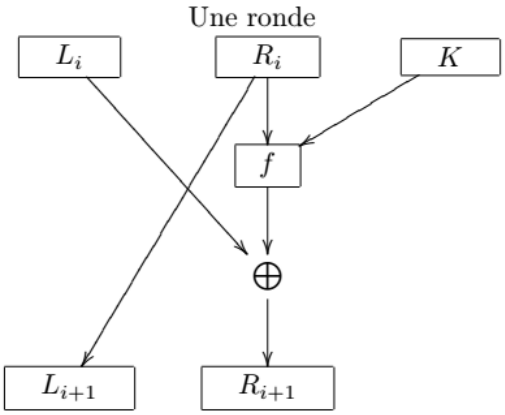
Institut des sciences et de la Technologie
Département : Mathématiques et Informatique
3ème Année Licence Informatique
Matière : Sécurité Informatique

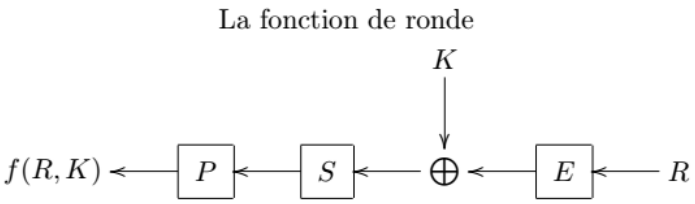
Fiche TD : 03

Exercice 01 :

1) Quels sont les éléments intervenants dans un système de chiffrement symétrique ?
2) Qu'est-ce qu'un algorithme de chiffrement par blocs ?
3) Quels sont les algorithmes principaux utilisés ?
4) Qu'est-ce qu'un schéma de Feistel ?
5) Comment utilise-t-on généralement un algorithme de chiffrement symétrique par blocs ? Pourquoi ? Quels sont les modes d'utilisation courants ?
6) Que signifie DES ?
7) Qu'est-ce qui compose l'algorithme DES ?
8) Expliquez la procédure de génération des sous-clés Ki dans DES.
9) Pour quelles raisons DES a-t-il été remplacé ? Par quoi ?

Exercice 02 : Soit l'algorithme MiniDES un chiffrement par bloc suivant le schéma de Feistel. Il chiffre des messages de 16 bits en un autre bloc de 16 bits avec une clé de longueur 12 bits. Il manipule des clés de ronde de 12 bits.





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

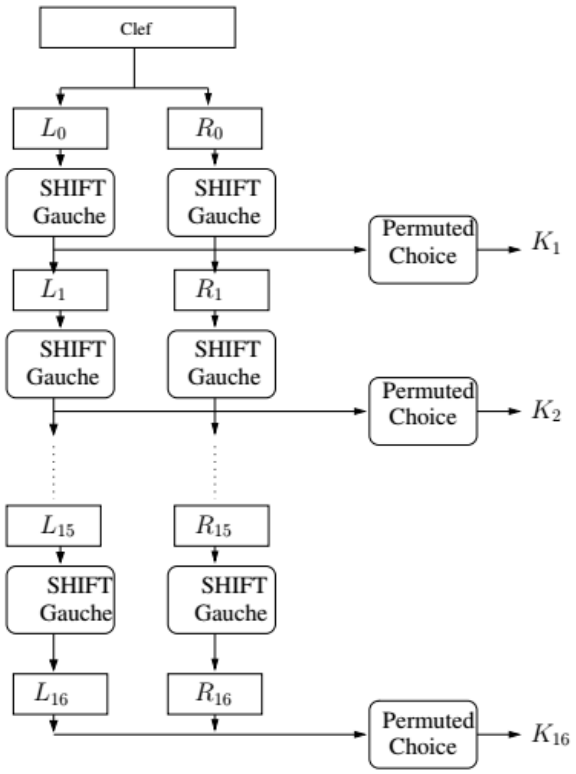
2	8	4	7
6	5	3	1

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

La diversification de la clé de ronde de MiniDES :



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.

Question : Calculez le chiffrement du message M = A0E0 après deux rondes du miniDES et la clef K = 07E.

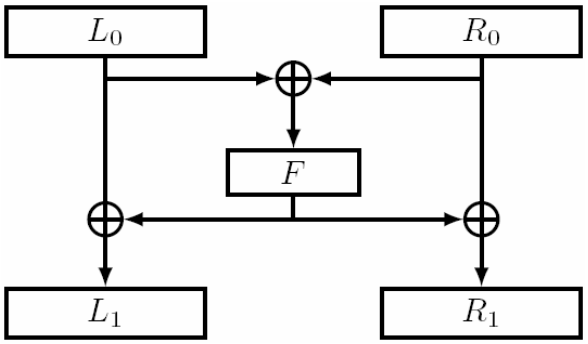
Exercice 03 : Le principe général des algorithmes de chiffrement par blocs (block cypher) est de séparer le message en mots de taille fixe, et appliquer l'algorithme de chiffrement pour chaque bloc en utilisant un « mode d'opération ».

1) Le mode ECB (Electronic Code Book)
   a) Déterminez deux fonctions une pour le chiffrement et l'autre pour le déchiffrement.
   b) Quel est le problème de ce mode ? Proposez une solution pour ce problème ?

c) Soit M = 1011000101001011 un message en clair, et l'algorithme de chiffrement donné par la permutation P = (2, 3, 4, 1). Chiffrez le message M avec le mode ECB.

2) Le mode CBC (Cipher Block Chaining)
   a) Donnez les fonctions de chiffrement et de déchiffrement de ce mode.
   b) Soit VI = 1010 un vecteur d'initialisation. Chiffrez le message M avec le mode CBC, et avec le même algorithme de chiffrement (la permutation P).
3) CFB (Cypher FeedBack)
   a) Donnez les fonctions de chiffrement et de déchiffrement de ce mode.
   b) Chiffrez le message M avec le mode CFB, avec le même vecteur d'initialisation et le même algorithme de chiffrement (la permutation P).

Exercice 04 : Le schéma décrit ci-dessous est une variante du mécanisme de Feistel:



1) Écrire les équations donnant l'expression du chiffré L_1 et R_1 en fonction du clair L_0 et R_0.
2) Montrer que ce schéma est inversible quelle que soit la fonction F et donner les formules décrivant le déchiffrement.