Master 1ère année
Initiation à la Cryptographie

Travaux Dirigés

Data Encryption Standard

Exercice 1 :
Vérifier la parité de la clé D.E.S. suivante : `1ADEC028FF342A8B`. Corriger si nécessaire.

Exercice 2 :
Utiliser la table de permutation IP du DES pour chiffrer le texte suivant :
Lepetitchaperonrouge,quientenditlagrossevoixduloup,eutpeurdabord

Permutation Initiale (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Trouver la permutation permettant de déchiffrer le texte. Que vous rappelle-t-elle?
Rappel : pour utiliser cette permutation (chiffrement par transposition), il faut que cette matrice soit secrète, ce qui n'est pas le cas dans l'algorithme DES. Dans le DES, cette matrice fait intervenir des positions de bit et non des positions de lettre.

Exercice 3 :
Soit K =`133457799BBCDFF1`. Déterminer la sous-clé K_1.

PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Exercice 4 :
Quelle est la sortie de Sbox1 si l'entrée est 011001? 110011? Quelle(s) est(sont) l'entrée(s) possible(s) si la sortie de Sbox1 est 12?

S1

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

Exercice 5 :
Soit R (32 bits)=`AF3216A3` et K_1 (48 bits)=`B22BEE5B5ECC`. Calculer les 4 bits de sortie de la Sbox1.

Exercice 6 : (Stinson Ex 3.3 sur les clés faibles)
Une manière de renforcer le DES consiste à faire un double chiffrement : étant données deux clés K_1 et K_2, on définit $y = DES_{K_1}(DES_{K_2}(x))$. Si la fonction de chiffrement DES_{K_1} est la même que la fonction de déchiffrement $DES_{K_2}^{-1}$, les clés K_1 et K_2 sont dites duales. De telles clés sont indésirables, car le texte chiffré est toujours égal au texte clair. Une clé est auto-duale si elle est sa propre duale.
1) Montrer que si C_0 à tous ses bits identiques (à 0 ou à 1) et si D_0 aussi, alors K est auto-duale.
2) Montrer que les clés suivantes (en notation hexadécimale) sont auto-duales :

```
0101010101010101
FEFEFEFEFEFEFEFE
1F1F1F1F0E0E0E0E
E0E0E0E0F1F1F1F1
```

3) Montrer que si $C_0 = 0101\ldots01$ ou $1010\ldots10$ (en binaire), alors les ou-exclusif des chaînes C_i et C_{17-i} sont $11111\ldots11$ pour $1 \leq i \leq 16$ (On montre la même chose pour D)
4) Prouver que les paires de clefs suivantes (en hexadécimal) sont duales :

```
( E001E001F101F101 , 01E001E001F101F1 )
( FE1FFE1FFE0EFE0E , 1FFE1FFE0EFE0EFE )
( E01FE01FF10EF10E , 1FE01FE00EF10EF1 )
```

Exercice 7 : Cryptanalyse du DES (1 tour)
Considérons la fonction f du DES. Nous disposons de 2 couples correspondant aux 6 premiers bits de la sortie de l'expansion de R et aux 4 bits de sortie de Sbox1. Les valeurs sont (011111,9) (111011,6).
1) Retrouvez à quelles entrées peuvent correspondre les sorties 9 puis 6.
2) Retrouvez les deux ensembles de clés possibles.
3) Retrouvez les 6 premiers bits de la clé k_1.

Exercice 8 : Modes d'utilisation du DES

1. ECB (electronic codebook mode) Le mode bloc.
2. OFB (output feedback mode) Les entrées sont chiffrées avec une suite de clés (z_i). Les clés (z_i) applicables aux blocs successifs (x_i) sont générées à partir d'un vecteur d'initialisation IV et chiffrent le bloc par un ou-exclusif (y_i).
$$z_1 = DES_k(IV), \quad y_i = x_i \oplus z_i, \quad z_{i+1} = DES_k(z_i)$$
3. CBC (cipher block chaining mode) Le bloc en clair (x_i) est transformé avant chiffrement par le bloc chiffré précédent (y_{i-1}).
$$y_1 = DES_k(x_1 \oplus IV), \quad y_i = DES_k(x_i \oplus y_{i-1})$$
4. CFB (cipher feedback mode) Les clés générées dépendent du texte chiffré.
$$z_1 = DES_k(IV), \quad y_i = x_i \oplus z_i, \quad z_{i+1} = DES_k(y_i)$$

Représenter chaque chiffrement et son déchiffrement associé sous forme de diagramme.