Cryptographie de clé privée

0.1 Chiffrement par bloc [2]

Un procédé de chiffrement par bloc sur n bits est une fonction:

$$E : \{0,1\}^n \times K \to \{0,1\}^n$$

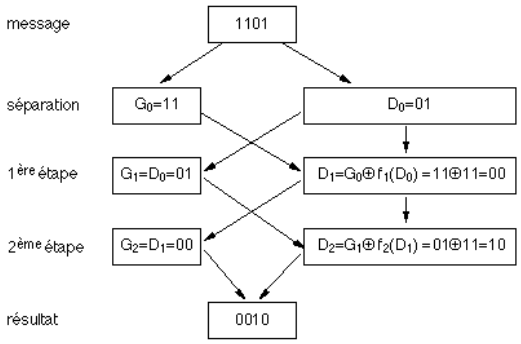
telle que pour toute clé $k \in K$, $E(.,k)$ est une bijection de $\{0,1\} \to \{0,1\}^n$ notée E_k.
Pour chiffrer un message m on sépare le texte en clair en blocs de même taille et puis on applique les transformations logique sur chaque bloc.
Le schéma de Feistel est considéré comme un cas particulier de cryptosystème de chiffrement par blocs. Dans ce cryptosystème de chiffrement on procède comme suit:

On définit deux fonction f_1 et f_2 telles que:

$$f_1 : \{0,1\}^2 \to \Big\{0,1\Big\}^2$$
$$00 \to 01$$
$$01 \to 11$$
$$10 \to 10$$
$$11 \to 11$$

$$f_2 : \{0,1\}^2 \to \Big\{0,1\Big\}^2$$
$$00 \to 11$$
$$01 \to 00$$
$$10 \to 00$$
$$11 \to 01$$

Le schéma de Feistel est le suivant:



Exemple .1. *Exemples sur le message en clair et le résultat après le schéma de Feistel:*

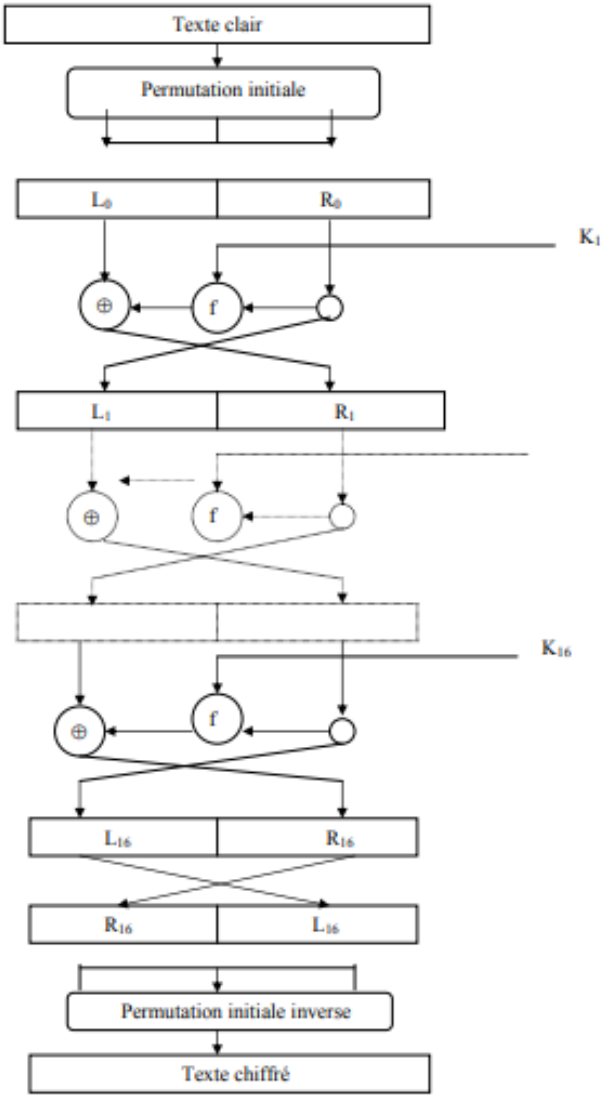
$$0000 \to 0100 \tag{1}$$
$$0111 \to 0000 \tag{2}$$
$$1001 \to 0101 \tag{3}$$

On remarque que ni f_1 ni f_2 est une bijection, mais en utilisant le schéma de Feistel on a pu construire une bijection à partir de f_1 et f_2.

0.2 Le chiffrement DES [1]

Le DES ou le Data Encryption Standard publié et adopté par le Bureau national de Standard en 1977 est considéré comme le cryptosystème le plus utilisé dans le monde.

Le principe de ce cryptosysème est de chiffrer un message de 64 bits avec une clé (secrète) de 56 bits en un message chiffré de 64 bits.
Les étapes de ce cryptosystème sont les suivantes:



- Une permutation initiale IP d'un bloc de 64 bits donnée par le tableau suivant:

- Après on sépare le message en deux parties de 32 bits L_0 et R_0 et on applique une fonction f bien définie (on appelle l'application une seule fois un tour),

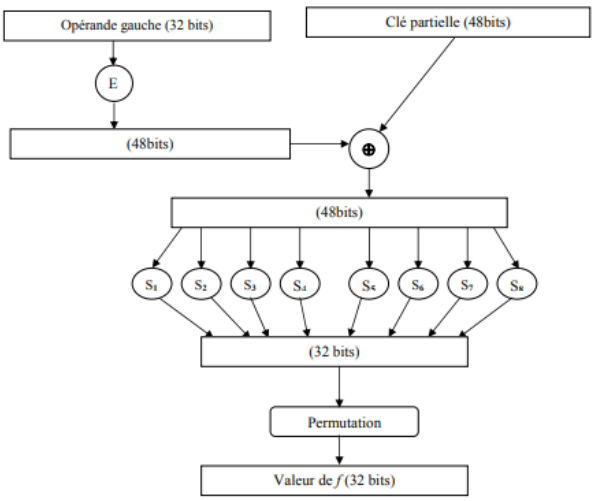
Permutation initiale

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

après chaque tour on obtient L_i et R_i deux parties de 32 bits On répète cette application 16 fois càd 16 tours en utilisant 16 clés partielles calculées de la clé K et les formules suivantes:

$$L_i = R_{i-1} \ et \ R_i = L_{i-1} \oplus f(R_{i-1}, K_i).$$

avec le schéma suivant:



Fonction E d'expansion

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

Permutation IP_{32} finale

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	23

Les huits S-boite suivantes permettent de calculer un bloc de 4 bits à partir d'un bloc de 6 bits.

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

S_3	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

- On applique l'inverse de l'application initiale IP^{-1} donnée par le tableau suivant:

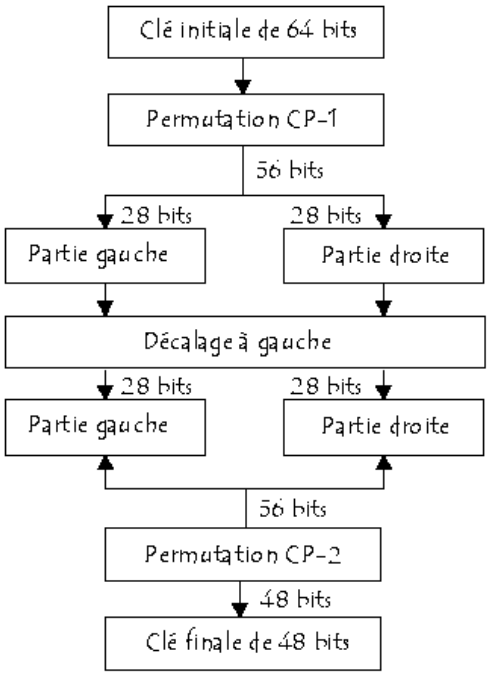
Permutation initiale inverse

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

Et on obtient le mot chiffré.

0.3 Génération des clés:

L'algorithme suivant montre comment on obtient les 16 clés.
On commence par avoir 8 clés différentes à partir d'une clé de 64 bits, en utilisant le schéma suivant [3]:



- Une permutation PC_1 pour avoir 56 bits en éliminant les bits de parité de

la clé donnée par le tableau suivant:

Permutation 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

- On obtient deux parties gauche G_i et D_i chaque partie est de 28 bits, commençant par G_0 et D_0, on applique une rotation à gauche à chaque partie telles que les bits en seconde position prennent la première, ceux de la troisième position prennent de la deuxième et les premiers bits prennent la dernière position.
  On regroupe les deux parties de 28 bits en un bloc de 56 bits et on applique une permutation PC_2 on obtient une clé K_i de 48 bits.

Règle d'extraction 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

A la fin on applique des itérations qui permettent d'obtenir 16 clés partielles de 48 bits.

0.3.1 Déchiffrement DES:

Pour déchiffrer, on doit appliquer les mêmes étapes de chiffrement en générant les clés partielles du chiffrement dans l'ordre inverse.

Bibliography

[1] S. Hamzaoui, Techniques de Cryptographie, Thèse de Magister, Université des sciences et de la technologie Houari Boumediene, 2004.

[2] https://www.apprendre-en-ligne.net/crypto/quantique/index.html

[3] https://web.maths.unsw.edu.au/ lafaye/CCM/crypto/des.htm