5.2.5 Clés

Finalement, il reste à expliquer comment sont calculées les chaînes de clés des tournées. Soit $k \in \{0,1\}^{64}$ une clé du DES, on va en déduire les clés des tournées K_i, $1 \leqslant i \leqslant 16$, de longueur 48. Pour cela, on définit des valeurs v_i, $1 \leqslant i \leqslant 16$, de la façon suivante.

$$v_i = \begin{cases} 1 & \text{pour } i \in \{1, 2, 9, 16\}, \\ 2 & \text{sinon.} \end{cases}$$

Le clés des tournées sont calculées par l'algorithme suivant qui utilise deux fonctions

$$\mathrm{PC1} : \{0,1\}^{64} \to \{0,1\}^{28} \times \{0,1\}^{28} \qquad \mathrm{PC2} : \{0,1\}^{28} \times \{0,1\}^{28} \to \{0,1\}^{48}$$

qui seront décrites plus loin.

1. On pose $(C_0, D_0) = \mathrm{PC1}(k)$.
2. Pour $1 \leqslant i \leqslant 16$:
   a) On note C_i la chaîne de caractères obtenue à partir de C_{i-1} par un décalage, en permutation circulaire, de v_i positions.
   b) On note D_i la chaîne de caractères obtenue à partir de D_{i-1} par un décalage, en permutation circulaire, de v_i positions.
   c) On pose $K_i = \mathrm{PC2}(C_i, D_i)$.

La fonction PC1 associe au mot binaire k de longueur 64 deux mots binaires C et D de longueur 28. Elle est définie par le tableau 5.6. La moitié supérieure de la table décrit C. Si $k = k_1 k_2 \ldots k_{64}$, alors $C = k_{57} k_{49} \ldots k_{36}$. La moitié inférieure de la table représente D, donc $D = k_{63} k_{55} \ldots k_4$. La fonction PC2 associe à un couple (C, D) de mots binaires de longueur 28, c'est-à-dire à un mot binaire de longueur 56, un mot binaire de longueur 48. Cette fonction est définie dans le tableau 5.6. La valeur $\mathrm{PC2}(b_1 \ldots b_{56})$ est $b_{14} b_{17} \ldots b_{32}$.

TABLEAU 5.6. Les fonctions PC1 et PC2

PC1						
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

PC2					
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

Ceci termine la description de l'algorithme de chiffrement du DES.

5.2.6 Déchiffrement

Pour déchiffrer un cryptogramme, on applique DES en utilisant la même suite de clés, mais en ordre inverse.

5.4 SÉCURITÉ DU DES

Depuis son invention, la sécurité du DES a fait l'objet d'études attentives. Des techniques spéciales telles que la cryptanalyse différentielle, ou linéaire, ont été inventées pour attaquer le DES **[49]** et **[70]**, mais les attaques les plus efficaces proviennent d'une exploration exhaustive de l'espace des clés. Avec des matériels spécifiques ou des grands réseaux de stations de travail, il est maintenant possible de déchiffrer les cryptogrammes venant du DES en quelques jours, voire même quelques heures. Au train où la puissance des PC augmente, on s'attend à ce que le DES puisse bientôt être cassé par un simple PC.

Aujourd'hui, le DES ne peut être considéré comme sûr que si un chiffrement triple, comme dans la section 3.7, est utilisé. Dans ces conditions, il est important de savoir que le DES n'a pas les propriétés mathématiques d'un groupe. En d'autres termes, étant données deux clés quelconques k_1 et k_2 on ne voudrait pas qu'il existe une troisième clé, k_3, telle que $\mathrm{DES}_{k_1} \circ \mathrm{DES}_{k_2} = \mathrm{DES}_{k_3}$. Si le DES était un groupe, un chiffrement répété ne pourrait pas conduire à une augmentation de la sécurité. En fait, le sous-groupe du groupe de permutations $S_{64!}$ engendré par les permutations du DES est au moins d'ordre 10^{2499} **[49]**.

5.2 ALGORITHME DU DES

Le DES est un chiffre de Feistel légèrement modifié avec l'alphabet $\{0, 1\}$ et la longueur des blocs 64. Dans cette section, nous donnons le détail de son fonctionnement.

5.2.1 Espaces des messages en clair et des cryptogrammes

L'espaces des messages en clair et l'espace des cryptogrammes du DES sont $\mathcal{P} = \mathcal{C} = \{0, 1\}^{64}$. Les clés du DES sont les mots binaires de longueur 64 qu ont la propriété suivante : quand une clé de 64 bits du DES est divisée en 8 octets la somme des 8 bits de chaque octet est impaire. Cela fait que 7 des 8 bits de l'octe déterminent la valeur du 8^e bit et on peut donc détecter les erreurs de transmission su un bit. Il résulte de cette condition que l'espace des clés est

$$\mathcal{K} = \left\{(b_1, \ldots, b_{64}) \in \{0, 1\}^{64} : \sum_{i=1}^{8} b_{8k+i} \equiv 1 \mod 2 \quad \text{avec } 0 \leqslant k \leqslant 7\right\}$$

Le nombre de clés du DES est $2^{56} \sim 7.2 * 10^{16}$.

Exemple 5.2.1 Une clé hexadécimale valable pour le DES e

133457799BBCDFF1.

Son développement binaire peut se lire dans le tableau 5.1.

TABLEAU 5.1. Une clé valable pour le DES

0	0	0	1	0	0	1	1
0	0	1	1	0	1	0	0
0	1	0	1	0	1	1	1
0	1	1	1	1	0	0	1
1	0	0	1	1	0	1	1
1	0	1	1	1	1	0	0
1	1	0	1	1	1	1	1
1	1	1	1	0	0	0	1

5.2.2 Permutation initiale

Pour chiffrer un message p, le DES passe par trois étapes.

Avant le chiffrement de Feistel, le DES applique une *permutation initiale* ($\mathcal{PI}$) à p. C'est une permutation de bits sur un vecteur de bits de longueur 64 qui ne dépend pas de la clé choisie. La permutation $\mathcal{PI}$ et son inverse sont définies dans le tableau 5.2. Ce tableau doit être lu de la façon suivante : si $p \in \{0, 1\}^{64}$, $p = p_1p_2p_3 \ldots p_{64}$, alors $\mathcal{PI}(p) = p_{58}p_{50}p_{42} \cdots p_7$.

TABLEAU 5.2. $\mathcal{PI}$, la permutation initiale

$\mathcal{PI}$							
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

$\mathcal{PI}^{-1}$							
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

Un chiffre de Feistel à 16 tournées est appliqué une fois que le message en clair est permuté, après quoi, le cryptogramme est définitivement calculé en appliquant la permutation inverse $\mathcal{PI}^{-1}$:

$$c = \mathcal{PI}^{-1}(R_{16}L_{16})$$

5.2.3 Chiffrement interne

Nous décrivons le chiffrement par bloc sur lequel s'appuie le chiffre de Feistel du DES. Son alphabet est $\{0,1\}$, la longueur des blocs est 32 et son espace des clés est $\{0,1\}^{48}$. Nous expliquons la fonction de chiffrement $f_K : \{0,1\}^{32} \to \{0,1\}^{32}$ associée à la clé $K \in \{0,1\}^{48}$ (Figure 5.3).

L'argument, $R \in \{0,1\}^{32}$, est d'abord allongé au moyen de la *fonction de développement* $E : \{0,1\}^{32} \to \{0,1\}^{48}$, définie dans le tableau 5.4. Pour résumer, si $R = R_1R_2 \dots R_{32}$, alors $E(R) = R_{32}R_1R_2 \dots R_{32}R_1$.

Ensuite, on calcule $E(R) \oplus K$ et le résultat est découpé en 8 blocs B_i de longueur 6, ce qui donne

$$E(R) \oplus K = B_1B_2B_3B_4B_5B_6B_7B_8 \tag{5.3}$$

avec $B_i \in \{0,1\}^6$. Dans l'étape suivante, on utilise 8 fonctions

$$S_i : \{0,1\}^6 \to \{0,1\}^4 \qquad 1 \leqslant i \leqslant 8$$

On les appelle les S-box et elles seront décrites plus loin. En calculant $C_i = S_i(B_i)$ au moyen de ces fonctions, on obtient $C = C_1C_2C_3C_4C_5C_6C_7C_8$, un mot binaire de longueur 32. Enfin la permutation P du tableau 5.4 est appliquée à la chaîne de caractères C et le mot binaire de longueur 32 que l'on obtient à cet instant est le cryptogramme $f_K(R)$.

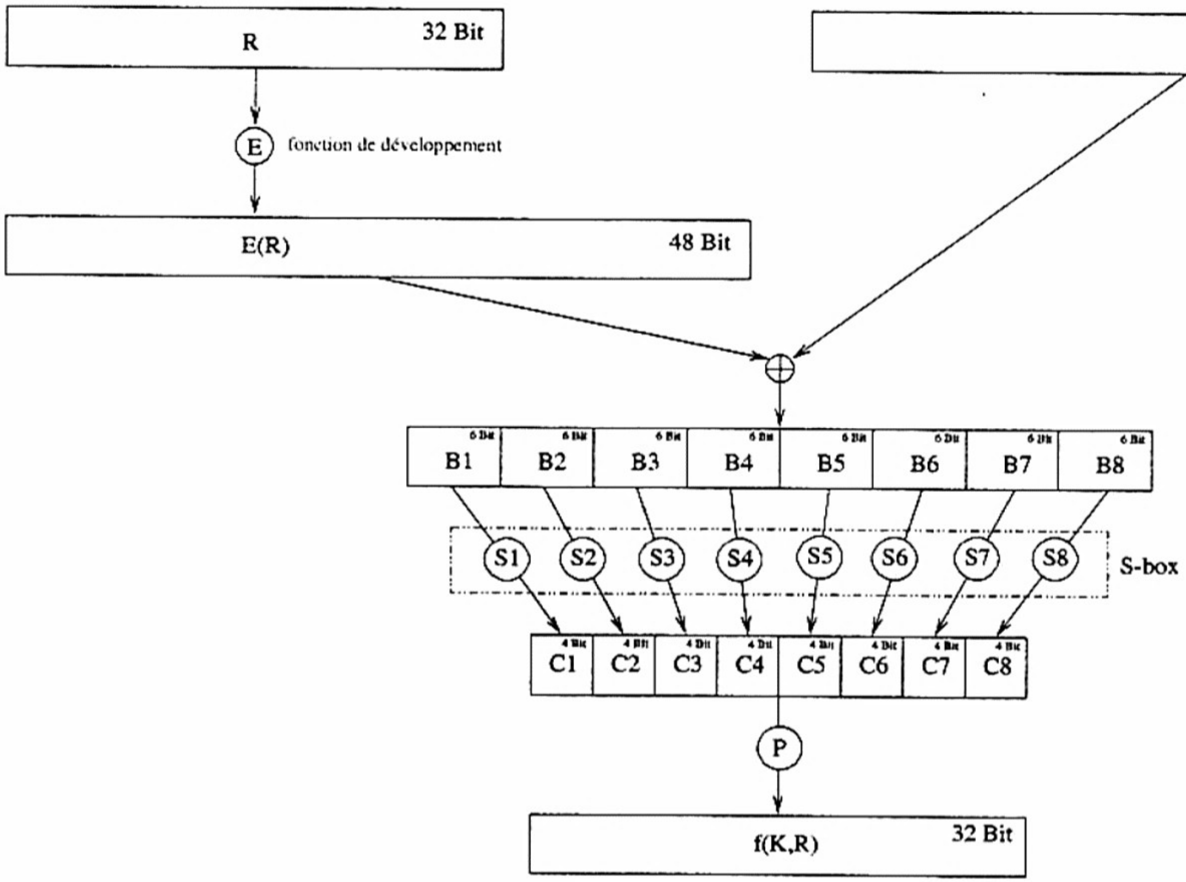

FIGURE 5.3. La fonction f du DES

TABLEAU 5.4. Les fonctions E et P

E					
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

P			
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	25

5.2.4 S-box

Maintenant nous décrivons les S-box S_i, avec $1 \leqslant i \leqslant 8$. Elles sont au cœur du DES parce que ce sont des fonctions hautement non linéaires (exercice 5.6). Le tableau 5.5 en donne la définition. Chaque S-box est représentée par un tableau de 4 lignes numérotées de [0] à [3] et 16 colonnes numérotées de [0] à [15]. Si $B = b_1b_2b_3b_4b_5b_6$, le mot binaire $S_i(B)$ est calculé de la façon suivante. L'entier qui a pour développement binaire b_1b_6 est utilisé comme indice de ligne, celui qui a pour développement binaire $b_2b_3b_4b_5$ est utilisé comme indice de colonne. À l'intersection de cette ligne et de cette colonne figure un nombre entier dans le tableau de S_i ; on écrit cet entier en binaire et s'il le faut, on place des 0 en tête du développement pour obtenir un mot binaire de longueur 4 ; c'est ce mot binaire qui est $S_i(B)$.

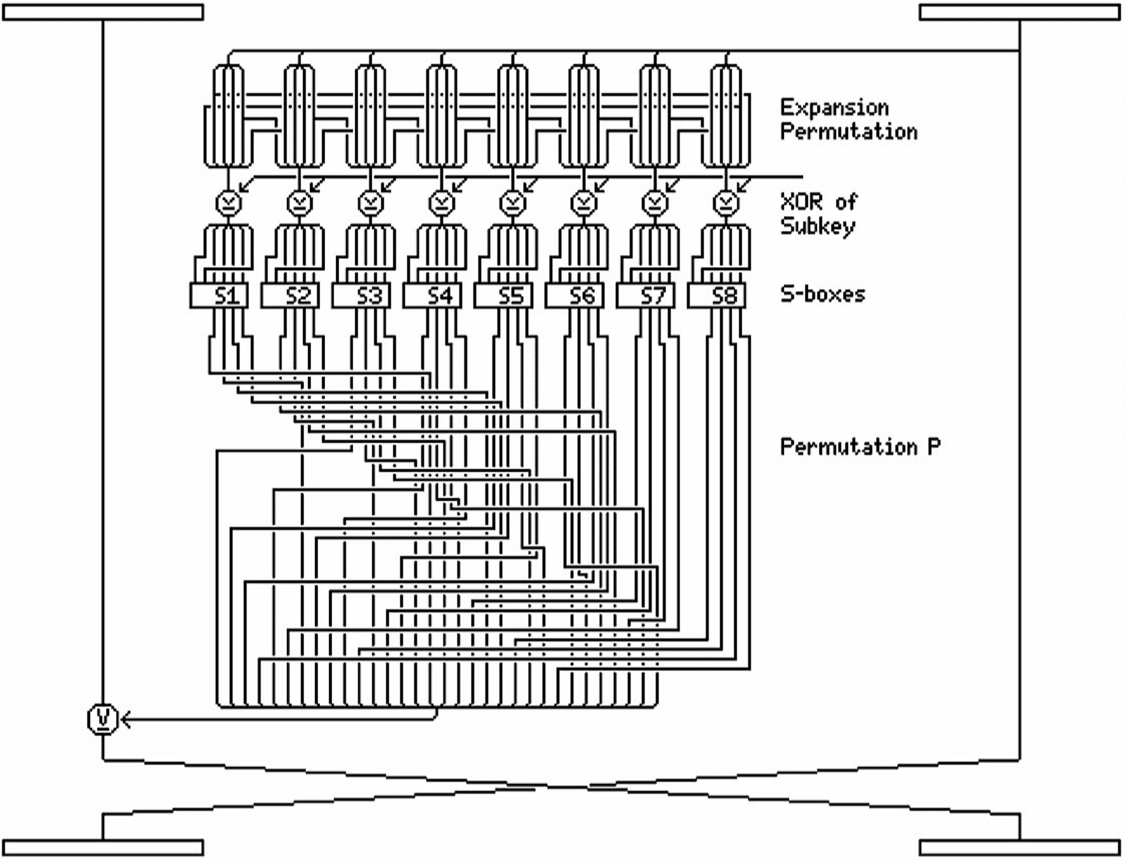

TABLEAU 5.5. Les S-box du DES

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