Exercice 1 (DES)

Le Data Encryption Standard (DES) a une propriété étonnante. Le but de cet exercice est de démontrer cette propriété. Pour plus de détails, la figure 1 présente le workflow du DES. Considérons un nombre A représenté en binaire composé de n bits. Notons A' le complément de A, que l'on définit comme $A' = A \oplus \{1\}^n$ (chaque bit de A' est l'inverse de A). Le DES a la propriété étonnante suivante. Si

$$y = DES(k, x)$$

avec x le message clair représenté en tant que nombre binaire, y le message chiffre représenté en tant que nombre binaire et k la clé, alors,

$$y' = DES(k', x')$$

1- Démontrer que pour tout A et B nombres en binaire de même longueur, nous avons :

$$A' \oplus B' = A \oplus B$$

et

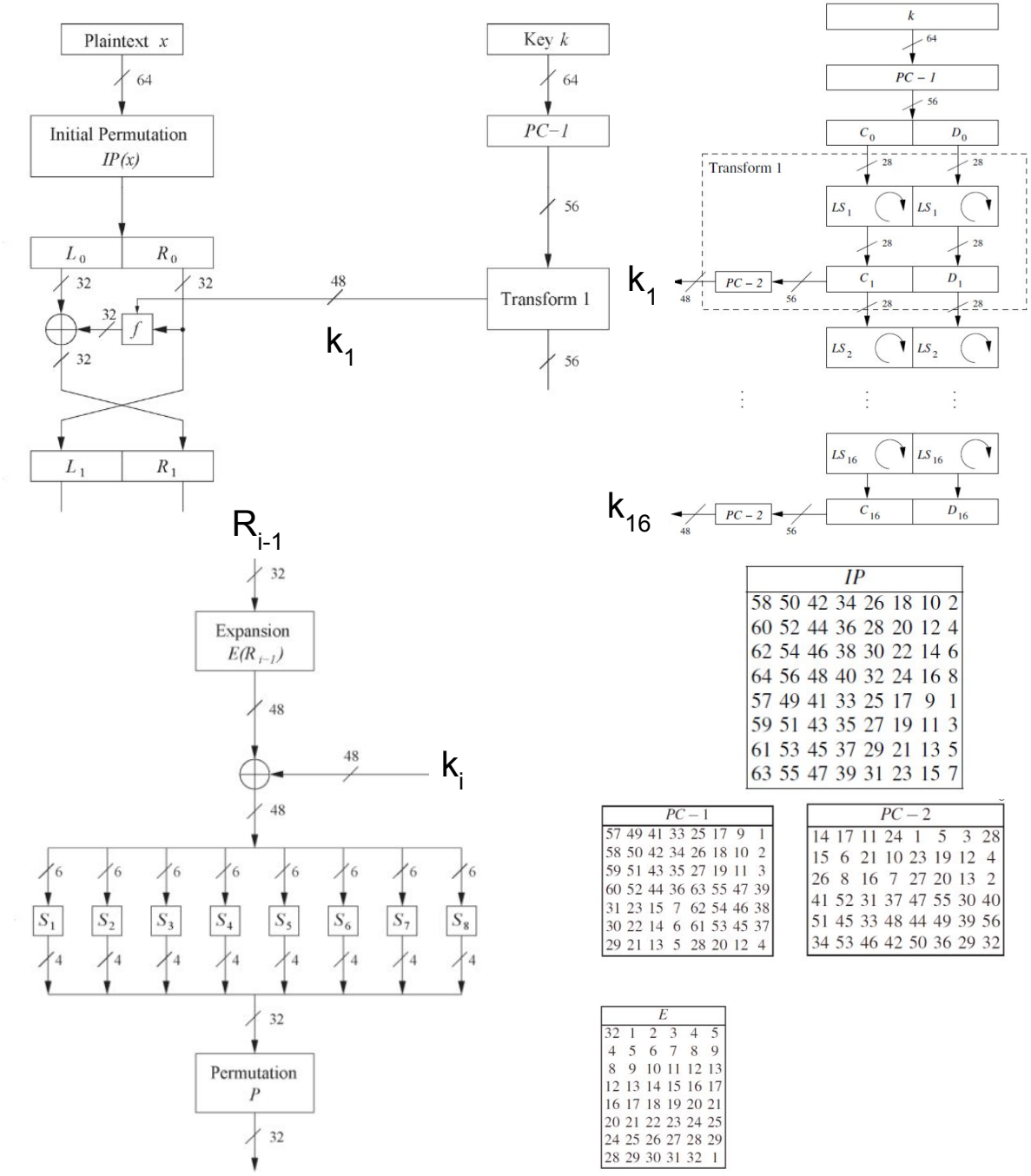
$$A' \oplus B = (A \oplus B)'$$

2- Étude des clés.
- Montrez que $PC-1(k') = (PC-1(k))'$
- Montrez que $LS_i(C'_{i-1}) = (LS_i(C_{i-1}))'$
- À partir des 2 résultats précédents, montrez que pour i = 1, 2 ,...,16, si k_i est une clé généré a partir de k, alors k'_i est une clé généré à partir de k'.

3- Étude des messages.
- Montrez que $IP(x') = (IP(x))'$
- Montrez que $E(R'_i) = (E(R_i))'$

4- Étude des messages et clés.
- En utilisant tout les résultats précédents, montrez que si R_{i-1}, L_{i-1}, k_i génèrent R_i, alors R'_{i-1}, L'_{i-1}, k'_i génèrent R'_i
- Déduisez en la propriété de l'exercice.

5- Utilisation de la propriété.
- À votre avis, cette propriété est elle valide si on change les valeurs des boites de substitutions dans le réseau de Feistel ?
- Comment cette propriété affecte l'exploration des clés lorsque l'on cherche a casser un chiffrement avec une recherche exhaustive ?



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

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

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

FIGURE 1 – Le texte clair x est chiffré avec la clé k. Le schéma en haut a gauche présente la première itération de chiffrement du DES. Le schéma a droite montre les décalages des clés. Le schéma en bas a gauche montre la fonction f, aussi appelé réseau de Feistel, pour une itération. Les permutations ou extensions sont données à titre informatif.

Exercice 2 (Chiffrement parfait)

Soit $\Gamma = \langle \mathsf{Enc}, \mathsf{Dec}, \mathcal{K}, \mathcal{M}, \mathcal{C} \rangle$ un cryptosystème. On rappelle que :
— $\mathcal{K}$ est l'ensemble des clés (il est fini)
— $\mathcal{M}$ est l'ensemble des messages en clair (il est fini)
— $\mathcal{C}$ est l'ensemble des cryptogrammes ; il a le même nombre d'éléments que $\mathcal{M}$
— Enc est une application de $\mathcal{K} \times \mathcal{M}$ dans $\mathcal{C}$.
— Dec est une application de $\mathcal{K} \times \mathcal{C}$ dans $\mathcal{M}$.

On se donne un espace probabilisé $\langle \Omega, \mathcal{P}(\Omega), \Pr \rangle$ et deux variables aléatoires indépendantes :

$$K : \Omega \to \mathcal{K}, \quad M : \Omega \to \mathcal{M}.$$

La loi de K est uniforme i.e.

$$\forall E \subseteq \mathcal{K}, \ \Pr(\{\omega \in \Omega \mid K(\omega) \in E\}) = \frac{\#(E)}{\#(\mathcal{K})}.$$

On suppose que, pour tous $k \in \mathcal{K}, m \in \mathcal{M}$:

$$\mathsf{Dec}(k, \mathsf{Enc}(k, m)) = m. \tag{1}$$

On rappelle que Γ a la propriété d'*indiscernabilité parfaite*[1] ssi pour tous $m, m' \in \mathcal{M}, c \in \mathcal{C}$,

$$\Pr(\mathsf{Enc}(K(\omega), m) = c) = \Pr(\mathsf{Enc}(K(\omega), m') = c) \tag{2}$$

Exemple 1(système de Vernam) :

$$\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0,1\}^5, \ \ \mathsf{Enc}(k, m) = k \oplus m, \ \ \mathsf{Dec}(k, m) = k \oplus m$$

où l'opération $\oplus$ est le ou exclusif sur chaque composante : si $k = k[0]k[1]\dots k[4]$ et $m = m[0]m[1]\dots m[4]$ alors

$$k \oplus m := (k[0] \oplus m[0]) \cdot (k[1] \oplus m[1]) \cdots (k[4] \oplus m[4])$$

Exemple 2 (système de Vigenère) :

$$\mathcal{K} = \{0,1\}^5, \mathcal{M} = \mathcal{C} = \{0,1\}^{10}, \ \ \mathsf{Enc}(k, m) = (k \cdot k) \oplus m, \ \ \mathsf{Dec}(k, m) = (k \cdot k) \oplus m$$

Exemple 3 (Permutation des positions, messages de longueur 15) :

$$\mathcal{K} = \mathcal{S}_5, \mathcal{M} = \mathcal{C} = \{0,1\}^{15}$$

Chaque élément de $\mathcal{S}_5$ est une permutation des entiers de $[0, 4]$ donnée par la suite de ses images. Par exemple $\sigma = (3, 0, 4, 1, 2)$ dénote la permutation $(0 \mapsto 3, 1 \mapsto 0, 2 \mapsto 4, 3 \mapsto 1, 4 \mapsto 2)$. Chaque message m peut être décomposé en 3 messages de longueur 5 :

$$m = f_0 \cdot f_1 \cdot f_2$$

On pose alors

$$\mathsf{Enc}(\sigma, m) := (f_0 \circ \sigma) \cdot (f_1 \circ \sigma) \cdot (f_2 \circ \sigma).$$

1. ce que nous désignerons par "parfait" dans la suite

Par exemple,

$$\mathsf{Enc}(((3,0,4,1,2),110101100000111) = 11010 \cdot 01010 \cdot 10101$$

1- Pour chacun des exemples ci-dessus, déterminer si le cryptosystème est parfait.

Étant donnée une application à deux arguments

$$f : A \times B \to C$$

nous noterons pour tous $a \in A, b \in B$, $\quad f(*,b) : A \to C$ et $\quad f(a,*) : B \to C$ les applications partielles :

$$f(*,b) : x \mapsto f(x,b), \quad f(a,*) : x \mapsto f(a,x).$$

2- Montrer que l'égalité (1) entraine que, pour toute clé $k \in \mathcal{K}$, l'application $\mathsf{Enc}(k,*)$ est injective.
3- En déduire que, pour toute clé $k \in \mathcal{K}$, l'application $\mathsf{Enc}(k,*)$ est une bijection de $\mathcal{M}$ dans $\mathcal{C}$.
4- Montrer que, pour tout cryptosystème vérifiant les hypothèses de l'énoncé (i.e. jusqu'à l'équation (1) comprise), et tous $k \in \mathcal{K}, c \in \mathcal{C}$:

$$\mathsf{Enc}(k, \mathsf{Dec}(k,c)) = c.$$

Aide : On pourra montrer que les deux applications $\mathsf{Enc}(k,*)$ et $\mathsf{Dec}(k,*)$ sont réciproques l'une de l'autre.
Une application $f : A \to B$ est dite *équilibrée* ssi

$$\forall b, b' \in B, \#(f^{-1}(b)) = \#(f^{-1}(b')).$$

5- Montrer que, si Γ est parfait, alors pour tout $c \in \mathcal{C}$, $\mathsf{Dec}(*,c)$ est équilibrée.
6- Montrer que, si pour tout $c \in \mathcal{C}$, $\mathsf{Dec}(*,c)$ est équilibrée, alors Γ est parfait.
7- Montrer que, si Γ est parfait, alors $\#(\mathcal{M})$ divise $\#(\mathcal{K})$.
Exemple 4 : (Permutation des positions, messages de longueur 5) :

$$\mathcal{K} = \mathcal{S}_5, \mathcal{M} = \mathcal{C} = \{0,1\}^5, \quad \mathsf{Enc}(\sigma, m) := m \circ \sigma.$$

8- Le cryptosystème de l'exemple 4 est-il parfait ?