Corrigé-type + Barème

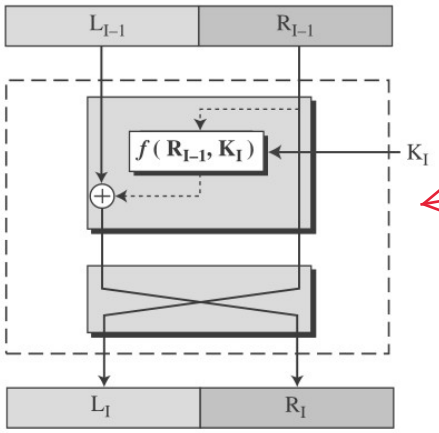
Réponse à l'exercice 1

1) Les inconvénients majeurs du mode d'opération « Electronic Code Book » ECB sont :
   1) Les blocs clairs identiques donnent des blocs chiffrés identiques. ← 01 pt
   2) Les textes clairs identiques donnent des textes chiffrés identiques. ← 01 pt
2) Avantages du mode d'opération « Cipher Block Chaining » CBC sont :
   (a) Les blocs clairs identiques donnent des blocs chiffrés différents. ← 01 pt
   (b) Accès aléatoire aux blocs chiffré.

   Inconvénient du mode d'opération « Cipher Block Chaining » CBC sont :
   (a) Performance réduite puisque le chiffrement ne peut être parallélisé (séquentiel).
   (b) Propagation limitée d'erreurs. ← 01 pt

Réponse à l'exercice 2

1) Un schéma de Feistel comme illustré par la figure suivante prend en entrée un bloc clair et le découpe en deux parties de longueurs égales nommées L_{i-1} et R_{i-1}. Il produit en sortie un bloc chiffré sous forme de deux parties de même longueur nommées L_i et R_i.



← 02 pts

2) L'opération de chiffrement est donnée par : $\begin{cases} L_i = & R_{i-1} \\ R_i = f(R_{i-1}; K_i) \oplus L_{i-1} \end{cases}$ ← 01 pt

3) L'opération de déchiffrement est donnée par : $\begin{cases} L_{i-1} = R_i \oplus f(L_i; K_i) \\ R_{i-1} = & L_i \end{cases}$ ← 01 pt

4) $m = 110100010001$ et $k = 100110$. Ainsi $L_{i-1} = 110100$ et $R_{i-1} = 010001$:

$$\begin{cases} L_i = 010001 \\ R_i = f(R_{i-1}; K_i) \oplus L_{i-1} = f(010001; 100110) \oplus 110100 = \overline{010001 \oplus 100110} \oplus 110100 \end{cases}$$

$$\begin{cases} L_i = 010001 \\ R_i = \overline{110111} \oplus 110100 = 001000 \oplus 110100 = 111100 \end{cases} \Rightarrow \text{c=010001111100}$$ ← 02 pts

5) $c = 110010010111$ et $k = 001011$. Ainsi $L_i = 110010$ et $R_i = 010111$:

$$\begin{cases} L_{i-1} = R_i \oplus f(L_i; K_i) = 010111 \oplus f(110010; 001011) = 010111 \oplus \overline{110010 \oplus 001011} \\ R_{i-1} = 110010 \end{cases}$$

$$\begin{cases} L_{i-1} = 010111 \oplus \overline{111001} = 010111 \oplus 000110 = 010001 \\ R_{i-1} = 110010 \end{cases} \Rightarrow \text{m=010001110010}$$ ← 02 pts

Réponse à l'exercice 3

1) Puisque la taille effective d'une clé DES est de 56 bits, la taille de l'espace de clés est
$N = 2^{56} = 72\,057\,594\,037\,927\,936$ clés. 01 pt

2) Le temps nécessaire pour tester une clé $T_{\text{clé}}$ est le temps nécessaire pour exécuter 1500 instructions.
Le temps nécessaire pour exécuter une seule instruction est
$T_{\text{inst}} = \frac{1}{5\times10^9} = 2 \times 10^{-10}$ seconde.
Donc $T_{\text{clé}} = T_{\text{inst}} \times 1500 = 2 \times 10^{-10} \times 1500 = 3 \times 10^{-7}$ seconde.
Ainsi, le temps moyen T_{attaque} d'une attaque par force brute est :
$T_{\text{attaque}} = T_{\text{clé}} \times 2^{55} = 3 \times 10^{-7} \times 36\,028\,797\,018\,963\,968 = 10\,808\,639\,105,68919$ seconde.
$T_{\text{attaque}} = \frac{10\,808\,639\,105,68919}{3600\times24\times365} = 342,73969$ années.
$T_{\text{attaque}} = 342$ années, 8 mois et 27 jours. 02 pts

3) Les données à l'entrée des S-Boxes sont :
$(C2BBCBE4F517)_{16} = (\overbrace{110000}^{S_1}\ \overbrace{101011}^{S_2}\ \overbrace{101111}^{S_3}\ \overbrace{001011}^{S_4}\ \overbrace{111001}^{S_5}\ \overbrace{001111}^{S_6}\ \overbrace{010100}^{S_7}\ \overbrace{010111}^{S_8})_2$.
$\overbrace{\mathbf{1}01011\mathbf{1}}^{S_2}$: N° ligne = $(11)_2 = 3$, N° colonne = $(0101)_2 = 5$. $S_2(101011) = 15 = (1111)_2$ 01 pt
$\overbrace{\mathbf{1}11001\mathbf{1}}^{S_5}$: N° ligne = $(11)_2 = 3$, N° colonne = $(1100)_2 = 12$. $S_5(111001) = 10 = (1010)_2$ 01 pt
$\overbrace{\mathbf{0}10111\mathbf{1}}^{S_8}$: N° ligne = $(01)_2 = 1$, N° colonne = $(1011)_2 = 11$. $S_8(010111) = 11 = (1011)_2$. 01 pt

4) Les données à la sortie des S-Boxes (entrée de la matrice P) sont :
$(DE5F27A8)_{16} = (11011110010111110010011110101000)_2$.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	1	0	1	1	1	1	0	0	1	0	1	1	1	1	1	0	0	1	0	0	1	1	1	1	0	1	0	1	0	0	0

$P(11011110010111110010011110101000) = (11001100111010011011010011011011)_2$
$P(11011110010111110010011110101000) = (CCE9B4DB)_{16}$ 02 pts

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