23/11/2021

Corrigé TD-2-SI

Exercice 1:

1/- $T = \begin{cases} L_1 = R_0 & (1) \\ R_1 = L_0 \oplus F(R_0, K_1) & (2) \end{cases}$

$\Leftrightarrow \begin{cases} R_0 = L_1 \\ L_0 = R_1 \oplus F(R_0, K_1) \end{cases}$

$\Leftrightarrow \begin{cases} R_0 = L_1 \\ L_0 = R_1 \oplus F(L_1, K_1) \end{cases}$

Conclusion: Pour (L_1, R_1), il existe (L_0, R_0) tel que :

$$(L_0, R_0) = T^{-1}(L_1, R_1).$$

2/- $(L_0, R_0) \longrightarrow (L_n, R_n)$ après n Rondes.

- Par récurrence sur n.

* Pour nous, c'est fait dans la question (1) pour la 1ère ronde.
* Hyp: On suppose que la propriété est vraie jusqu'au ronde n-1 et on montre qu'elle est vraie pour la ronde n.

$$T_n : \begin{cases} L_n = R_{n-1} \\ R_n = L_{n-1} \oplus F(R_{n-1}, k_n) \end{cases}$$

T_n est bijective d'après la 1ère question.

D'après H.R on a :

	L_0	R_0
T_1	L_1	R_1
⋮	⋮	⋮
T_n	L_n	R_n

$T_1, T_2, \dots, T_{n-1}$ sont bijectives.

D'où $T_1, T_2, \dots, T_{n-1}, T_n$ est bijective.

Exercice 2 :

1/- Chiffrons le mot 1111 :

On a : $$\begin{cases} L_n = R_{n-1} \\ R_n = L_{n-1} \oplus F(R_{n-1}, k_n) \end{cases}$$

Alors : $$\begin{cases} L_1 = R_0 \\ R_1 = L_0 \oplus F(R_0, k_1) \end{cases}$$

$$\begin{cases} L_2 = R_1 \\ R_2 = L_1 \oplus F(R_1, k_2) \end{cases}$$

$$\begin{cases} L_2 = R_1 \\ R_2 = L_1 \oplus F(R_1, K_2) \end{cases}$$

On remplace R_1 et L_1 :

$$\begin{cases} L_2 = L_0 \oplus F(R_0) \\ R_2 = R_0 \oplus F(R_1) \end{cases} \Rightarrow \begin{cases} L_2 = L_0 \oplus F(R_0) \\ R_2 = R_0 \oplus F(L_0 \oplus R_0) \end{cases}$$

$$\Rightarrow \begin{cases} L_2 = 11 \oplus F(11) \\ R_2 = 11 \oplus F(11 \oplus F(11)) \end{cases}$$

$$\Rightarrow \begin{cases} L_2 = 11 \\ R_2 = 00 \end{cases}$$

Le mot est : 0011.

2/- Trouvons les invariants :

On veut trouver que : $\begin{cases} L_2 = L_0 \\ R_2 = R_0 \end{cases}$

il faut que : $\begin{cases} f_1(R_0) = 00 \\ f_2(L_0 \oplus f_1(R_0)) = 00 \end{cases} \Leftrightarrow \begin{cases} f_1(R_0) = 00 \Leftrightarrow R_0 = 11 \text{ ou } R_0 = 01 \\ f_2(L_0 \oplus f_1(R_0)) \end{cases}$ (2)

En remplaçant $f_1(R_0)$ dans (2):

$$\begin{cases} f_1(R_0) = 00 \Leftrightarrow R_0 = 11 \\ \qquad\qquad\quad \text{ou} \quad R_0 = 01 \\ f_2(L_0 \oplus 00) = 00 \Rightarrow f_2(L_0) = 00 \end{cases}$$

alors: $\begin{cases} R_0 = 11 \text{ ou } R_0 = 01 \\ L_0 = 10 \end{cases}$

Nous donnes les invariants $\begin{cases} 1110 \\ 0110 \end{cases}$.

3)- on a les blocs du message:

$M_1 = 1000$; $M_2 = 1101$; $M_3 = 0011$; $M_4 = 1110$.

$E(M)$ est l'image du message M par le digramme de Feistel on obtient:

$C_1 = E(M_1 \oplus IV) = E(1000 \oplus 0000) = E(1000) = 0111$.

$C_2 = E(M_2 \oplus C_1) = E(1101 \oplus 0111) = E(1010) = 1101$.

$C_3 = E(M_3 \oplus C_2) = E(0011 \oplus 1101) = E(1110) = 1110$.

$C_4 = E(M_4 \oplus C_3) = E(1110 \oplus 1110) = E(0000) = 1111$.

alors on aura à la fin, le message crypté:

0111 1101 1110 1111.

(1)

Corrigé du Problème sur le D.E.S

(1) Montrons que les chaines C_{16} et D_{16} du D.E.S sont obtenus à partir de C_1 et D_1 par un décalage en permutation circulaire d'1 cran vers la droite.

Il suffit de le montrer pour C_1. La démonstration sera la même pour D_1, car C_1 et D_1 subissent les mêmes opérations.

on a: $K_1 = PC-2(C_1 D_1)$

$C_1 = C_{11} C_{12} C_{13} \dots C_{127} C_{128}$ $\quad D_1 = D_{11} D_{12} \dots D_{128}$

Nous savons que durant la 1ère ronde, telle que $\in \{1, 2, 9, 16\}$ on fait un décalage à gauche d'un bit.

Et pour toutes les autres rondes (12 rondes) on fait un décalage de 2 bits à gauche.

Donc, au total: $(2 \times 12) + 3 = 27$ bits seront décalés à gauche

Note: on ne compte pas le bit qui a été décalé à gauche pour passer de C_0 à C_1. Parce que dans l'énoncé on précise: à partir de C_1

Or, si 27 bits sont décalés à gauche, on obtient

$C_{(16)} = C_{128} C_{11} C_{12} \dots C_{127}$

D'autre part si on fait un décalage circulaire à droite d'1 cran on obtient aussi:

$C_{128} C_{11} C_{12} \dots C_{127}$

D'où le résultat. _

II

(2) Montrons que tous les bits de C_1 sont égaux.
Formellement cela revient à montrer que

$$C_{1\,j} = C_{1\,(j+1)} \text{ pour tout } 1 \leq j \leq 27$$

On a par Hypothèse : $K_1 = K_2 = \dots = K_{16}$ (H.P)
Donc il faut trouver une relation entre $K_1, \dots, K_{16}$ et C_1.
En effet: D'après la question (1) : sachant que C_{16} est obtenue à partir de C_1 par un décalage circulaire de 1 bit à droite alors: le bit qui se trouve à la $i^{ème}$ position dans C_1 se trouve dans la position $i+1$ dans C_{16}, d'où

$$(R_1) \quad C_{1\,j} = C_{16\,j+1} \text{ pour } 1 \leq j \leq 27$$

D'autre part, on sait que les K_i sont obtenues en appliquant (PC-2) à $(C_i D_i)$:
Observons que la partie supérieure de (PC-2) (les 4 premières lignes s'appliquent ou opèrent sur C_i, et la partie inférieure de (PC-2) opère sur D_i.
Nous pouvons définir une fonction, g qui est équivalente à (PC-2), comme suit.

$g(1) = 14 \quad g(2) = 17, \dots \dots g(24) = \dots$

$g : \{1, 2, 3, \dots 24\} \longrightarrow \{1, 2, 3, \dots 28\}$

g est bijective de $\{1, 2, 3, \dots 24\}$ vers $\text{Image}(g) = \{1, 2, \dots 28\}$

On en déduit que :

si $K_i = K_{i1} K_{i2} \dots K_{i24} K_{i25} \dots K_{i48}$

$$K_{ij} = C_{i\,g(i)} \quad \text{pour } 1 \leq i \leq 24$$

D'où : $\Leftrightarrow$ $\boxed{\begin{array}{ll} K_1 f = C_1 g(j) & \forall\, 1 \le j \le 28 \\ K_1 g^{-1}(j) = C_1 j & (R_2) \end{array}}$

Or d'après (R_1) on a : $C_1 j = C_{16}(j+1)$ $\quad \forall\, 1 \le j \le 27$

et d'après (R_2) $C_{16}(j+1) = K_{16} g^{-1}(j+1) \overset{(H.P)}{=} K_1 g^{-1}(j+1) = C_1 j+1$

Mais avec $j+1 \notin \{9, 18, 22, 25\}$
c'est à dire $j \notin \{8, 17, 21, 24\}$

(parce que g^{-1} n'est pas définie pour les 4 valeurs en question)

D'où : $C_1 j = C_{16}(j+1) = C_1 j+1$ avec $j \notin \{8, 17, 21, 24\}$ et $1 \le j \le 28$

Montrons maintenant à vérifier que :

$C_{18} = C_{19}$ $\quad C_{17} = C_{18}$ $\quad C_{21} = C_{22}$ et $C_{24} = C_{25}$

Il suffit de montrer que $C_{18} = C_{19}$ les autres égalités sont similaires

On a par construction $C_{28} = C_{19}$ (car C_2 est obtenue à partir de C_1 par un décalage d'1 vers la gauche)

or $C_{18} \overset{(R_3)}{=} K_1 g^{-1}(8) \overset{(H.P)}{=} K_2 g^{-1}(8) \overset{(R_2)}{=} C_{28} = C_{19}$

Conclusion : $\boxed{C_{18} = C_{19}}$.

(3) On va en déduire qu'il existe exactement 4 clé du DES qui donnent des clés des tournées toutes égales

En effet Nous pouvons donner aux bits de C_1 des valeurs de bits egales toute à 1 ou toute egale à 0 (2 possibilité)
De meme pour le D_1. (2 possibilité)
Donc en tout, 4 possibilité pour la clé DES pour aboutir à 4 clés de rondes (les 16 clé) toute égales.