Devoir # 1
Sécurité informatique - IFT 3275/ IFT 6271

Jonathan Caspar (20059041) - Johnny Pho (20046014)

28 Février 2019

Partie Théorique

1 Soit un masque jetable utilisant une clef $k = 0^l$ (composée seulement de zéros). Nous remarquons que $k \oplus m = m$ et que notre message chiffré est en fait notre message clair! De ce fait, est-il nécessaire d'utiliser des générateurs de bits qui produisent seulement des clefs $k \neq 0^l$ pour utiliser un masque jetable?

Non, cela n'est pas nécessaire. Si on retire la clé 0^l, on viole deux principes du masque jetable :

1. La clé 0^l est retiré de l'espace clé K, alors la répartition des clés n'est plus équiprobable.
2. Cela représente une information supplémentaire que l'on peut extraire du masque jetable, or un masque jetable ne doit donner aucune autre information autre que la longueur du message.

2 Soit un réseau de Feistel composé de deux "rounds" utilisant les fonctions de "rounds" f_1 et f_2. Démontrez que : Feistel $f_1, f_2(L_0,\ R_0) = (L_2,\ R_2) \Rightarrow$ Feistel $f_2, f_1(R_2,\ L_2) = (R_0,\ L_0)$

Pour prouver cette implication (A⇒B), on suppose que le réseau A Feistel $f_1, f_2(L_0,\ R_0) = (L_2,\ R_2)$ est vrai et à partir des expressions qu'on arrive à dériver du réseau A : on se sert de ces expressions pour montrer que le réseau B Feistel est de la forme $f_2, f_1(R_2,\ L_2) = (R_4,\ L_4)$ et que $L_4 = L_0$ et $R_4 = R_0$.

<u>Hypothèses :</u>

$$L_2 = R_1 = \boxed{(L_0 \oplus F(k_1, R_0))}$$

$$R_2 = (L_1 \oplus F(k_2, R_1)) = \boxed{(R_0 \oplus F(k_2, R_1))} \textbf{ car } L_1 = R_0$$

On exprime de la même manière les valeurs de R_4 et L_4 du réseau B :

$R_4 = L_3 = \boxed{(R_2 \oplus F(k_2, L_2))}$

$L_4 = (R_3 \oplus F(k_1, L_3)) = \boxed{(L_2 \oplus F(k_1, L_3))}$ **car** $R_3 = L_2$

En se servant des hypothèses, on fait une substitution de valeurs dans R_4 et L_4 et on simplifie :

$R_4 = (R_2 \oplus F(k_2, L_2)) = (R_2 \oplus F(k_2, R_1))$ **car** $L_2 = R_1$

$= [(R_0 \oplus F(k_2, R_1)] \oplus F(k_2, R_1))$ **car** $R_2 = (R_0 \oplus F(k_2, R_1)$ **par hypothèse**

$= (R_0 \oplus [F(k_2, R_1) \oplus F(k_2, R_1))]$ **par associativité du XOR**

$= R_0 \oplus 0$ **car** $X \oplus X = 0$

$\boxed{R_4 = R_0}$ **car** $X \oplus 0 = X$

$L_4 = L_2 \oplus F(k_1, L_3) = (L_2 \oplus F(k_1, R_0))$ **car** $L_3 = L_4 = R_0$ **(prouvé précédemment)**

$= [(L_0 \oplus F(k_1, R_0)] \oplus F(k_1, R_0))$ **car** $L_2 = (L_0 \oplus F(k_1, R_0))$ **par hypothèse**

$= (L_0 \oplus [F(k_1, R_0) \oplus F(k_1, R_0))]$ **par associativité du XOR**

$= L_0 \oplus 0$ **car** $X \oplus X = 0$

$\boxed{L_4 = L_0}$ **car** $X \oplus 0 = X$

3 Démontrez la propriété de complémentarité de DES, c'est- à-dire que :

$$DES_k(m) = \overline{DES_{\overline{k}}(\overline{m})}$$

pour toute clef k et message m (où $\overline{x}$ représente la négation logique bit à bit de x).

//TODO

4

Table 1: Fréquences des différentielles de sortie ΔY (colonnes) pour chaque différentielle d'entrée ΔX (lignes) :

		ΔY															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
ΔX	**0**	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	0	0	0	0	0	2	6	4	0	0	0	2	2
	2	0	0	0	0	0	0	0	0	2	2	2	6	4	0	0	0
	3	0	2	6	4	0	2	2	0	0	0	0	0	0	0	0	0
	4	0	0	0	0	6	6	2	2	0	0	0	0	0	0	0	0
	5	0	0	0	0	0	0	0	0	0	0	2	2	6	2	4	0
	6	0	0	0	0	0	0	0	0	4	0	0	0	2	2	6	2
	7	0	2	2	0	2	0	4	6	0	0	0	0	0	0	0	0
	8	0	0	0	0	0	0	0	0	0	4	0	0	2	2	2	6
	9	0	2	0	2	2	0	6	4	0	0	0	0	0	0	0	0
	A	0	0	2	2	6	6	0	0	0	0	0	0	0	0	0	0
	B	0	0	0	0	0	0	0	0	0	0	2	2	2	6	0	4
	C	0	0	0	0	0	0	0	0	2	2	6	2	0	4	0	0
	D	0	2	4	6	0	2	0	2	0	0	0	0	0	0	0	0
	E	0	8	2	2	0	0	2	2	0	0	0	0	0	0	0	0
	F	0	0	0	0	0	0	0	0	6	2	0	4	0	0	2	2

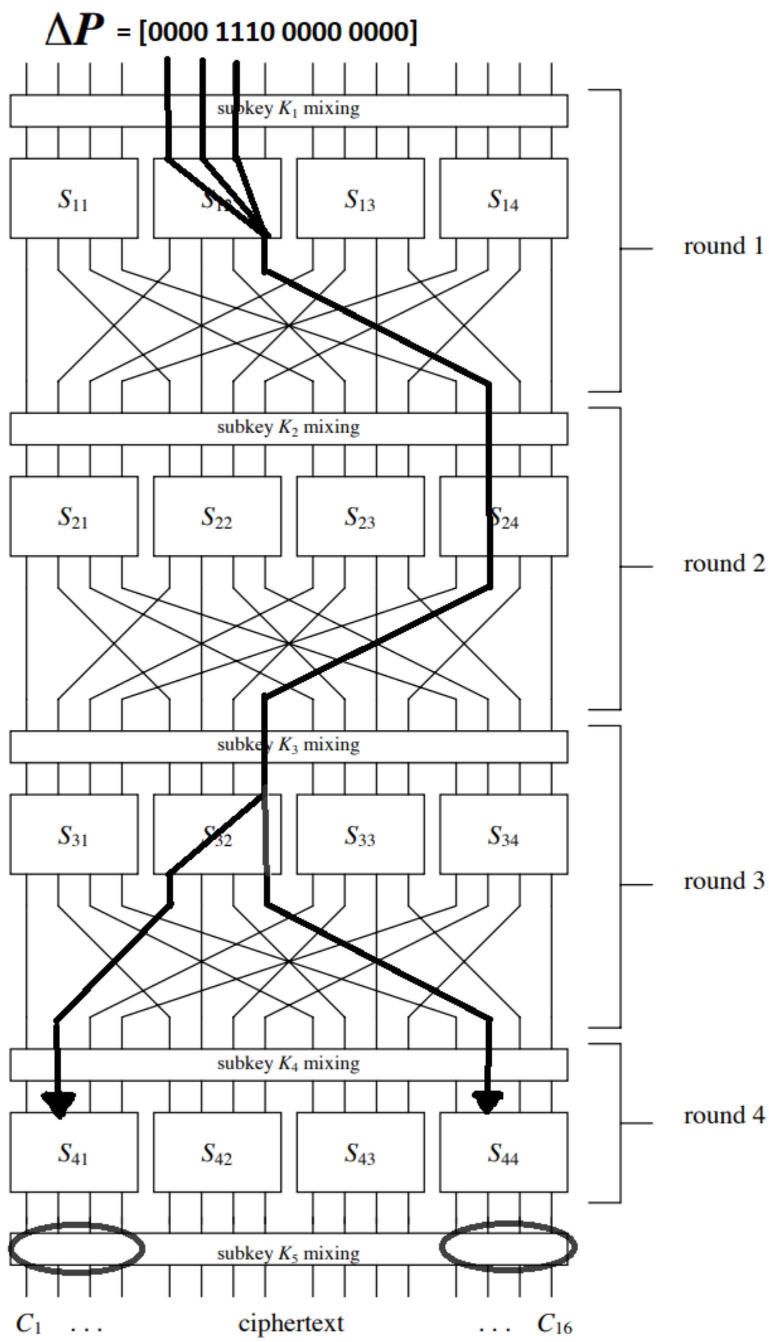
Schéma du SPN démontrant une différentielle caractéristique avec : $\boxed{\Delta P = \text{ 0000 1110 0000 0000}}$

On se sert de ces différentielles dans les S-Boxes :

$$S_{1,2} : \Delta X = E \Rightarrow \Delta Y = 1 \text{ avec probabilité } \frac{8}{16}$$

$$S_{2,4} : \Delta X = 4 \Rightarrow \Delta Y = 4 \text{ avec probabilité } \frac{6}{16}$$

$$S_{3,2} : \Delta X = 1 \Rightarrow \Delta Y = 9 \text{ avec probabilité } \frac{6}{16}$$



On obtient la différentielle intermédiaire suivante $\boxed{\Delta I = \text{ 0100 0000 0000 0100}}$