

# Devoir # 1

## Sécurité informatique - IFT 3275/ IFT 6271

Jonathan Caspar (20059041) - Johnny Pho (20046014)

28 Février 2019

### Partie Théorique

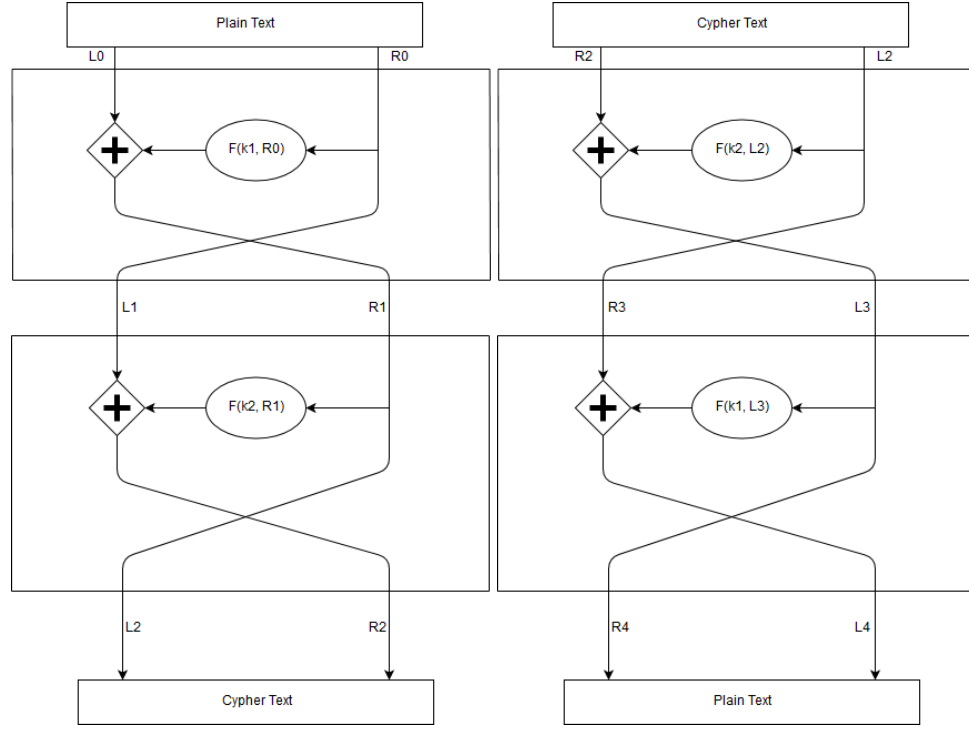
- 1** Soit un masque jetable utilisant une clef  $k = 0^l$  (composée seulement de zéros). Nous remarquons que  $k \oplus m = m$  et que notre message chiffré est en fait notre message clair! De ce fait, est-il nécessaire d'utiliser des générateurs de bits qui produisent seulement des clefs  $k \neq 0^l$  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 ( $A \Rightarrow B$ ), 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  $R_4 = R_0$ .



Hypothèses :

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

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

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

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

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

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

$$\begin{aligned} R_4 &= (R_2 \oplus F(k_2, L_2)) = (R_2 \oplus F(k_2, R_1)) \text{ car } L_2 = R_1 \\ &= [(R_0 \oplus F(k_2, R_1)) \oplus F(k_2, R_1)] \text{ car } R_2 = (R_0 \oplus F(k_2, R_1)) \text{ par hypothèse} \\ &= (R_0 \oplus [F(k_2, R_1) \oplus F(k_2, R_1)]) \text{ par associativité du XOR} \\ &= R_0 \oplus 0 \text{ car } X \oplus X = 0 \text{ et donc } \boxed{R_4 = R_0} \text{ car } X \oplus 0 = X \end{aligned}$$

$$\begin{aligned}
L_4 &= L_2 \oplus F(k_1, L_3) = (L_2 \oplus F(k_1, R_0)) \text{ car } L_3 = L_4 = R_0 \text{ (prouvé précédemment)} \\
&= [(L_0 \oplus F(k_1, R_0)) \oplus F(k_1, R_0)] \text{ car } L_2 = (L_0 \oplus F(k_1, R_0)) \text{ par hypothèse} \\
&= (L_0 \oplus [F(k_1, R_0) \oplus F(k_1, R_0)]) \text{ par associativité du XOR} \\
&= L_0 \oplus 0 \text{ car } X \oplus X = 0 \\
\boxed{L_4 = L_0} &\text{ car } X \oplus 0 = X
\end{aligned}$$

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

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

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

La notation  $L_x, R_x$  correspond à la concaténation des deux séquences.

Supposons qu'on applique deux DES (le premier avec la clé  $K_0$ , le deuxième avec la clé  $k_0$ ) à deux messages  $m_1 = L_0, R_0$  et  $m_2 = l_0, r_0$ , la version chiffrée de ces messages est de la forme  $c_1 = L_n, R_n$  et  $c_2 = l_n, r_n$  avec  $n$  le nombre de rounds des DES.

On va montrer que sous l'hypothèse où  $\boxed{l_0 = \bar{L}_0, r_0 = \bar{R}_0 \text{ et } k_0 = \bar{K}_0}$  alors  $\boxed{l_n = \bar{L}_n, r_n = \bar{R}_n \text{ et } k_n = \bar{K}_n}$  et donc que  $c_2 = l_n, r_n = \bar{L}_n, \bar{R}_n = \bar{c}_1$

Cas de base (n = 1):

$$\begin{aligned}
L_1 &= R_0 \\
R_1 &= L_0 \oplus F(R_0, K_0)
\end{aligned}$$

$$\begin{aligned}
l_1 &= r_0 = \bar{R}_0 \text{ par hypothèse} = \boxed{\bar{L}_1} \text{ car } R_0 = L_1 \\
r_1 &= l_0 \oplus F(r_0, k_0) = \bar{L}_0 \oplus F(\bar{R}_0, \bar{K}_0) \text{ par hypothèse} \\
&= \overline{\bar{L}_0 \oplus F(\bar{R}_0, \bar{K}_0)} \text{ car } \overline{A \oplus B} = \bar{A} \oplus \bar{B} \\
&= \overline{\bar{L}_0 \oplus F(R_0, K_0)} \text{ car la fonction F se base sur XOR et } \bar{\bar{A}} \oplus \bar{\bar{B}} = A \oplus B \\
&= \boxed{\bar{R}_1} \text{ car } L_0 \oplus F(R_0, K_0) = R_1
\end{aligned}$$

Par induction sur n, si vrai pour n alors vrai pour n+1 :

$$L_{n+1} = R_n$$

$$R_{n+1} = L_n \oplus F(R_n, K_n)$$

$$l_{n+1} = r_n = \overline{R_n} \text{ par hypothèse } = \boxed{\overline{L_{n+1}}} \text{ car } R_n = L_{n+1}$$

$$r_{n+1} = l_n \oplus F(r_n, k_n) = \overline{L_n} \oplus F(\overline{R_n}, \overline{K_n}) \text{ par hypothèse}$$

$$= \overline{L_n \oplus F(\overline{R_n}, \overline{K_n})} \text{ car } \overline{A \oplus B} = \overline{A} \oplus \overline{B}$$

$$= \overline{L_n \oplus F(R_n, K_n)} \text{ car la fonction F se base sur XOR et } \overline{A \oplus B} = A \oplus B$$

$$= \boxed{\overline{R_{n+1}}} \text{ car } L_n \oplus F(R_n, K_n) = R_{n+1}$$

On obtient donc  $\boxed{c_2 = l_n, r_n = \overline{L_n}, \overline{R_n} = \overline{c_1}}$

#### 4 Fréquences des différentielles de sortie $\Delta Y$ (colonnes) pour chaque différentielle d'entrée $\Delta X$ (lignes) :

		$\Delta Y$															
$\Delta X$		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	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

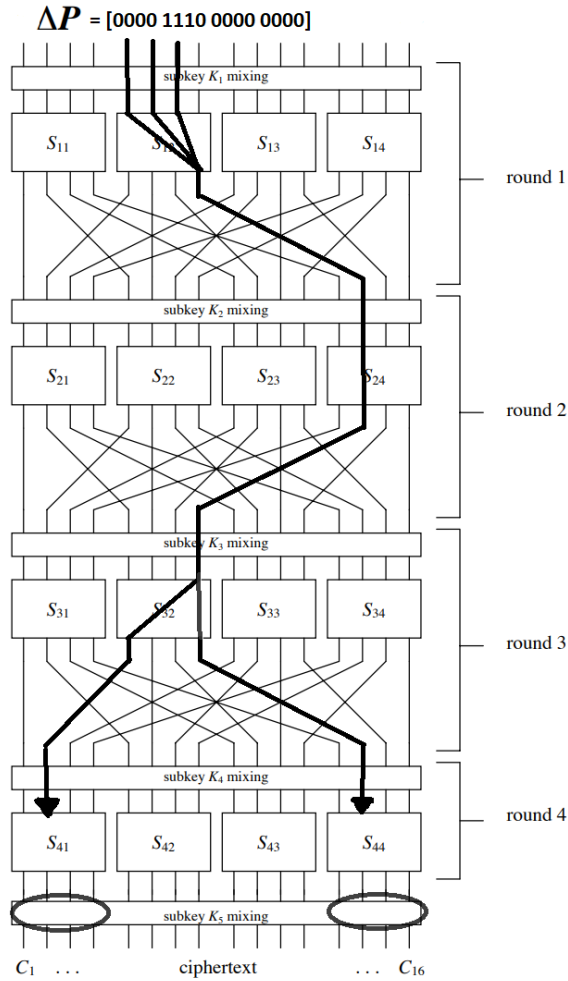
Schéma du SPN démontrant une différentielle caractéristique avec :  $\Delta P = 0000\ 1110\ 0000\ 0000$

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

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

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

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



Après une dernière permutation, on obtient la différentielle intermédiaire suivante  $\Delta I = 0000\ 1001\ 0000\ 0000$  avec probabilité  $\frac{8}{16} * \frac{6}{16} * \frac{6}{16} = \frac{288}{4096} \approx 7\%$