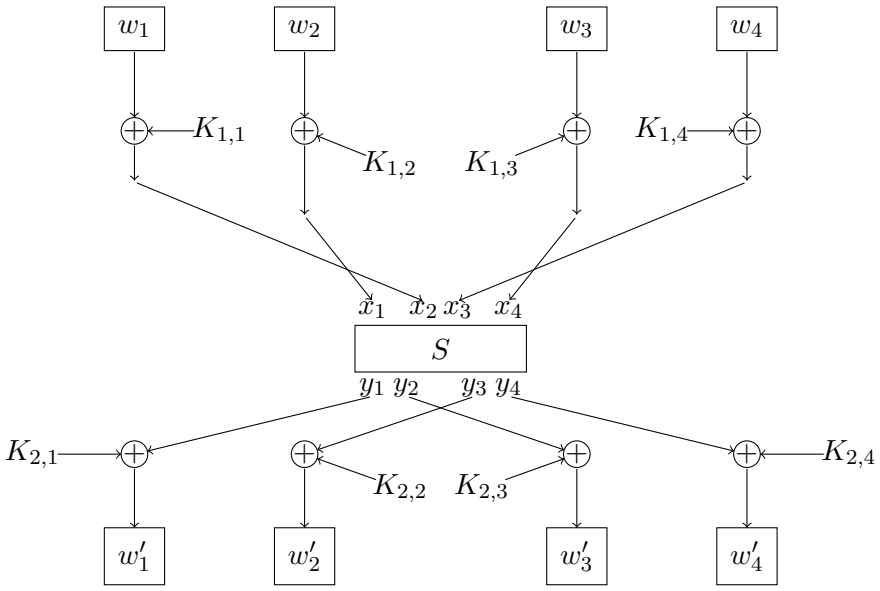
# Examen Final – Cryptographie

**vendredi 16 janvier 2009, 16h – 17h30**

**Solutions**

**Problème 1 (Cryptanalyse différentielle)**
On considère le cryptosystème $E$ sur 4 bits suivant.




La $S$-boîte est donnée par le tableau suivant (entrée : $x_1x_2x_3x_4$, sortie : $y_1y_2y_3y_4$)

| $x_1x_2x_3x_4$ | $y_1y_2y_3y_4$ | $x_1x_2x_3x_4$ | $y_1y_2y_3y_4$ | $x_1x_2x_3x_4$ | $y_1y_2y_3y_4$ | $x_1x_2x_3x_4$ | $y_1y_2y_3y_4$ |
|---|---|---|---|---|---|---|---|
| 0000 | 1110 | 0100 | 0010 | 1000 | 0011 | 1100 | 0101 |
| 0001 | 0100 | 0101 | 1111 | 1001 | 1010 | 1101 | 1001 |
| 0010 | 1101 | 0110 | 1011 | 1010 | 0110 | 1110 | 0000 |
| 0011 | 0001 | 0111 | 1000 | 1011 | 1100 | 1111 | 0111 |

1. Calculer l'image du mot 1011 par le cryptosystème $E$ avec les sous-clés

$$K_1 = K_{1,1}K_{1,2}K_{1,3}K_{1,4} = 0110 \quad \text{et} \quad K_2 = K_{2,1}K_{2,2}K_{2,3}K_{2,4} = 1110$$

*Commençons par écrire les équations qui relient les différents bits :*

$$\begin{aligned} x_1 &= w_2 \oplus K_{1,2} & \qquad w'_1 &= y_1 \oplus K_{2,1} \\ x_2 &= w_1 \oplus K_{1,1} & \qquad w'_2 &= y_3 \oplus K_{2,2} \\ x_3 &= w_4 \oplus K_{1,4} & \qquad w'_3 &= y_2 \oplus K_{2,3} \\ x_4 &= w_3 \oplus K_{1,3} & \qquad w'_4 &= y_4 \oplus K_{2,4} \end{aligned}$$

*On trouve $X = 1110$, d'où $Y = S(1110) = 0000$ et le mot de sortie est* 1110.

2. Justifier pourquoi il est nécessaire d'ajouter une sous-clé avant et après la $S$-boîte.

*La S-boîte fait partie du protocole et donc est* publique. *Si on n'ajoute pas de sous-clé au départ, alors la valeur de $X$, et donc aussi celle de $Y$, est totalement connue à partir de celle de $W$. De même, si on n'ajoute pas de sous-clé en sortie de S-boîte, on peut retrouver la valeur de $X$ en partant de $W'$.*

3. Déterminer l'ensemble $\mathcal{E}$ des mots $X$ de 4 bits tels que

$$S(X \oplus 0100) = S(X) \oplus 1011$$

*Cela revient à déterminer les $X$ tels que*

$$S(X \oplus 0100) \oplus S(X) = 1011. \tag{1}$$

*On trouve l'ensemble suivant*

$$\mathcal{E} = \{0001, 0101, 1011, 1111\}$$

4. En déduire que, pour $X$ un mot aléatoire de 4 bits, on a

$$\text{Prob}\big(S(X \oplus 0100) = S(X) \oplus 1011\big) = \frac{1}{4}$$

*Le mot $X$ peut prendre 16 valeurs distinctes parmi lesquelles seules 4 vérifient l'équation (1). Donc*

$$Prob\big(S(X \oplus 0100) = S(X) \oplus 1011\big) = \frac{4}{16} = \frac{1}{4}$$

5. En déduire que, pour $W$ un mot aléatoire de 4 bits, *et quelles que soient les valeurs des sous-clés $K_1$ et $K_2$*, on a

$$\text{Prob}\big(E(W \oplus 1000) = E(W) \oplus 1101\big) = \frac{1}{4}$$

*On cherche à déterminer la probabilité de l'événement*

$$E(W \oplus 1000) \oplus E(W) = 1101$$

*Notons $M$ et $N$ les deux transformations suivantes sur les mots de 4 bits*

$$M(a_1a_2a_3a_4) = a_2a_1a_4a_3 \quad et \quad N(b_1b_2b_3b_4) = b_1b_3b_2b4$$

*Notons que les fonctions $M$ et $N$ sont linéaires, c'est-à-dire*

$$M(A \oplus B) = M(A) \oplus M(B), \quad N(A \oplus B) = N(A) \oplus N(B)$$

*On a $X = M(W \oplus K_1)$. On pose $\tilde{W} = W \oplus 1000$ et $\tilde{X}$, $\tilde{Y}$, $\tilde{W'}$ les valeurs correspondant. On a*

$$\begin{aligned} X \oplus \tilde{X} &= M(W \oplus K_1) \oplus M(\tilde{W} \oplus K_1) \\ &= M(W \oplus K_1 \oplus \tilde{W} \oplus K_1) \\ &= M(W \oplus \tilde{W}) = M(1000) = 0100 \end{aligned}$$

*Et donc $Y \oplus \tilde{Y} = 1011$ avec une probabilité de $1/4$ et on a alors avec la même probabilité*

$$W' \oplus \tilde{W'} = K_2 \oplus N(Y) \oplus K_2 \oplus N(\tilde{Y}) = N(Y \oplus \tilde{Y}) = N(1011) = 1101$$

6. Quelle est cette probabilité si on remplace $E$ par une fonction aléatoire sur 4 bits ?

   *Dans ce cas la valeur $E(W \oplus 1000) \oplus E(W)$ est une valeur aléatoire dans un ensemble à 16 éléments, donc cette probabilité est de $1/16$.*

7. On considère à présent une attaque à texte clair connu sur le cryptosystème $E$ avec deux sous-clés $K_1$ et $K_2$ inconnues.

(a) Pour le couple message clair/message crypté $(W, E(W)) = (1001, 0001)$, on remarque que

$$E(W \oplus 1000) = E(W) \oplus 1101$$

En déduire les valeurs possibles de la sous-clé $K_1$.

*Par le raisonnement (et les notations) de la question 5, on voit que l'équation*

$$E(W \oplus 1000) = E(W) \oplus 1101$$

*est vérifiée si et seulement si, pour le $X$ correspondant, on a*

$$S(X \oplus 0100) = S(X) \oplus 1011$$

*et donc ssi $X \in \mathcal{E}$. D'un autre côté, on sait que $X = M(W \oplus K_1)$ et on en déduit 4 valeurs possibles pour $K_1$*

$$K_1 = 1011, 0011, 1110, \text{ ou } 0110.$$

(b) Justifier pourquoi il est relativement facile de trouver un tel couple.

*On peut trouver un tel couple avec une probabilité de $1/4$ et donc relativement facilement (notamment par rapport à une probabilité de hasard de $1/16$).*

**Problème 2 (Borne sur la résistance linéaire)**

1. Soit $f$ une fonction booléenne sur $\{0,1\}^n$.

(a) Soit $u \in \{0,1\}^n$, montrer que :

$$\tilde{f}(u)^2 = \sum_{x,y \in \{0,1\}^n} \left( (-1)^{f(x) \oplus f(y)} (-1)^{u*(x \oplus y)} \right)$$

*On a*

$$\begin{aligned}
\tilde{f}(u)^2 &= \left( \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus u*x} \right) \left( \sum_{y \in \{0,1\}^n} (-1)^{f(y) \oplus u*y} \right) \\
&= \sum_{x,y \in \{0,1\}^n} (-1)^{f(x) \oplus u*x \oplus f(y) \oplus u*y} \\
&= \sum_{x,y \in \{0,1\}^n} (-1)^{f(x) \oplus f(y)} (-1)^{u*x \oplus u*y} \\
&= \sum_{x,y \in \{0,1\}^n} (-1)^{f(x) \oplus f(y)} (-1)^{u*(x \oplus y)}
\end{aligned}$$

(b) Montrer que, pour $x$ et $y$ dans $\{0,1\}^n$, on a :

$$\sum_{u \in \{0,1\}^n} (-1)^{u*(x \oplus y)} = \begin{cases} 2^n & \text{si } x = y, \\ 0 & \text{sinon} \end{cases}$$

*Si $x = y$ alors $x \oplus y = 0...0$ et $u * (x \oplus y) = 0$ pour tout $u \in \{0,1\}^n$. Donc on obtient*

$$\sum_{u \in \{0,1\}^n} (-1)^{u*(x \oplus y)} = \sum_{u \in \{0,1\}^n} 1 = card\left(\{0,1\}^n\right) = 2^n$$

*Supposons à présent que $x \neq y$. On pose $z = x \oplus y$, et donc $z \neq 0...0$. Ainsi,, il existe au moins un bit de $z$ égal à 1, disons le bit $i$. Si on prend $u_0$ le mot dont tous les bits sont égaux à 0, sauf le bit $i$ égal à 1, alors, on a $z * u_0 = 1$. On calcule, en utilisant le fait que $u \mapsto u \oplus u_0$ est une bijection sur $\{0,1\}^n$*

$$\begin{aligned}\sum_{u\in\{0,1\}^n}(-1)^{u*z} &= \sum_{u\in\{0,1\}^n}(-1)^{(u\oplus u_0)*z} = \sum_{u\in\{0,1\}^n}(-1)^{u*z\oplus u_0*z}\\ &= \sum_{u\in\{0,1\}^n}(-1)^{u*z}(-1)^{u_0*z} = -\sum_{u\in\{0,1\}^n}(-1)^{u*z}\end{aligned}$$

*ce qui implique que cette somme est nulle.*

(c) En utilisant les deux questions précédentes, montrer que :

$$\sum_{u\in\{0,1\}^n}\tilde{f}(u)^2 = 2^{2n}$$

*En utilisant successivement les questions 1(a) et 1(b), on obtient*

$$\begin{aligned}\sum_{u\in\{0,1\}^n}\tilde{f}(u)^2 &= \sum_{u\in\{0,1\}^n}\sum_{x,y\in\{0,1\}^n}(-1)^{f(x)\oplus f(y)}(-1)^{u*(x\oplus y)}\\ &= \sum_{x,y\in\{0,1\}^n}(-1)^{f(x)\oplus f(y)}\sum_{u\in\{0,1\}^n}(-1)^{u*(x\oplus y)}\\ &= \sum_{\substack{x,y\in\{0,1\}^n\\ x=y}}(-1)^{f(x)\oplus f(y)}\,2^n\\ &= 2^n\sum_{x\in\{0,1\}}(-1)^{2f(x)} = 2^n\sum_{x\in\{0,1\}}1 = 2^n\cdot 2^n = 2^{2n}\end{aligned}$$

2. On pose

$$M = \max_{u\in\{0,1\}^n}\left|\tilde{f}(u)\right|$$

(a) Montrer que

$$\sum_{u\in\{0,1\}^n}\tilde{f}(u)^2 \leq 2^n M^2$$

*On a*

$$\sum_{u\in\{0,1\}^n}\tilde{f}(u)^2 = \sum_{u\in\{0,1\}^n}\left|\tilde{f}(u)\right|^2 \leq \sum_{u\in\{0,1\}^n}M^2 = 2^n\,M^2$$

(b) En déduire, en utilisant la partie 1, que :

$$M \geq 2^{n/2}$$

*Par les résultats de la question 1, on a*

$$2^n\,M^2 \geq \sum_{u\in\{0,1\}^n}\tilde{f}(u)^2 = 2^{2n}$$

*et ainsi*

$$M^2 \geq 2^n \quad \textit{puis} \quad M \geq 2^{n/2}$$

*puisque $M$ est un nombre positif.*

(c) Que peut-on en déduire sur la résistance linéaire de $f$ ?

*En utilisant l'inégalité ci-dessus, on obtient*

$$\begin{aligned}\mathcal{RL}(f) &= 2^{n-1} - \frac{1}{2}\max_{v\in\{0,1\}^n}\left|\tilde{f}(v)\right|\\ &\leq 2^{n-1} - \frac{1}{2}2^{n/2} = 2^{n-1} - 2^{n/2-1}\end{aligned}$$