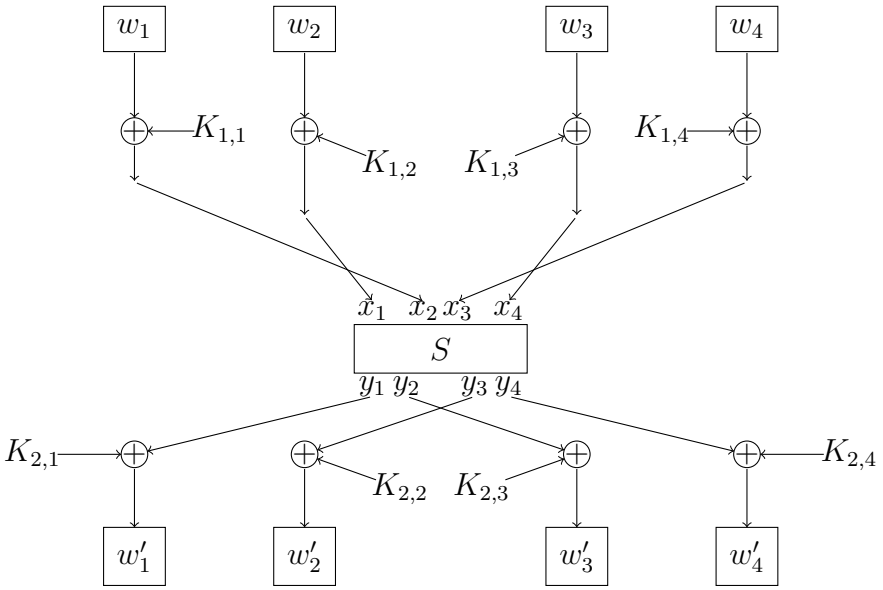
Examen Final – Cryptographie

vendredi 16 janvier 2009, 16h – 17h30

Documents de cours autorisés
Toutes les réponses doivent être soigneusement justifiées

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

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

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

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

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

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

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

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

$$\text{Prob}\big(E(W \oplus 1000) = E(W) \oplus 1101\big) = \frac{1}{4} \tag{2}$$

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

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.

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

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

   (b) Montrer que, pour x et y dans $\{0,1\}^n$, on a :
   $$\sum_{u\in\{0,1\}^n} (-1)^{u*(x\oplus y)} = \begin{cases} 2^n & \text{si } x = y, \\ 0 & \text{sinon} \end{cases}$$

   (c) En utilisant les deux questions précédentes, montrer que :
   $$\sum_{u\in\{0,1\}^n} \tilde{f}(u)^2 = 2^{2n}$$

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

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

   (b) En déduire, en utilisant la partie 1, que :
   $$M \geq 2^{n/2}$$

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