

Examen Partiel - Cryptographie

mardi 7 décembre 2010, 9h – 10h30

Documents de cours autorisés

Toutes les réponses devront être soigneusement justifiées

Exercice 1

On considère le cryptogramme de César modifié de la manière suivante : On identifie les lettres avec les entiers modulo 26 de la manière usuelle :

$$A = 0, B = 1, \dots, Z = 25.$$

La clé est une lettre k . Pour un message clair $m_1, m_2, \dots, m_n, \dots$ le message crypté $c_1, c_2, \dots, c_n, \dots$ est donnée par

$$c_1 = m_1 + k \text{ et } c_i = m_i + c_{i-1} + k.$$

- (1) Crypter le message “PARTIEL” avec la clé E .
- (2) Décrypter le message “GFHVBQ” avec la clé C .
- (3) Que peut-on dire de la sécurité de ce cryptogramme ?

Solution

- (1) TXSPBJY
- (2) EXAMEN
- (3) L'espace des clés (26 lettres) est trop petit pour une sécurité quelconque. De plus, si on pose $d_1 = c_1$ et $d_i = c_i - c_{i-1}$, on obtient le cryptogramme de César habituel qui se casse facilement avec une analyse probabiliste.

Exercice 2

- (1) Soit P un polynôme réduit dans $\mathbb{F}_2[X_1, \dots, X_n]$ non nul. Montrer en détail qu'il existe $(a_1, \dots, a_n) \in \{0, 1\}^n$ tel que $P(a_1, \dots, a_n) \neq 0$.
- (2) Soient P et Q deux polynômes réduits distincts de $\mathbb{F}_2[X_1, \dots, x_n]$. Montrer qu'il définissent deux fonctions booléennes différentes.

Solution

- (1) Par récurrence sur le nombre de variables n . Si $n = 1$, alors $P(X)$ est soit 1, soit X_1 , soit $X_1 + 1$. Dans le deuxième cas on prend $X_1 = 1$, dans le troisième cas $X_1 = 0$.
Supposons le théorème vrai pour des polynômes réduits non-nuls en n variables, et soit $P \in \mathbb{F}_2[X_1, \dots, X_{n+1}]$ réduit non-nul. Par commutativité il existent des polynômes $S, T \in \mathbb{F}_2[X_1, \dots, X_n]$ avec $P = X_{n+1}S + T$. Puisque P est réduit, S et T le sont aussi ; comme P est non-nul, soit S soit T est non-nul et il existe $(a_1, \dots, a_n) \in \{0, 1\}^n$ avec $S(a_1, \dots, a_n) = 1$ ou $T(a_1, \dots, a_n) \neq 1$. Dans le premier cas on prend $a_{n+1} = T(a_1, \dots, a_n) + 1$, dans le deuxième cas on prend $a_{n+1} = 0$.
- (2) Le polynôme $P+Q$ est réduit et non-nul. Donc il existe $(a_1, \dots, a_n) \in \{0, 1\}^n$ avec $(P - Q)(a_1, \dots, a_n) \neq 0$, c'est-à-dire $P(a_1, \dots, a_n) \neq Q(a_1, \dots, a_n)$, et $P \neq Q$.

Exercice 3

Soit a la fonction booléenne vectorielle de $\{0, 1\}^3 \times \{0, 1\}^3 \rightarrow \{0, 1\}^4$ qui correspond à l'addition des entiers < 8 (écrits en base 2, donc 101 correspond à 5).

- (1) Exprimer a à l'aide de $\neg, \wedge, \vee$ et $\oplus$.
- (2) Calculer la représentation algébrique normale de a .

Solution

$$\begin{aligned}
(1) \\
^2 \quad a_1(x_1, x_2, x_3, y_1, y_2, y_3) &= x_1 \oplus y_1 \\
a_2(x_1, x_2, x_3, y_1, y_2, y_3) &= x_2 \oplus y_2 \oplus (x_1 \wedge y_1) \\
a_3(x_1, x_2, x_3, y_1, y_2, y_3) &= x_3 \oplus y_3 \oplus [(x_2 \wedge y_2) \vee (x_2 \vee y_2) \wedge x_1 \wedge y_1] \\
a_4(x_1, x_2, x_3, y_1, y_2, y_3) &= (x_3 \wedge y_3) \vee \{(x_3 \vee y_3) \wedge [(x_2 \wedge y_2) \vee ((x_2 \vee y_2) \wedge x_1 \wedge y_1)]\} \\
(2)
\end{aligned}$$

$$\begin{aligned}
a_1(x_1, x_2, x_3, y_1, y_2, y_3) &= x_1 \oplus y_1 \\
a_2(x_1, x_2, x_3, y_1, y_2, y_3) &= x_2 \oplus y_2 \oplus x_1 y_1 \\
a_3(x_1, x_2, x_3, y_1, y_2, y_3) &= x_3 \oplus y_3 \oplus x_2 y_2 \oplus x_2 x_1 y_1 \oplus y_2 x_1 y_1 \\
a_4(x_1, x_2, x_3, y_1, y_2, y_3) &= x_3 y_3 \oplus (x_3 \oplus y_3)[x_2 y_2 \oplus (x_2 \oplus y_2)x_1 y_1] \\
&= x_3 y_3 \oplus x_3 x_2 y_2 \oplus y_3 x_2 y_2 \oplus x_3 x_2 x_1 y_1 \oplus x_3 y_2 x_1 y_1 \oplus y_3 x_2 x_1 y_1 \oplus y_3 y_2 x_1 y_1
\end{aligned}$$

Exercice 4

On considère un diagramme de Feistel sur les mots binaires de 4 bits, où les fonctions f_1 et f_2 sont donnés par

x	$f_1(x)$	$f_2(x)$
00	11	11
01	10	11
10	01	00
11	00	00

- (1) Crypter le mot 1010 en utilisant ce diagramme.
- (2) Trouver les mots de 4 bits qui sont invariants par ce diagramme de Feistel.
- (3) Encrypter le message binaire suivant par ce diagramme de Feistel en utilisant le mode CBC à deux rondes avec pour IV le mot 0101:

1010 0001 1100 0111

Solution

- (1) 1011
- (2) $w'_2 = f_1(w_1) \oplus w_2 = w_2$, donc $f_1(w_1) = 00$ et $w_1 = 11$. Ensuite,
$$w'_1 = f_2(w'_2) \oplus w_1 = f_2(w_2) \oplus w_1 = w_1,$$
donc $f_2(w_2) = 00$ et $w_2 \in \{10, 11\}$. Les mots invariants sont 1110 et 1111.
- (3) 1111 1110 0001 0101.

Exercice 5 On supposera que les 56 sous-clés de I.D.E.A. soient tous les mêmes. Montrer que tous les bits de la première sous-clé ont la même valeur. En déduire que tous les bits de la clé ont la même valeur.

Solution Soient $k_1, \dots, k_{128}$ les bits de la clé. Puisque toutes les sous-clés sont les mêmes, pour $i \equiv j \pmod{16}$ on a $k_i = k_j$. Aussi pour $j = i + 25 \pmod{128}$ on a $k_j = k_i$ par construction des sous-clés, et comme les sous-clés sont les mêmes. Donc pour $j = i + 9 \pmod{16}$ on a $k_j = k_i$. Alors pour $j = i + \gcd(9, 16)$ on a $k_j = k_i$. Or, $\gcd(9, 16) = 1$. Donc $k_1 = \dots = k_{16}$. Comme toutes les sous-clés sont égales, $k_1 = \dots = k_{16} = k_{17} = \dots = k_{128}$.