Solutions pour l'examen partiel – Cryptographie

vendredi 14 décembre 2007, 13h – 14h30

Exercice 1

Soient X et Y deux variables aléatoires indépendantes. Montrer que

$$H(X,Y) = H(X) + H(Y).$$

Solution. On a

$$H(X,Y) = -\sum_{x\in\Omega_X, y\in\Omega_Y} P(X=x, Y=y)\log_2 P(X=x, Y=y)$$

Et puisque X et Y sont indépendantes, on a

$$P(X=x, Y=y) = P(X=x)P(Y=y)$$

d'où en remplaçant, on trouve

$$\begin{aligned}
H(X,Y) &= -\sum_{x\in\Omega_X, y\in\Omega_Y} P(X=x)P(Y=y)\log_2\Big(P(X=x)P(Y=y)\Big) \\
&= -\sum_{x\in\Omega_X, y\in\Omega_Y} P(X=x)P(Y=y)\Big(\log_2 P(X=x) + \log_2 P(Y=y)\Big) \\
&= -\sum_{x\in\Omega_X, y\in\Omega_Y} P(X=x)P(Y=y)\log_2 P(X=x) \\
&\qquad\qquad -\sum_{x\in\Omega_X, y\in\Omega_Y} P(X=x)P(Y=y)\log_2 P(Y=y) \\
&= -\sum_{x\in\Omega_X} P(X=x)\log_2 P(X=x)\sum_{y\in\Omega_Y} P(Y=y) \\
&\qquad\qquad -\sum_{y\in\Omega_Y} P(Y=y)\log_2 P(Y=y)\sum_{x\in\Omega_X} P(X=x)
\end{aligned}$$

Et on obtient le résultat en utilisant le fait que

$$\sum_{x\in\Omega_X} P(X=x) = \sum_{y\in\Omega_Y} P(Y=y) = 1.$$

Exercice 2

On considère un diagramme de Feistel sur des mots binaires de 4 bits à deux rondes où les fonctions f_1 et f_2 sont les suivantes :

f_1	$00\mapsto 00$,	$01\mapsto 10$,	$10\mapsto 00$,	$11\mapsto 00$
f_2	$00\mapsto 11$,	$01\mapsto 11$,	$10\mapsto 10$,	$11\mapsto 11$

1. Crypter le mot 1001 en utilisant ce diagramme.
   Solution. Le mot 1001 *est codé en* 0101.

2. Trouver tous les mots de 4 bits qui sont invariants par ce diagramme de Feistel.
   Solution. Soit $w_1\cdot w_2$ un mot invariant par le diagramme. On a donc

   $$w_1 = w_1 \oplus f_2(f_1(w_1)\oplus w_2) \quad et \quad w_2 = w_2 \oplus f_1(w_1).$$

   La première équation donne $f_2(f_1(w_1)\oplus w_2) = 00$, or la fonction f_2 ne prend jamais la valeur 00. *Donc il n'existe pas de mot invariant par ce diagramme.*

3. Encrypter le message binaire suivant par ce diagramme de Feistel en utilisant le mode CBC avec pour IV le mot 1111 :

$$1010\,0101\,1011\,1001$$

Solution. On obtient

$$1011\,0110\,0001\,0100$$

Exercice 3
On considère le cryptogramme de César récursif. La procédure de cryptage est la suivante : notons $m_1, m_2, \ldots, m_n, \ldots$ les lettres du message avec la correspondance usuelle entre lettres et entiers modulo 26 :

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

La clé est une lettre K. Le message crypté est alors donné par les lettres $c_1, c_2, \ldots, c_n, \ldots$ avec

$$c_1 = m_1 + K \text{ et pour } i \geq 2,\ c_i = m_i + c_{i-1}.$$

1. Crypter le message "MESSAGE" avec la clé "C".
Solution. On calcule "M+C=O", puis "E+O=S", "S+S=K", etc. Finalement on obtient la version cryptée "OSKCCIM".

2. Décrypter le message "PNAAMUKEI" crypté avec la clé "M".
Solution. On calcule "P-M=D", "N-P=Y", "A-N=N", etc. On obtient ainsi la version décryptée "DYNAMIQUE".

3. Que peut-on dire de la sécurité de ce cryptogramme ?
Solution. L'ensemble des clés possibles est celui des 26 lettres de l'alphabet, donc de taille insuffisante pour assurer la moindre sécurité.
De plus, on peut décrypter toutes les lettres d'un message crypté, sauf la première, sans connaître la clé, juste en faisant la soustraction avec la lettre précédente.

Exercice 4
Effectuer les opérations suivantes dans le corps A.E.S.

1. $\{EF\} + \{39\}$
Solution. On a $\{EF\} = 1110\,1111$ *et* $\{39\} = 0011\,1001$. *En faisant un "ou exclusif", on obtient*

$$\{EF\} + \{39\} = 1110\,1111 \oplus 0011\,1001 = 1101\,0110 = \{D6\}$$

2. $\{C1\} \times \{12\}$
Solution. On utilise les représentations polynômiales (on peut aussi utiliser l'algorithmique donné dans le cours). On a $\{C1\} = X^7 + X^6 + 1$ *et* $\{12\} = X^4 + X$. *On calcule*

$$(X^7 + X^6 + 1) \cdot (X^4 + X) \equiv X^5 + X^4 + X^3 + X^2 + 1 = \{3D\}.$$