# Examen Partiel – Cryptographie

**vendredi 14 décembre 2007, 13h – 14h30**

**Documents autorisées**
**Toutes les réponses devront être soigneusement justifiées**

**Exercice 1**
Soient $X$ et $Y$ deux variables aléatoires indépendantes. Montrer que

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

**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.
2. Trouver tous 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 avec pour IV le mot 1111 :

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

**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”.
2. Décrypter le message “PNAAMUKEI” crypté avec la clé “M”.
3. Que peut-on dire de la sécurité de ce cryptogramme ?

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

1. $\{EF\} + \{39\}$
2. $\{C1\} \times \{12\}$