# Master CSI 2 2007-2008

## Crypto : DS du 3 mars 2008

*Durée : 1h30. Sans document. Les exercices sont indépendants.*

– Exercice 1. On considère le système de chiffrement donné par le tableau suivant, où l'espace des messages en clair est $\mathcal{M} = \{a, b, c, d\}$, l'espace des messages chiffrés $\mathcal{C} = \{1, 2, 3, 4\}$ et l'espace des clés est $\mathcal{K} = \{K_1, K_2, K_3, k_4\}$.

| $\mathcal{K}^{\mathcal{M}}$ | a | b | c | d |
|---|---|---|---|---|
| $K_1$ | 1 | 2 | 3 | 4 |
| $K_2$ | 2 | 1 | 4 | 3 |
| $K_3$ | 3 | 4 | 2 | 1 |
| $K_4$ | 1 | 3 | 4 | 2 |

**a)** Montrer qu'en général ce système n'est pas à confidentialité parfaite. On expliquera précisément pourquoi.

**b)** Trouver les lois de probabilité sur l'ensemble des messages en clair qui rendent tout de même la confidentialité parfaite.

– Exercice 2. On considère le système de signature défini par le tableau suivant, où l'ensemble des messages en clair est $\mathcal{M} = \{a, b, c\}$, l'ensemble des clés $\mathcal{K} = \{K_1, K_2, K_3, k_4\}$, et les six signatures possibles $\{1, 2, 3, 4, 5, 6\}$.

| $\mathcal{K}^{\mathcal{M}}$ | a | b | c |
|---|---|---|---|
| $K_1$ | 2 | 5 | 3 |
| $K_2$ | 2 | 1 | 4 |
| $K_3$ | 6 | 1 | 3 |
| $K_4$ | 6 | 5 | 4 |

Le cryptogramme $C$ est constitué du couple $(M, S_K(M))$ où $S_K(M)$ est la signature du message $M$, définie par la clé $K$ et le tableau ci-dessus. Quelles sont les probabilités de substitution et d'imposture du système ?

– Exercice 3. Soit $f_K$ la fonction de chiffrement d'un chiffre par blocs, par exemple l'AES. On rappelle que le mode CBC chiffre une suite de blocs $M_1 \dots M_n$

en convenant d'un vecteur d'initialisation $C_0$ et, pour $i = 1 \dots n$, en définissant la suite des chiffrés

$$C_i = f_K(C_{i-1} + M_i).$$

On suppose que le $i$-ième bloc chiffré $C_i$ est reçu de manière erronée, c'est-à-dire qu'un bloc différent, $C'_i$, est reçu à la place de $C_i$. Montrer que deux blocs de clair sont corrompus.

– EXERCICE 4. On considère la suite $(a_i)_{i \geqslant 0}$ engendrée par la récurrence linéaire :

$$a_{i+7} = a_{i+6} + a_{i+5} + a_{i+4} + a_{i+3} + a_i$$

et par les conditions initiales $(a_0, a_1, a_2, a_3, a_4, a_5, a_6) = (1000001)$.

**a)** Quel est le polynôme de rétroaction $h(X)$ de cette récurrence ?

**b)** Trouver la complexité linéaire de la suite, en déduire une nouvelle récurrence linéaire satisfaite par la suite, et un autre polynôme de rétroaction $k(X)$. Montrer que $k(X)$ divise $h(X)$.

**c)** Calculer la période de la suite et l'ordre des racines de $k(X)$ ? Qu'observe-t-on ? Commentaire ?