Master CSI 1 2008-2009

Crypto : DS du 2 mars 2009

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 $\mathcal{M} = \{a, b, c\}$, l'espace des messages chiffrés $\mathcal{C} = \{1, 2, 3\}$ et l'espace des clés est $\mathcal{K} = \{K_1, K_2, K_3, K_4, K_5\}$.

$\mathcal{K}^{\mathcal{M}}$	a	b	c
K_1	1	2	3
K_2	3	1	2
K_3	2	3	1
K_4	1	3	2
K_5	2	1	3

Les clés sont, comme d'habitude, choisies indépendantes des messages en clair et avec une loi uniforme. Calculer $P(M = x \,|\, C = y)$ pour $x = a, b, c$ et $C = 1, 2, 3$ en fonction des probabilités $P(M = x)$. La confidentialité du système est-elle parfaite ?

– Exercice 2. Montrer que si un système cryptographique a le même nombre de messages en clair $|\mathcal{M}|$ que de messages chiffrés $|\mathcal{C}|$, alors les probabilités d'imposture et de substitution doivent valoir 1.

– Exercice 3. On considère un système cryptographique où l'ensemble des messages en clair $\mathcal{M}$ est $\{0, 1, \dots, n-1\}$ et l'ensemble des clés et l'ensemble des chiffrés sont tous les deux égaux à $\{0, 1, \dots, n-1\} \times \{0, 1, \dots, n-1\}$. Au message m et à la clé (x, y) le système associe le cryptogramme

$$C = (m, m + x + y \mod n).$$

a) Que pouvez-vous dire de la confidentialité du système ?

b) Calculer les probabilités d'imposture et de substitution.

– Exercice 4. On considère la suite $(a_i)_{i \geqslant 0}$ dont les 12 premiers termes sont

$$1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0 \cdots$$

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

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

a) Quelle est la complexité linéaire de cette suite ?

b) Trouver son polynôme de rétroaction.

c) Est-il irréductible ?

d) Quelle est la période de la suite (a_i) ?