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 ?

– **Solution.** On a :

$$P(M = a \,|\, C = 1) = \frac{P(M = a, C = 1)}{P(C = 1)}.$$

Or

$$P(M = a, C = 1) = P(M = a,\ K \in \{K_1, K_4\}) = P(M = a)P(K \in \{K_1, K_4\})$$

puisque M et K sont indépendantes, soit

$$P(M = a, C = 1) = P(M = a)\frac{2}{5}.$$

Par ailleurs

$$P(C = 1) = P(M = a,\ K \in \{K_1, K_4\}) + P(M = b,\ K \in \{K_2, K_5\}) + P(M = c, K = K_3)$$

soit, toujours par indépendance de M et K,

$$\begin{aligned} P(C=1) &= P(M=a)\frac{2}{5} + P(M=b)\frac{2}{5} + P(M=c)\frac{1}{5} \\ &= \frac{2}{5} - \frac{1}{5}P(M=c). \end{aligned}$$

D'où

$$\boxed{P(M=a \,|\, C=1) = \frac{P(M=a)}{1-\frac{1}{2}P(M=c)}.}$$

Les autres valeurs se calculent de manière analogue. On trouve :

$$\begin{aligned} P(M=b \,|\, C=1) &= \frac{P(M=b)}{1-\frac{1}{2}P(M=c)} \\ P(M=c \,|\, C=1) &= \frac{P(M=c)}{2-P(M=c)} \\ P(M=a \,|\, C=2) &= \frac{P(M=a)}{1-\frac{1}{2}P(M=b)} \\ P(M=b \,|\, C=2) &= \frac{P(M=b)}{2-P(M=b)} \\ P(M=c \,|\, C=2) &= \frac{P(M=c)}{1-\frac{1}{2}P(M=b)} \\ P(M=a \,|\, C=3) &= \frac{P(M=a)}{2-P(M=a)} \\ P(M=b \,|\, C=3) &= \frac{P(M=b)}{1-\frac{1}{2}P(M=a)} \\ P(M=c \,|\, C=3) &= \frac{P(M=c)}{1-\frac{1}{2}P(M=a)}. \end{aligned}$$

On n'a pas $P(M=x \,|\, C=y) = P(M=x)$, la confidentialité du système n'est donc pas 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.

– **Solution.** Pour toute valeur fixée de la clé, la transformation qui associe une valeur du chiffré à une valeur du clair doit être injective, sinon on ne sait pas déchiffrer. Si $|\mathcal{M}| = |\mathcal{C}|$ la transformation est donc bijective, et toute valeur du chiffré est légale. Une imposture est donc toujours réussie en choisissant une valeur quelconque du chiffré. Pour la même raison, une substitution réussit toujours si on remplace le chiffré par une quelconque autre valeur.

– Exercice 3. On considère un système cryptographique où l'ensemble des messages en clair $\mathcal{M}$ est $\{0, 1, \ldots, n-1\}$ et l'ensemble des clés et l'ensemble des chiffrés sont tous les deux égaux à $\{0, 1, \ldots, n-1\} \times \{0, 1, \ldots, n-1\}$. 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.

– **Solution.**

a) Il n'y a pas de confidentialité, le message en clair est une partie explicite du cryptogramme.

b) Il y a n valeurs possibles de $x+y$, et pour chacune de ces valeurs il y a n couples (x, y) distincts atteignant cette valeur. Si on fait l'hypothèse habituelle que la loi des clés est uniforme, alors on en déduit que la loi de $x + y$ est uniforme. une imposture n'est réussie que si l'on devine la bonne valeur de $x + y$, ce qui arrive donc avec probabilité $1/n$.

Si on observe le cryptogramme $C = (c_1, c_2) = (m, m + x + y)$, le calcul de $c_2 - c_1 \mod n$ donne la valeur de $x + y$. Tout cryptogramme

$$C' = (m', m' + c_2 - c_1 \mod n)$$

avec $m' \neq m$ consiste en une substitution réussie. La probabilité de substitution vaut donc 1.

– 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) Quelle est la complexité linéaire de cette suite, en supposant que celle-ci est $\leqslant 6$?

b) Trouver son polynôme de rétroaction.

c) Est-il irréductible ?

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

– **Solution.**

a) La matrice

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_5 \\ a_1 & a_2 & \cdots & a_6 \\ \cdots & & \cdots & \\ a_5 & a_6 & \cdots & a_{10} \end{bmatrix}$$

est de rang plein (de rang 6), la complexité linéaire de la suite est donc au moins 6.

b) On remarque que (éventuellement en résolvant un système linéaire)

$$[a_6, a_7, \ldots, a_{11}] = [1,1,1,0,1,0] = [a_4 \ldots a_9] + [a_2 \ldots a_7] + [a_1 \cdots a_6] + [a_0 \cdots a_5]$$

d'où l'on déduit la récurrence linéaire :

$$a_{i+6} = a_{i+4} + a_{i+2} + a_{i+1} + a_i.$$

Le polynôme de rétroaction est donc :

$$X^6 + X^4 + X^2 + X + 1.$$

c) Oui. Il suffit d'exclure les diviseurs $X, X{+}1, X^2{+}X{+}1, X^3{+}X{+}1, X^3{+}X^2{+}1$.

d) 21.