Master CSI 1 2009-2010

Crypto : DS du 8 mars 2010

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

– EXERCICE 1. 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 $\mathcal{K} = \{K_1, K_2, K_3, k_4, k_5, k_6, k_7\}$, et l'ensemble des cryptogrammes possibles $\{1, 2, 3, 4, 5, 6, 7\}$.

$\mathcal{K}^{\mathcal{M}}$	a	b	c
K_1	1	2	4
K_2	5	1	3
K_3	6	7	1
K_4	2	3	6
K_5	7	5	2
K_6	3	4	7
K_7	4	6	5

a) Le système est-il à confidentialité parfaite ?

b) Quelles sont les probabilités de substitution et d'imposture du système ?

– EXERCICE 2. On considère un sytème de chiffrement dont l'ensemble des messages en clair $\mathcal{M} = \{0, 1\}$ est limité à deux bits, et l'on souhaite que la probabilité de substitution de ce système soit inférieure ou égale à $1/4$. Si m est une valeur du message et k une valeur de la clé on note $c = f(m, k)$ la valeur correspondante du chiffré.

a) Montrer que si $c = f(m, k_0)$ est une valeur du chiffré correspondant aux valeurs m et k_0 du message et de la clé, alors l'ensemble K_c des valeurs de la clé chiffrant m de la même manière, soit

$$K_c = \{k, f(m, k) = c\}$$

est de cardinalité au moins 4, i.e. $|K_c| \geqslant 4$. Montrer de même que l'ensemble F_c des valeurs correspondantes du chiffré du message complémentaire $\overline{m} = m + 1 \mod 2$, soit

$$F_c = \{f(\overline{m}, k), f(m, k) = c\}$$

est de cardinalité au moins 4, i.e. $|F_c| \geqslant 4$.

b) En déduire que l'ensemble des chiffrés $\mathcal{C}$ est de cardinalité au moins 4 et que l'ensemble des clés $\mathcal{K}$ est de cardinalité au moins 16.

c) En déduire un système de chiffrement (on pourra le représenter sous forme d'un tableau) avec $|\mathcal{M}| = 2, |\mathcal{K}| = 16, |\mathcal{C}| = 4$ pour lequel la probabilité de substitution égale 1/4.

d) Que vaut la probabilité d'imposture de votre système ?

e) Votre système est-il à confidentialité parfaite ?

– EXERCICE 3. Soit L une application linéaire de $\{0,1\}^n$ dans $\{0,1\}^n$, c'est-à-dire avec la propriété que $L(x+y) = L(x) + L(y)$ où $+$ désigne l'addition (modulo 2) dans $\{0,1\}^n$. On considère le système de chiffrement par blocs à r rondes qui à tout message en clair $M \in \{0,1\}^n$ associe le cryptogramme $C = f(M)$ par l'intermédiaire des itérés intermédiaires M_i définis par :

$$\begin{aligned} M_0 &= M \\ M_i &= L(M_{i-1} + K_i) 1 \leqslant i \leqslant r \\ C &= M_r \end{aligned}$$

où K_i est la clé de chiffrement associée à ronde i.

a) Étant donné deux messages en clair M et M', montrer que la somme $f(M) + f(M')$ s'exprime simplement et est indépendante des clés K_i.

b) Vous ne connaissez pas les clés K_i mais vous connaissez un clair particulier x ainsi que son chiffré $f(x)$. Montrer comment vous pouvez décrypter simplement n'importe quel chiffré $C = f(M)$.

– EXERCICE 4. Vous chiffrez m fois un même message M par le DES avec des clés différentes à chaque fois. Suivant les valeurs de m que pouvez-vous dire de la probabilité d'obtenir deux fois le même cryptogramme ?

– EXERCICE 5. On considère la suite binaire $a = (a_i)$ qui commence ainsi :

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

a) Trouver le plus petit générateur linéaire qui engendre cette séquence. Quelle est la période de la suite ainsi engendrée ? Quelle est sa complexité linéaire ?

b) Quel est le polynôme de rétroaction $h(X)$ de la suite a ? Le décomposer en facteurs irréductibles.

c) Combien y a-t-il de suites distinctes satisfaisant la récurrence linéaire trouvée en **a)** ? Quelles sont les différentes périodes et les différentes complexités linéaires de ces suites ?