Master CSI 1 2010-2011

Crypto : DS du 18 février 2011

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

– EXERCICE 1. On considère un système de chiffrement où l'espace des messages en clair est $\mathcal{M} = \{a, b, c\}$, l'espace des messages chiffrés est $\mathcal{C} = \{1, 2, 3, 4\}$ et l'espace des clés est $\mathcal{K} = \{K_1, K_2, K_3, K_4, K_5, K_6\}$. Le système est décrit par le tableau suivant :

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

On suppose que les lois des messages en clair et des clés sont les lois uniformes. La clé est indépendante du message en clair.

a) Calculer la probabilité conditionnelle $P(M = c \mid C = 2)$. Le système de chiffrement est-il à confidentialité parfaite ?

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

– **Solution.**

a)

$$\begin{aligned} P(M = c \mid C = 2) &= \frac{P(M = c, C = 2)}{P(C = 2)} = \frac{P(M = c, K = K_4 \text{ou} K_5)}{P(M = c)} \\ &= \frac{P(M = c, K = K_4) + P(M = c, K = K_5)}{P(M = c)} \\ &= \frac{P(M = c)\frac{2}{6}}{P(M = a)\frac{1}{6} + P(M = b)\frac{2}{6} + P(M = c)\frac{2}{6}} \\ &= \frac{2}{5} \end{aligned}$$

b) La probabilité d'imposture vaut $P_I = 5/6$ car si l'on envoie le cryptogramme $C = 3$, on échoue si et seulement si la clé vaut K_4 ce qui arrive avec probabilité $1/6$. Pour que la probabilité d'imposture soit supérieure il faudrait qu'un même cryptogramme apparaisse dans chaque ligne.

La probabilité de substitution vaut $4/5$. Car si le cryptogramme intercepté est 2, il peut être associé aux cinq clés K_1, K_2, K_4, K_5, K_6. Le cryptogramme 3 est un cryptogramme légal pour chacune de ces clés, sauf K_4. Le autres cas ne font pas apparaître une probabilité de substitution plus élevée.

– Exercice 2. On considère la suite binaire a dont les six premiers bits sont 010110 et engendrée par la récurrence

$$a_i = a_{i-3} + a_{i-4} + a_{i-5} + a_{i-6} \mod 2.$$

a) Quelle est la période de cette suite ?

b) Que pouvez-vous dire du polynôme de rétroaction de cette récurrence ?

c) Quelle est la complexité linéaire de cette suite ?

– **Solution.**

a) Le déroulement de la récurrence fait apparaître un motif périodique de période 15.

b) Le polynôme de rétroaction de la récurrence vaut

$$1 + X + X^2 + X^3 + X^6.$$

On constate que la décomposition en facteurs irréductibles de ce polynôme est : $1 + X + X^2 + X^3 + X^6 = (1 + X + X^2)(1 + X^3 + X^4)$

c) Si la même suite est engendré par un polynôme de degré moins élevé, celui-ci doit être un diviseur de $1+X+X^2+X^3+X^6$. Comme $1+X+X^2$ n'engendre que des suites de période 3, le seul choix est $1 + X^3 + X^4$. On constate que la récurrence associée, soit $a_i = a_{i-1} + a_{i-4}$, engendre également la suite. La complexité linéaire de celle-ci vaut donc 4.

– Exercice 3. On rappelle que le mode OFB d'un système de chiffrement consiste à fixer une valeur arbitraire X_0, et à fabriquer la suite définie par la récurrence $X_{i+1} = f_K(X_i)$, puis à définir le cryptogramme $(X_0, C_1, \ldots, C_n)$ (message chiffré) associé au message en clair $(M_1, \ldots, M_n)$ par $C_i = M_i + X_i$. Supposons que la fonction de chiffrement soit une fonction DES. Que pouvez-vous dire de la période de la suite X_i ? En déduire une méthode de cryptanalyse à clair partiellement connu : combien de blocs de clair faut-il connaître pour la mettre en œuvre ?

– **Solution.**

a) La suite (X_i) constitue un générateur pseudo-aléatoire. Comme elle est à valeurs dans un ensemble à 2^{64} éléments, on doit s'attendre à ce que sa période soit de l'ordre de grandeur de 2^{32}. Si l'on dispose d'environ 2^{32} couples clair-chiffré, la suite X_i devient prévisible et on trouve les clairs suivants à partir de leurs chiffrés.

– EXERCICE 4. On souhaite chiffrer un message de un bit $M \in \{0, 1\}$ dont la loi est uniforme par un ensemble $\mathcal{C} = \{a, b, c, d\}$ de quatre chiffrés.

a) Quelle est la plus petite valeur que vous puissiez espérer pour la probabilité de substitution ?

b) Proposer un système qui réalise cette probabilité de substitution (vous choisissez le nombre de clés).

c) Proposer un système qui réalise à la fois la probabilité de substitution précédente et la confidentialité parfaite.

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

e) (Délicat) Quelle est la meilleure (la plus faible) probabilité d'imposture que vous pouvez espérer ?

– **Solution.**

a) Si on intercepte un cryptogramme x quelconque, on n'a plus que trois choix pour faire une substitution. L'un de ces choix est donc le bon avec une probabilité au moins $1/3$. On a donc $P_S \geqslant \frac{1}{3}$.

b) On peut proposer, par exemple :

$\mathcal{K}^{\mathcal{M}}$	0	1
K_1	a	b
K_2	c	d
K_3	d	a
K_4	b	c
K_5	a	c
K_6	d	b

c) Le système précédent n'est pas à confidentialité parfaite, car si on intercepte le cryptogramme a, par exemple, on sait que le message 0 est plus probable que le message 1.

Pour rétablir la confidentialité parfaite il faut introduire plus de clés. Par exemple :

$\mathcal{K}^{\mathcal{M}}$	0	1
K_1	a	b
K_2	a	c
K_3	a	d
K_4	b	a
K_5	b	c
K_6	b	d
K_7	c	a
K_8	c	b
K_9	c	d
K_{10}	d	a
K_{11}	d	b
K_{12}	d	c

d) $P_I = \frac{1}{2}$.

e) La probabilité d'imposture minimale est $1/2$.

La fréquence d'apparition du symbole x dans la première colonne est, lorsque l'on moyenne sur x, de $1/4$ puisqu'il y a quatre valeurs du symbole x. De même pour la deuxième colonne. *Mais* un symbole x donné ne peut jamais apparaître simultanément dans les deux colonnes, car on ne peut pas chiffrer 0 et 1 par le même symbole. Donc la fréquence d'apparition de x dans au moins une colonne est, en moyenne sur x, de $1/2$. Donc il existe au moins une des valeurs de x qui apparait dans la moitié des lignes du tableau, i.e. pour la moitié des clés.