# 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.

– **Solution.** Confidentialité parfaite veut dire que pour tous $m$ et $c$,

$$P(M = m \,|\, C = c) = P(M = m).$$

On regarde donc les probabilités conditionnelles $P(M = m|C = c)$. On constate qu'il y a un problème car les colonnes 1 et 3 ne contiennent pas tous les cryptogrammes possibles. En particulier la probabilité conditionnelle $P(M = a \,|\, C = 4)$ vaut, si elle est definie,

$$P(M = a \,|\, C = 4) = \frac{P(M = a, C = 1)}{P(C = 4)} = 0$$

car $P(M = a, C = 1) = 0$. Donc on ne peut avoir confidentialité parfaite que si $P(M = a) = 0$, ce qui n'est pas le cas en général.

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

– **Solution.** On vient de voir qui si la confidentialité doit être parfaite il faut $P(M = a) = 0$. De même, comme le chiffré «1» n'apparaît pas dans la troisième colonne, on a $P(M = c \,|\, C = 1) = 0$ et on doit donc avoir

$P(M = c) = 0$. Montrons que la confidentialité est parfaite pour toutes les lois de $M$ telles que $P(M = a) = P(M = c) = 0$.
On a

$$\begin{aligned} P(C = 2) &= P(C = 2, M = b) + P(C = 2, M = d) \\ &= P(K = K_1, M = b) + P(K = K_4, M = d) \end{aligned}$$

et avec l'hypothèse habituelle d'indépendance de $K$ et $M$ et d'uniformité de $K$ on obtient

$$P(C = 2) = \frac{1}{4}(P(M = b) + P(M = d)) = \frac{1}{4}.$$

De même,

$$\begin{aligned} P(C = 1) &= P(M = b, K = K_2) + P(M = d, K = K_3) \\ &= \frac{1}{4}(P(M = b) + P(M = d)) = \frac{1}{4}. \\ P(C = 3) &= P(M = b, K = K_4) + P(M = d, K = K_1) \\ &= \frac{1}{4}(P(M = b) + P(M = d)) = \frac{1}{4}. \\ P(C = 4) &= P(M = b, K = K_3) + P(M = d, K = K_1) \\ &= \frac{1}{4}(P(M = b) + P(M = d)) = \frac{1}{4}. \end{aligned}$$

Enfin, puisque chaque chiffré $1, 2, 3, 4$ apparaît exactement une fois dans les colonnes $b$ et $d$, on a, pour $x = b, d$ et toutes les valeurs possibles de $y$, $P(M = x, C = y) = P(M = x, K = K_i)$ pour un certain $i$ et

$$P(M = x, K = K_i) = \frac{1}{4}P(M = x).$$

Donc

$$P(M = x \,|\, C = y) = \frac{P(M = x, C = y)}{P(C = y)} = \frac{\frac{1}{4}P(M = x)}{\frac{1}{4}} = P(M = x).$$

– 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 ?

– **Solution.** On constate que si toutes les signatures apparaîssent exactement deux fois dans une colonne (pour un même message $M$ donc). De plus, si pour toute autre valeur du message, les signatures correspondant aux deux clés possibles sont différentes, on a donc une chance sur deux de réussir une substitution. Par exemple, si on intercepte $(a, 2)$, on a :

$$P(S(b) = 5 | S(a) = 2) = \frac{P(S(a) = 2, S(b) = 5)}{P(S(a) = 2)} = \frac{P(K = K_1)}{P(K \in \{K_1, K_2\})} = \frac{1/4}{1/2} = \frac{1}{2}.$$

De même pour tous les autres cas : la probabilité de substitution vaut donc $P_S = 1/2$.

La probabilité d'imposture est celle de réaliser une signature authentique a priori. On remarque qu'une signature apparaît dans chaque colonne soit zéro fois, soit deux fois. Si l'on choisit une signature qui apparaît deux fois, par exemple $(a, 2)$, la probabilité qu'elle soit authentique vaut

$$P(K = K_1 \text{ ou } K = K_2) = \frac{1}{2}$$

de même dans les autres cas. On a donc $P_I = 1/2$.

– 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.

– **Solution.** Le déchiffrement de $M_i$ se fait à l'aide de $C_i$ et $C_{i-1}$ en calculant $M_i = f_K^{-1}(C_i) + C_{i-1}$. Supposons $C_i$ corrompu : tous les $M_j$ pour $j < i$ sont clairement déchiffrés correctement. Par contre le déchiffrement de $C'_i$ donne

$$M'_i = f_K^{-1}(C'_i) + C_{i-1} = M_i + (f_K^{-1}(C_i) + f_K^{-1}(C'_i))$$

qui est systématiquement erroné si $f_K$ est bijective (et avec une probabilité très forte sinon). Le déchiffrement du cryptogramme suivant $C_{i+1}$ donne

$$M'_{i+1} = f_K^{-1}(C_{i+1}) + C'_i = M_i + (C_i + C'_i)$$

qui est toujours différent de $M_i$. Par contre, $M_{i+2} = f_K^{-1}(C_{i+2}) + C_{i+1}$ est correct, ainsi que les $M_j$, $j > i+2$.

– 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 ?
– **Solution.** $h(X) = X^7 + X^6 + X^5 + X^4 + X^3 + 1$.

**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 $h(X)$.
– **Solution.** La complexité linéaire de la suite $(a_i)$ est le plus petit entier $\lambda > 0$ tel que la suite $(a_{i+\lambda})$ soit une combinaison linéaire des suites $(a_i), (a_{i+1}), \ldots, (a_{i+\lambda-1})$. On sait déjà que $\lambda$ est au plus 7, mais elle pourrait être plus petite. Testons l'existence ou non de cette combinaison linéaire sur les 7 premiers bits de la suite. On commence par calculer, en utilisant la récurrence qui définit $(a_i)$, $[a_0 \ldots a_{12}] = [1000001010010]$. Puis on forme la matrice

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_6 \\ a_1 & a_2 & \cdots & a_7 \\ \vdots & \vdots & \vdots & \vdots \\ a_6 & a_7 & \cdots & a_{12} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Un examen rapide des six premières lignes montre qu'elles sont indépendantes (La sous-matrice $6\times 6$ supérieure droite est triangulaire). La complexité linéaire est donc au moins 6. On s'aperçoit par contre que la dernière ligne est combinaison linéaire des précédentes, si l'on numérote les lignes en partant du haut par $\ell_0 \ldots \ell_6$ on a

$$\ell_6 = \ell_4 + \ell_2 + \ell_1 + \ell_0.$$

Si la suite $(a_{i+6})$ doit être combinaison linéaire de $(a_i) \ldots (a_{i+5})$ ce ne peut donc qu'être

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

Il reste à vérifier que cette relation a bien lieu pour tout $i$, et pas seulement pour $i = 0 \ldots 6$. Or la suite $(a'_i)$ définie par (1) et les mêmes conditions initiales que $(a_i)$ vérifie

$$\begin{aligned} a'_{i+6} &= a'_{i+4} + a'_{i+2} + a'_{i+1} + a'_i \\ a'_{i+7} &= a'_{i+5} + a'_{i+3} + a'_{i+2} + a'_{i+1}. \end{aligned}$$

On constate que la somme des ces deux égalités donne la même récurrence linéaire qui définit $(a_i)$. Les suites $(a_i)$ et $(a'_i)$ sont donc égales et la récurrence $(1)$ est une autre manière de définir $(a_i)$. La complexité linéaire de $(a_i)$ est donc $6$ et l'on a :

$$k(X) = X^6 + X^4 + X^2 + X + 1.$$

On constate que $h(X) = k(X)(X+1)$.

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

– **Solution.** Le développement d'une récurrence qui définit la suite fait apparaître la période $21$. On vérifie rapidement que $k(X)$ n'a pas de facteur irréductible de degré $1$, $2$ $(X^2+X+1)$ et $3$ $(X^3+X+1,\ X^3+X^2+1)$ : le polynôme $k(X)$ est donc irréductible. L'ordre de ses racines est donc un diviseur de $2^6 - 1 = 63$. La théorie nous dit que l'ordre des racines de $k(X)$ doit être égal à la période de $(a_i)$, ce que l'on peut vérifier par le calcul.