Master CSI 1 2012-2013

Crypto : DS du 4 mars 2013

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 $\mathcal{C} = \{1, 2, 3, 4\}$ et l'espace des clés est $\mathcal{K} = \{K_1, K_2, K_3, K_4, K_5, K_6\}$.

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

Les clés sont, comme d'habitude, choisies indépendantes des messages en clair et avec une loi uniforme.

a) Calculer $P(M = x \,|\, C = y)$ pour $x = a$ et $C = 1, 2, 3, 4$ en fonction des probabilités $P(M = x)$. La confidentialité du système est-elle parfaite ?

b) En supposant maintenant que la loi de M est uniforme, calculer pour chaque valeur $y = 1, 2, 3, 4$, la loi de K sachant $C = y$, c'est-à-dire donner les probabilités $P(K = k \,|\, C = y)$.

– EXERCICE 2. Proposez un système de *signature*, c'est-à-dire que chaque cryptogramme transmis est de la forme $C = (M, S)$ où M est le message en clair, qui remplit les conditions suivantes :
– l'ensemble des messages en clair est $\mathcal{M} = \{0, 1\}$,
– les probabilités d'imposture et de substitution valent toutes les deux $1/4$.
Quel est le minimum de clés qu'il faut pour remplir ces conditions ?

– EXERCICE 3. On considère deux éléments M et M' de $\{0, 1\}^{64}$ qui diffèrent juste sur un bit, en position i. On rappelle que la fonction E d'expansion du DES prend 32 bits en entrée, et en duplique 16 d'entre eux pour donner 48 bits de sortie.

Les messages M et M' sont soumis à un seul tour du DES (au lieu des 16 du DES complet) pour donner les sorties C et C'.

a) Discuter le nombre de positions où C et C' diffèrent : on distinguera
- le cas où i est un des 32 bits de la partie gauche L,
- le cas où i est un des 16 bits non dupliqués de la partie droite R,
- le cas où i est un des 16 bits dupliqués de la partie droite R.

b) Même question lorsque cette fois on soumet les messages M et M' à deux tours du DES.

– EXERCICE 4. On considère la suite binaire $(a_i)_{i\geqslant 0}$ dont les 18 premiers termes sont

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

a) En supposant que la suite (a_i) est engendrée par un récurrence linéaire de degré raisonnable, trouver son polynôme de rétroaction.

b) Est-il irréductible ?

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

d) On considère maintenant la suite $b = (b_i)_{i\geqslant 0}$, définie par $b_i = b_{3i}$, soit

$$b = a_0, a_{3i}, a_{6i}, a_{9i}, a_{12i}, \ldots = 0, 0, 0, 0, 0, 1, \ldots$$

Quelle est la période de (b_i) ?

e) Trouver la complexité linéaire et le polynôme de rétroaction de (b_i).