Master CSI 1 2014-2015

Crypto : DS du 2 mars 2015

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

– Exercice 1. On considère la matrice binaire dont les lignes sont constituées des sept décalages circulaires du mot binaire [1101000], soit

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{1}$$

On cherche à en déduire un système de chiffrement, où
– l'espace des messages en clair est $\{a, b, c\}$, soit de taille 3 égale au poids des lignes de (1) ;
– l'espace des cryptogrammes est $\{1, 2, \ldots, 7\}$,
– l'espace des clés est l'ensemble des lignes du tableau (1) noté

$$\{i, ii, iii, iv, v, vi, vii\}.$$

La donnée de la clé détermine les trois valeurs autorisées du cryptogramme en associant à la ligne de la matrice (1) son support.

Par exemple, la clé i donne les trois valeurs du cryptogramme $1, 2, 4$. La clé iv donne les valeurs $4, 5, 7$. Le système de chiffrement n'est pas encore entièrement déterminé car on n'a pas spécifié, pour chaque clé k, la correspondance entre les valeurs $\{a, b, c\}$ du clair et les 3 valeurs du cryptogramme.

a) Montrer que la probabilité de substitution du système est indépendante de la manière dont on termine de spécifier le de chiffrement et la calculer.

b) Montrer qu'il est possible de spécifier le système de chiffrement de telle sorte que chaque valeur $1, 2, \ldots, 7$ du cryptogramme soit le chiffré de a pour exactement une valeur de la clé, le chiffré de b pour exactement une valeur de la clé, et le chiffré de c pour exactement une valeur de la clé.

c) Dans ce cas montrer que le système est à confidentialité parfaite.

d) Quelle est la probabilité d'imposture du système ?

e) Montrer que quel que soit un système cryptographique à 3 valeurs du clair, 7 valeurs de la clé, et 7 valeurs du cryptogramme, la probabilité de substitution ne peut être inférieure à la valeur calculée en **a)**. On pourra supposer que l'espace des messages en clair est muni de la loi uniforme.

– Exercice 2. On rappelle que le mode OFB d'un système de chiffrement consiste à fixer une valeur arbitraire S_0, et à fabriquer la suite définie par la récurrence $S_{i+1} = f_K(S_i)$, puis à définir le cryptogramme $(C_0 = S_0, C_1, \ldots, C_n)$ (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 AES. Que pouvez-vous dire de la période typique 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 ?

– Exercice 3. 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 ?