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 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.

– **Solution.**

a) Un cryptogramme fixé ne peut être engendré que par exactement trois clés : chaque valeur de la clé associe deux autres valeurs du cryptogramme, qui sont disjointes de celles obtenues par les deux autres valeurs de la clé. On ne peut donc réussir une substitution qu'en pariant sur la valeur de la clé : $P_S = 1/3$.

b) Par exemple avec le tableau, dont les colonnes sont indexées par $\{a, b, c\}$ et dont les lignes sont indexées par les clés $i, ii, \ldots, vii$.

$$\begin{bmatrix} 1 & 2 & 4 \\ 2 & 5 & 3 \\ 4 & 3 & 6 \\ 5 & 4 & 7 \\ 6 & 1 & 5 \\ 7 & 6 & 2 \\ 3 & 7 & 1 \end{bmatrix}$$

c) Il s'agit de voir que pour tous m, c, $P(M = m|C = c) = P(M = m)$. Or on a :

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

Comme $M = m$ et $C = c$ ne peut se produire que pour une seule valeur de la clé, et que la clé est indépendante du message, on a $P(M = m, C = c) = P(M = m, K = k) = P(M = m)\frac{1}{7}$. Par ailleurs, comme le cryptogramme c apparaît dans chaque colonne exactement une fois, on a $P(C = c) = P(M = a, K = x) + P(M = b, K = y) + P(M = c, K = z)$ pour trois valeurs distinctes de la clé x, y, z, donc

$$P(C = c) = P(M = a)\frac{1}{7} + P(M = b)\frac{1}{7} + P(M = c)\frac{1}{7}$$

soit $P(C = c) = 1/7$, d'où le résultat.

d) $P_I = 3/7$.

e) On intercepte un cryptogramme, mettons 1 sans perte de généralité. Si 1 n'apparaît que dans trois lignes, ou moins, du tableau, la probabilité de substitution vaut au moins $1/3$ en mettant une valeur quelconque de ces trois lignes. Si 1 apparaît dans quatre, cinq ou six lignes. Alors, comme il n'y a que 6 valeurs du cryptogramme à répartir entre ces lignes, l'une d'entre elles doit apparaître

dans au moins deux lignes, et si on la choisit, la probabilité de réussir la substitution est au moins $2/6 = 1/3$. Enfin, si 1 apparaît dans les 7 lignes, alors si on intercepte un quelconque message différent de 1, le substituer par 1 réussit avec probabilité 1.

– 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 $C_i = M_i + S_i$. Supposons que la fonction de chiffrement soit une fonction AES. Que pouvez-vous dire de la période typique de la suite S_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.** La période typique de la suite (S_i), si on assimile f_K à une fonction aléatoirement choisie, doit être d'ordre de grandeur $2^{64} = \sqrt{2^{128}}$. L'hypothèse d'assimiler f_K à une fonction aléatoire est empirique, mais raisonnable dans la mesure où f_K n'a absolument pas été choisie pour ses propriétés de période, mais l'a été justement pour ressembler le plus possible à une fonction aléatoire. Dans ces conditions, si on connait le clair sur les 2^{64} premiers chiffrés on connait la suite (S_i) entièrement et on peut décrypter le reste. Bien sûr cette cryptanalyse est surtout théorique, car 2^{64} reste très grand, mais elle est tout de même beaucoup moins coûteuse que la recherche de la clé par force brute (complexité 2^{128}).

– 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 ?

– **Solution.**

a) On trouve que la suite satisfait la récurrence $ai + 5 = a_{i+1} + a_i$ et aucune récurrence linéaire de degré inférieur. La complexité linéaire de la suite vaut donc 5. On constate en déroulant le reste de la suite que la période vaut $\pi = 21$.

b) $h(X) = X^5 + X + 1$. On a $h(X) = (X^2 + X + 1)(X^3 + X + 1)$.

c) Il y a autant de suites que de conditions initiales, soit $2^5 = 32$. Si une suite satisfait une récurrence associée au polynôme $p(X)$, elle satisfait aussi toutes

les récurrences associées aux polynômes multiples de $p(X)$. Donc les autres suites satisfaisant $a_{i+5} = a_{i+1} + a_i$ doivent avoir pour polynôme de rétroaction un diviseur de $h(X)$, soit 1, X^2+X+1, X^3+X+1. Les complexités linéaires associées sont donc 0 (pour la suite nulle), 2 et 3. Les périodes associées sont 1, 3, 7 et 21.