Master CSI 1 2023-2024

Cryptologie — 4TCY802U

Devoir Surveillé — lundi 4 mars 2024

Documents non autorisés

1 Soit la matrice

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 2 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix}.$$

On définit un système de chiffrement pour lequel $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{1, 2, 3\}$ et où on associe à la clef i et au message clair j le message chiffré $a_{i,j}$. Pour tout i, on pose $p_i := P(M = i)$ et on suppose que $p_1 = 1/4$, $p_2 = 1/2$, $p_3 = 1/4$. On suppose que les choix de clefs sont équiprobables et on suppose que ce choix est indépendant de celui du message.

(a) Montrer que le système de chiffrement n'est pas parfaitement sûr.

(b) Changer le contenu d'une seule entrée de la matrice de manière à rendre le système parfaitement sûr. Bien redémontrer que le système obtenu est parfaitement sûr.

2 On considère la suite $z = (z_t)_{t \geqslant 0}$ dont les vingt premiers bits sont :

$$1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1.$$

On sait que cette suite provient d'un LFSR et que sa complexité linéaire est $\leqslant 6$.

(a) Déterminer un polynôme de rétroaction possible. Quelle est la valeur du 21^e bit de la suite ?

(b) Quel est la complexité linéaire de la suite ? Quelle est sa période ?

3 On note $E(k, m) = c$ un chiffrement par bloc prenant en entrée un clair m de n bits et une clef k de ℓ bits et produisant un chiffré c de n bits. Montrer que les trois fonctions de compression f_1, f_2 et f_3 suivantes ne sont pas à sens-unique :

(a) f_1 qui a une chaîne de bits $x \in \{0,1\}^\ell$ et une chaîne de bits $y \in \{0,1\}^n$ associe $f_1(x||y) = E(x, y)$;

(b) f_2 qui a une chaîne de bits $x \in \{0,1\}^n$ et une chaîne de bits $y \in \{0,1\}^n$ associe $f_2(x||y) = E(y,x) \oplus y$, en supposant $n = \ell$;

(c) f_3 qui a une chaîne de bits $x \in \{0,1\}^n$ et une chaîne de bits $y \in \{0,1\}^n$ associe $f_3(x||y) = E(y,y) \oplus x$, en supposant $n = \ell$.

4 On pose $p = 67$. On note $g = 2$ dans $(\mathbf{Z}/p\mathbf{Z})^*$.

(a) Montrer que g est une racine primitive modulo p.

(b) Alice et Bob décident d'utiliser le protocole de Diffie-Hellman dans le groupe engendré par g. Alice choisit l'exposant secret $a = 5$ et Bob l'exposant secret $b = 11$. Que s'échangent-ils sur le canal et quel est leur secret partagé à l'issue du protocole ? Calculer les valeurs.

(c) Soit A la quantité envoyée par Alice à Bob et B la quantité envoyée par Bob à Alice. Soit $q = (p-1)/3 = 22$. Une observatrice malintentionnée, Ève, intercepte A, l'élève à la puissance q, et remplace le message à destination de Bob par A^q. De même elle remplace le message B à destination d'Alice par B^q. Montrer que, quelles que soient les valeurs secrètes a et b choisies par Alice et Bob, le « secret » partagé ainsi arrangé par Ève ne peut prendre que trois valeurs : lesquelles ?

5 On rappelle que le mode OFB d'un système de chiffrement par bloc consiste à fixer une valeur arbitraire $z_0 = IV$, et à fabriquer la suite définie par la récurrence $z_{i+1} = E(k, z_i)$ pour $i \geqslant 0$, puis à chiffrer une suite de blocs $m_1, m_2 \ldots$ par $c_1, c_2 \ldots$ tels que $c_i = m_i \oplus z_i$ pour tout i. Supposons que la fonction de chiffrement E soit l'AES.

Que pouvez-vous dire de la période typique de la suite (z_i) ? Vous faites une attaque à chiffrés choisis : vous pouvez obtenir le déchiffrement m_i de certains blocs c_i (mais pas tous !). Combien de blocs de clair vous faut-il connaître pour déchiffrer la communication toute entière ?