Master CSI 1 2024-2025

Cryptologie — 4TCY802U

Devoir Surveillé — jeudi 13 mars 2025

Documents non autorisés

$\boxed{1}$ Soit la matrice $A = (a_{i,j})_{1 \leqslant i,j \leqslant 3}$ définie par

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

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 $p_1 = 1/2$, $p_2 = 1/4$, $p_3 = 1/4$. 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) Intervertir deux entrées de la matrice de manière à rendre le système parfaitement sûr. Bien redémontrer que le système obtenu est parfaitement sûr.

$\boxed{2}$ On considère la suite binaire $u = (u_t)_{t \geqslant 0}$ engendrée par la relation de récurrence pour tout $t \geqslant 0$,

$$u_{t+5} = u_{t+2} + u_t,$$

et d'initialisation $(u_0, \ldots, u_4) = (1, 0, 0, 0, 1)$.

On considère également la suite binaire v périodique de période 4,

$$v : 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, \ldots$$

(a) Sans calculer les termes suivants de la suite u, déterminer sa complexité linéaire et sa période.

(b) Sans calcul dire si la suite v est une m-suite ou non ? (Justifier)

(c) Trouver la récurrence linéaire la plus courte satisfaire par v.

(d) Soit $z = u + v$. Quelle est la complexité linéaire de la suite z ?

$\boxed{3}$ On note $||$ la concaténation de chaînes de bits.

Soient un entier $\ell \geqslant 1$ et une application $f : \{0,1\}^\ell \to \{0,1\}^\ell$. Pour tout bloc $L||R \in \{0,1\}^{2\ell}$, où L et $R \in \{0,1\}^\ell$ sont les parties gauche et droite du bloc, on pose

$$T_f(L||R) = L \oplus f(L \oplus R) \;||\; R \oplus f(L \oplus R).$$

On considère le schéma de chiffrement symétrique suivant : on chiffre un bloc $L||R$ en appliquant successivement les transformations $T_{f_1}, T_{f_2}, \ldots, T_{f_s}$ où $s \geqslant 1$ et où les f_i sont des applications de $\{0,1\}^\ell$ dans lui-même. La donnée de ces applications $f_1, \ldots, f_s$ constitue la clef secrète.

(a) Donner un algorithme de déchiffrement.

(b) Peut-on distinguer ce schéma d'une transformation aléatoire ? Si oui, comment ?

(c) Montrer que la transformation T_f correspond à un schéma de Feistel comportant trois tours $L||R \to R||(L \oplus g_i(R))$ avec $1 \leqslant i \leqslant 3$ avec une permutation finale des parties gauche et droite et où les g_i sont des applications de $\{0,1\}^\ell$ dans lui-même que l'on précisera.

$\boxed{4}$ Soient q un nombre premier et $(G, \times)$ un groupe cyclique d'ordre q. On note g un générateur de G. On utilise une variante du chiffrement Elgamal. La clef secrète est un entier aléatoire x avec $1 < x < q$. La clef publique est $h = g^x$. Pour chiffrer un message $m \in G$ avec la clef publique h, on prend au hasard un entier r avec $1 < r < q$. Le chiffré de m est le couple $c := (c_1, c_2) := (mg^r, h^r) \in G \times G$.

(a) Dans cette question seulement on considère une application numérique sur un petit exemple. On pose $p = 71$ et on considère le sous-groupe G de $(\mathbf{Z}/p\mathbf{Z})^\times$ engendré par $g = 20$. Quel est l'ordre de g ? Bob a pour clef publique $h = 48$. Quel est sa clef privée ? Donner le chiffré pour cette clef publique de $m = 20$ avec l'aléa $r = 2$.

(b) Retour au cas général pour la suite de l'exercice. Donner un algorithme de déchiffrement.

(c) Alice et Bob utilisent tous les deux cette variante du chiffrement Elgamal. On note h_A la clef publique d'Alice et x_A sa clef privée. De même, on note h_B la clef publique de Bob et x_B sa clef privée. On suppose que Carl connaît la quantité $x_B x_A^{-1} \mod q$. On note c_A un chiffré de m utilisant la clef publique d'Alice. Montrer que Carl peut transformer c_A en un chiffré c_B que Bob pourra déchiffrer pour retrouver m. Montrer que Carl peut également transformer un chiffré c'_B de m' utilisant la clef publique de Bob en un chiffré c'_A de m' déchiffrable par Alice.