Master CSI 2 2016-2017

Cryptanalyse — 4TCY902U

Responsable : G. Castagnos

Devoir surveillé — 25 octobre 2016

Durée 1h30
accès aux fonctions programmées en TP, aux énoncés des TP et à la fiche d'initiation à Sage autorisés, autres documents non autorisés
Les deux exercices sont indépendants.

1 Exercice théorique

Soit $n > 1$ un entier. Soit L un réseau de dimension n de R^n et soit B une matrice $n \times n$ à coefficients entiers dont les lignes constituent une base de L. Soit P une matrice $n \times n$ à coefficients entiers telle que $det\ \mathrm{P} = \pm 1$. On note $\mathrm{B}' = \mathrm{PB}$ une autre base de L. On note σ un petit entier.

On considère le chiffrement à clef publique suivant. La clef publique est la base B', la clef privée la base B.

Pour chiffrer m un vecteur de $\mathbf{Z}^n$ avec la clef publique B', on tire au hasard un vecteur $e \in \mathbf{Z}^n$, dont les coordonnées sont $\pm\sigma$. Le chiffré c de m est le vecteur $c = m\mathrm{B}' + e$.

Pour déchiffrer c avec la clef privée B, on calcule le vecteur $v = c\mathrm{B}^{-1} \in \mathbf{Q}^n$, puis on ressort $\lfloor v \rceil \mathrm{P}^{-1}$, où $\lfloor v \rceil$ désigne le vecteur de $\mathbf{Z}^n$, où chaque coordonnée de v a été arrondie à l'entier le plus proche.

(a) Soit $c = m\mathrm{B}' + e$ un chiffré de m. On note $u = (u_1, \dots, u_n) = e\mathrm{B}^{-1} \in \mathbf{Q}^n$. Montrer que si pour tout $i \in \{1, \dots, n\}$, $|u_i| < 1/2$ alors le déchiffrement de c retourne bien m.

(b) On note ρ le maximum des normes 1 des colonnes de B^{-1} : $\rho = max_{1 \leqslant j \leqslant n} \sum_{i=1}^{n} |x_{i,j}|$ où les $x_{i,j}$ sont les coefficients de la matrice B^{-1}. Déduire de la question précédente que si $\sigma < 1/(2\rho)$ alors le déchiffrement de $c = m\mathrm{B}' + e$ retourne bien m.

(c) Soit c un chiffré avec la clef publique B'. Expliquer comment décrypter c sans connaître la clef secrète en utilisant le réseau engendré par la matrice $(n+1) \times (n+1)$:

$$\mathrm{M} := \begin{pmatrix} & & 0 \\ & \mathrm{B}' & \vdots \\ & & 0 \\ & c & 1 \end{pmatrix}$$

(d) On pose $s = (\sigma, \dots \sigma) \in \mathbf{Z}^n$. Soit c un chiffré de m avec la clef publique B'. Que vaut $c + s$ $(mod\ 2\sigma)$ (c'est à dire le vecteur dont toutes les coordonnées sont modulo 2σ) ? En supposant que B' est inversible modulo 2σ, montrer que l'on peut obtenir de l'information sur m et améliorer l'attaque de la question précédente.

2 Exercice pratique (à part la première question)

On considère le générateur de suite chiffrante suivant. On utilise deux LFSR : $\mathrm{LFSR_P}$ et $\mathrm{LFSR_Q}$ de longueurs respectives ℓ_P et ℓ_Q. Les états initiaux des deux LFSR notés K_P et K_Q constituent la clef secrète. Les rétroactions de ces deux LFSR sont publiques, on note P (resp. Q) le polynôme de rétroaction du $\mathrm{LFSR_P}$ (resp. du $\mathrm{LFSR_Q}$).

Après avoir chargées les clefs, on met à jour les deux LFSR 100 fois sans produire de suite chiffrante.
Puis à chaque tour,

1. Les $\mathrm{LFSR_P}$ et $\mathrm{LFSR_Q}$ sont mis à jour, produisant deux bits p et q ;
2. Si $p = 1$ alors le bit de sortie du générateur est q,
3. Sinon si $p = 0$, alors le bit de sortie du générateur est $1 \oplus q$.

Par exemple, avec le $\mathrm{LFSR_P}$, de longueur $\ell_P = 2$, de polynôme de rétroaction $P = 1+X+X^2$ initialisé par $K_P = [0, 1]$ et le $\mathrm{LFSR_Q}$ de longueur $\ell_Q = 3$ de polynôme de rétroaction $Q = 1 + X + X^3$ initialisé par $K_Q = [0, 1, 1]$, la suite produite par le générateur est $1, 1, 1, 1, 0, 1, 1, 1, 0, 0$ ...

(a) Expliquer comment Alice et Bob peuvent utiliser ce générateur afin de s'échanger N bits de manière confidentielle.

(b) Donner le code d'une fonction qui produit N bits par ce générateur. Elle doit prendre en entrée les clefs K_P et K_Q, et les polynômes de rétroaction P et Q des $\mathrm{LFSR_P}$ et $\mathrm{LFSR_Q}$ et l'entier N. Donner les 5 premiers bits produits par le générateur avec : $\ell_P = 4, K_P = [1, 1, 1, 0]$, $P = 1 + X + X^4$, $\ell_Q = 6, K_Q = [1, 0, 1, 1, 1, 0], Q = 1 + X + X^3 + X^4 + X^6$.

(c) Avec $\ell_P = 4, K_P = [0, 0, 0, 1], P = 1+X+X^4, \ell_Q = 6, Q = 1+X+X^3+X^4+X^6$, les 10 premiers bits du générateur sont $0, 1, 1, 1, 0, 1, 1, 0, 1, 1$. Quel est la valeur de la clef K_Q ? Expliquer la méthode utilisée, pas forcément tout le code.

Indication: Il pourra être utile d'utiliser la matrice de rétroaction d'un LFSR : Pour un LFSR de longueur ℓ et de polynôme de rétroaction $f(X) = 1+c_1X+c_2X^2+\cdots+c_\ell X^\ell$ c'est la matrice $\ell \times \ell$ à coefficients dans $\mathbf{F}_2$:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 \\ c_\ell & c_{\ell-1} & \dots & c_3 & c_2 & c_1 \end{pmatrix}$$

(d) Avec $\ell_P = 4$, $P = 1 + X + X^4$, $\ell_Q = 20$, $Q = X^{20} + X^{10} + X^9 + X^7 + X^6 + X^5 + X^4 + X + 1$, les 24 premiers bits du générateur sont $1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1$. Le polynôme Q et cette suite sont disponibles dans le fichier `questiond.sage` sont les noms de variables `Qquestiond` et `zquestiond`.

Quelles sont les valeurs des clefs K_P et K_Q ? Expliquer la méthode utilisée, pas forcément tout le code.