Master CSI 2 **2019-2020**

Cryptanalyse — 4TCY902U

Responsable : G. Castagnos

Devoir surveillé — 12 novembre 2019

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 Cryptanalyse basée sur les réseaux

On considère le générateur de suite chiffrante suivant. Soit m et s deux entiers avec $0 < s < m$. On note k le nombre de bits de m, c'est à dire $2^{k-1} \leqslant m < 2^k$ et on suppose k pair. Les paramètres m, s et k sont publics, la clef secrète $sk \in \mathbf{N}$ avec $0 < sk < m$ est l'état initial du générateur. On note $x_0 = sk$, puis l'état interne au temps $t \geqslant 1$, noté x_t est calculé par $x_t = s\,x_{t-1} \bmod m$. La suite chiffrante est $z_t = \lfloor x_t/2^{k/2} \rfloor$ pour $t \geqslant 0$.

(a) Donner le **code d'une fonction Sage** qui produit les termes $z_0, z_1, \dots, z_{\ell-1}$ de suite chiffrante. Cette fonction doit prendre en entrée le nombre de termes, ℓ, et les entiers m, s, k et sk. **Application numérique** : pour cette question seulement on pose $m = 1009$, $s = 25$, $k = 10$ et $sk = 14$. Les 5 premiers termes de la suite de sortie sont $0, 10, 21, 25, 30$. Donner les 5 suivants.

Retour au cas général. Dans toute la suite de l'exercice, on suppose avoir récupéré les ℓ premiers termes $z_0, z_1, \dots, z_{\ell-1}$ de suite chiffrante d'un tel générateur avec m, s, k publics. On cherche à retrouver la clef secrète sk.

(b) Pour $t = 0, \dots, \ell-1$, on note $y_t = x_t - z_t 2^{k/2}$. Montrer que $y_t \equiv s^t y_0 + (s^t z_0 - z_t)2^{k/2} \pmod{m}$ pour tout t.

On considère le réseau $\mathscr{L}$ de $\mathbf{R}^\ell$ engendré par les lignes de la matrice $\ell \times \ell$:

$$A = \begin{pmatrix} m & 0 & \cdots & \cdots & 0 \\ -s & 1 & \ddots & & \vdots \\ -s^2 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ -s^{\ell-1} & 0 & \cdots & 0 & 1 \end{pmatrix}$$

On note $(b_0, \dots, b_{\ell-1})$ une base LLL réduite de $\mathscr{L}$. On suppose dans la suite qu'il existe un entier α tel que pour $i = 0, \dots, \ell-1$, $\|b_i\| \leqslant 2^{(\ell-1)/2}\alpha$.

(c) Soit $c \in \mathbf{Z}^\ell$. Supposons qu'il existe un vecteur $y \in \mathbf{Z}^\ell$ tel que $Ay \equiv c \pmod{m}$ avec $\|y\| \leqslant \frac{m}{\alpha(2^{((\ell+1)/2}+1)}$. Montrer que l'on peut trouver y en temps polynomial.

(d) En déduire une méthode heuristique pour retrouver la clef secrète sk à partir de $z_0, z_1, \dots, z_{\ell-1}$, et des paramètres publics m, s et k.

(e) **Application numérique** : récupérer une suite chiffrante z de $\ell = 5$ termes et les paramètres publics m, s et k dans le fichier

```
https://www.math.u-bordeaux.fr/~gcastagn/exo1.sage
```

Retrouver la valeur de sk mod 10000. Justifiez si vous n'avez pas donné la méthode à la question précédente.

[2] LFSR

(a) Soit $z = (z_t)_{t\geqslant 0}$ la suite binaire produite par le LFSR de longueur 5 de polynôme de rétroaction $X^5 \oplus X^3 \oplus 1$ et d'état initial $[0,0,1,0,1]$. Soit s la suite binaire définie par $s_t = z_t \oplus 1$ pour tout $t \geqslant 0$. **Avec Sage**, donner un polynôme de rétroaction minimal pour s. (Donner et justifier la méthode utilisée, pas tout le code)

La suite de l'exercice consiste à trouver la forme de ce polynôme dans le cas général. Dans la suite, $z = (z_t)_{t\geqslant 0}$ désigne une suite binaire strictement périodique non constante de polynôme de rétroaction $f(X)$ quelconque et $Z(X)$ sa série génératrice définie par $Z(X) = \sum_{t\geqslant 0} z_t X^t$.

(c) Soit $f(X) \in \mathbf{F}_2[X]$ un polynôme de degré ℓ avec $f(X) = 1 \oplus c_1 X \oplus c_2 X_2 \oplus \cdots \oplus c_\ell X^\ell$. Rappeler sans démonstration la formule reliant $Z(X)$ et $f(X)$ pour que z soit produite par un LFSR de polynôme de rétroaction $f(X)$.

(d) Soit s la suite binaire définie par $s_t = z_t \oplus 1$ pour tout $t \geqslant 0$. Donner un polynôme $h(X)$ tel que s soit produite par un LFSR de polynôme de rétroaction $h(X)$ (Justifier le résultat).

(e) On suppose que le polynôme $f(X)$ est le polynôme de rétroaction minimal pour la suite z. Quelle est le complexité linéaire de la suite s ?