Cryptanalyse — 4TCY902U Responsable : G. Castagnos

Devoir surveillé — 13 novembre 2018

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.

I Cryptanalyse basée sur les réseaux

Soit n > 1 un entier et p un nombre premier tel que p > 8n + 2. On considère le chiffrement à clef publique suivant. On note $\mathcal{M}_n(\mathbf{Z}/p\mathbf{Z})$ l'ensemble des matrices de taille $n \times n$ à coefficients dans $\mathbf{Z}/p\mathbf{Z}$ et I_n la matrice identité de taille $n \times n$.

Soit $R \in \mathcal{M}_n(\mathbf{Z}/p\mathbf{Z})$ une matrice aléatoire inversible. Soient $C, D \in \mathcal{M}_n(\mathbf{Z}/p\mathbf{Z})$ deux autres matrices aléatoires dont les coefficients sont choisis dans $\{-1,0,1\}$. De plus D est inversible. On note $\Delta \in \mathcal{M}_n(\mathbf{Z}/p\mathbf{Z})$ la matrice diagonale $\Delta := \lfloor p/2 \rfloor I_n$. La clef privée est R et la clef publique est constituée de n, p et de la juxtaposition de deux matrices R et R et R dire la matrice R et R et la clef publique est constituée de R et R et la juxtaposition de deux matrices R et R et R et la clef publique est constituée de R et R et la juxtaposition de deux matrices R et R et R et la clef publique est constituée de R et la juxtaposition de deux matrices R et R et R et la clef publique est constituée de R et la juxtaposition de deux matrices R et R et R et la clef publique est constituée de R et la juxtaposition de deux matrices R et R et R et la clef publique est constituée de R et R et la juxtaposition de deux matrices R et R et R et la juxtaposition de deux matrices R et R et R et la juxtaposition de deux matrices R et R

$$A := R^{-1}(\Delta - C)$$
$$B := -R^{-1}D.$$

L'espace des messages clairs est $\{0,1\}^{2n}$. Le chiffrement de $m \in \{0,1\}^{2n}$ avec la clef publique E se fait en calculant, modulo p,c := Em, en voyant m comme un vecteur colonne.

(a) On note $\ell = Rc$ où c est un chiffré de m. Montrer que

$$(\Delta \mathbf{o})m = \ell + (\mathbf{C} \mathbf{D})m$$
,

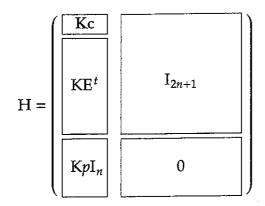
où o désigne la matrice nulle de $\mathcal{M}_n(\mathbf{Z}/p\mathbf{Z})$.

- **(b)** En déduire un algorithme de déchiffrement (en pseudo-code). Bien justifier que le déchiffrement est correct.
- (c) Application avec Sage. Récupérer le ficher

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

qui définit une clef publique n, p, A, B, E, une clef secrète associée R et un chiffré c pour ces clefs. Donner les 8 derniers bits du déchiffrement de c. Justifiez si vous n'avez pas donné l'algorithme à la question précédente.

(d) Soit K un grand entier, c un chiffré avec une clef publique quelconque n, p, E. On considère le réseau de \mathbb{R}^{3n+1} engendré par les lignes de la matrice carrée de taille 3n+1 suivante (où l'on voit c comme un vecteur ligne et c et E sont vus avec des coefficients entiers)



Montrer que le message clair m correspondant à c=Em est relié à un vecteur court de ce réseau. En déduire une méthode pour décrypter un chiffré (donner des arguments informels).

(e) Application avec Sage. Récupérer le ficher

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

qui définit une clef publique n2, p2, A2, B2, E2 et un chiffré c2 pour cette clef. Donner les 8 derniers bits du déchiffrement de c2. Justifiez si vous n'avez pas donné la méthode à la question précédente.

2 Somme de deux cases d'un LFSR

- (a) On considère un LFSR de longueur ℓ et de polynôme de rétroaction P primitif. On note z la suite de sortie du LFSR, et on construit une suite s telle que pour tout $t \in \mathbb{N}$, $s_t = z_{t+i} + z_{t+j}$ avec $0 \le i < j \le \ell 1$. Montrer que s est toujours un décalé de z (Indication : on pourra utiliser le résultat, vu en TD : si $\alpha \in \mathbb{F}_{2^\ell}$ est une racine de P, alors il existe $\beta \in \mathbb{F}_{2^\ell}$ tel que pour tout $t \in \mathbb{N}$, $z_t = trace(\beta \alpha^{-t})$).
- (b) On considère dans toute la suite le LFSR de longueur 8 et de polynôme de rétroaction X⁸ + X⁴ + X³ + X² + 1, initialisé par [1,0,0,1,1,1,0,1]. On note z la suite de sortie de ce LFSR. Déterminer, la période de ce LFSR (on pourra utiliser des commandes Sage). Expliquer la méthode utilisée.
- (c) À partir de ce LFSR, on construit une nouvelle suite de sortie s, dont le terme s_t correspond à la somme à l'instant t de la case 3 et de la case 6 du registre du LFSR, de telle sorte que pour tout $t \in \mathbb{N}$, $s_t = z_{t+3} + z_{t+6}$.

Trouver en utilisant **Sage** la valeur de l'entier r tel que la suite s est un décalé de r pas de la suite s, c'est à dire que pour tout $t \in \mathbb{N}$, $s_t = z_{t+r}$. Expliquer la méthode et donner le code Sage utilisé.