Cryptanalyse — M1MA9W06

Responsable : G. Castagnos

# TP 7 — LLL à l'attaque de Merkle-Hellman

L'un des premiers cryptosystèmes à clef publique proposé par Merkle et Hellman en 1978, était basé sur le problème du sac à dos. Ce système est spécifié de la façon suivante.

1. **Génération des clefs** Soit $n$ un entier, le paramètre de sécurité. On choisit un sac à dos d'entiers positifs à super-croissance, $a = (a_0, a_1, \ldots, a_{n-1})$, c'est à dire

$$a_j > \sum_{i=0}^{j-1} a_i \text{ avec } j = 1, \ldots, n-1.$$

   On choisit de plus chaque $a_i$ de $n+i$ bits. Soit M un entier tel que $M > \sum_{i=0}^{n-1} a_i$, et $w$ un autre entier tel que $1 < w < M$ avec $w$ et M premiers entre eux. Soit $b = (b_0, b_1, \ldots, b_{n-1})$ tel que $b_i = a_i w \mod M$, pour $i = 0, \ldots, n-1$. On calcule $u$ l'inverse de $w$ modulo M. La clef publique est $b$ la clef privée $(M, u, a)$.
2. **Chiffrement** d'un message de $n$ bits : $m = (m_0, \ldots, m_{n-1})$ est chiffré par $c := \sum_{i=0}^{n-1} m_i b_i$, calculé dans $\mathbf{N}$.
3. **Déchiffrement** d'un chiffré $c \in \mathbf{N}$. Calculer $s = cu \mod M$. On a alors $s = \sum_{i=0}^{n-1} m_i a_i$ dans $\mathbf{N}$. On retrouve les $m_i$ en résolvant le sac à dos à super-croissance par l'algorithme glouton :
   — déterminer le plus grand des $a_i$ tel que $a_i \leq s$ ;
   — remplacer $s$ par $s - a_i$ ;
   — recommencer tant que $s \neq 0$.

1 Implanter les algorithmes de génération des clefs, de chiffrement et de déchiffrement.

2 Cryptanalyse : retrouver le message $m$ à partir d'un chiffré $c$. Utiliser l'algorithme LLL, appliqué au réseau engendré par les lignes de la matrice

$$M = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & Kb_0 \\ 0 & 1 & \ldots & 0 & 0 & Kb_1 \\ \vdots & & & & \vdots & \\ 0 & 0 & \ldots & 1 & 0 & Kb_{n-1} \\ 0 & 0 & \ldots & 0 & 1 & -Kc \end{pmatrix}$$

en choisissant K tel que $K^2 > (n+1)/2$. Tester pour $n = 30$, par exemple.

Pour appliquer LLL sur une matrice M d'entiers avec Sage, utiliser la commande `M.LLL()`.