Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Maike Ritzenhofen, Alexander Meurer

Hausübungen zur Vorlesung

Kryptanalyse

SS 2008

Blatt 4 / 05. Juni 2008 / Abgabe 19. Juni 2008 bis 12Uhr in den Kasten auf NA 02

AUFGABE 1 (5 Punkte)**:**
Beweisen Sie für Satz 45 aus dem Skript die beiden Behauptungen:

(a) d ist ein nächster Gittervektor zum Targetvektor y'.

(b) Jeder Gittervektor in L, der Abstand exakt $\sqrt{n/4}$ zum Targetvektor y' hat, ist von der Form $(y_1 - x'_1, \ldots, y_n - x'_n)$ mit $s = \sum_{i=1}^{n} x'_i a_i$ und $x'_i \in \{0, 1\}$.

AUFGABE 2 (5 Punkte)**:**
Seien $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ mit $|a_n| = 1$. Die Menge

$$L = \left\{ (x_1, \ldots, x_n) \in \mathbb{Z}^n \mid \sum_{i=1}^{n} a_i x_i = 0 \right\}$$

ist ein Gitter. Geben Sie eine Basis von L an. Welche Gitterdimension hat L?

AUFGABE 3 (5 Punkte)**:**
Beweisen Sie ein Analogon von Satz 50 für inhomogene Gleichungen

$$a_1 x_1 + \cdots + a_n x_n = b \bmod N.$$

Dabei soll $|x_i| \leq X_i$ und $\prod_{i=1}^{n} X_i \leq N$ gelten.
Hinweis: Verwenden Sie ein $(n+1)$-dimensionales Gitter.

AUFGABE 4 (5 Punkte)**:**
Alice hat wieder mal Geburtstag und lädt ein. Da sie zu faul ist, neue Einladungen zu entwerfen, nimmt sie die alten Einladungen und ersetzt nur den Ort der Feier durch einen neuen geheimen Ort x. D.h. die Einladung m ist von der Form $m = \tilde{m} + x$. Sie verschlüsselt diese Nachricht mit einem RSA-Schlüssel (N, e) mit $e = 3$.
Eve fängt den Chiffretext $c = m^3 \bmod N$ ab. Da sie die letztes Jahr schon Alices Mails entschlüsselt hat, kennt sie den Text $\tilde{m}$ bereits. Zeigen Sie, dass Eve mit Hilfe eines Linearisierungsangriffs x bestimmen kann, sofern $x \leq N^{\frac{1}{6}}$.