RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

Hausübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 4 / 6. November 2012 / Abgabe bis spätestens 13. November 2012, 8:30 Uhr in dem Kasten auf NA 02

AUFGABE 1 (5 Punkte)**:**
Seien $a_1, \ldots, a_n \in \mathbb{Z}$. Geben Sie eine Basismatrix $\mathbf{B}$ für das Gitter

$$L := \{\mathbf{z} \in \mathbb{Q}^n \quad : \quad a_1 z_1 + \ldots + a_n z_n = 0\}$$

an und zeigen Sie $L = \text{span}(B)$. Berechnen Sie $\dim(L)$.

AUFGABE 2 (5 Punkte)**:**
Beweisen Sie für Satz 45 aus dem Skript die beiden Behauptungen:

(a) $\mathbf{d}$ ist ein nächster Gittervektor zum Targetvektor $\mathbf{y}'$.

(b) Jeder Gittervektor in L, der Abstand exakt $\sqrt{n/4}$ zum Targetvektor $\mathbf{y}'$ 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 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.