RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 3 / 2. November 2011

Der erste Schritt einer Iteration des Gauß-Algorithmus besteht darin, vom längeren Vektor $\mathbf{b}_2$ ein ganzzahliges Vielfaches $\mu\mathbf{b}_1, \mu \in \mathbb{Z}$ des kürzeren Vektors $\mathbf{b}_1$ abzuziehen. Wir wollen in der nächsten Aufgabe untersuchen, wie wir ein optimales μ wählen sollten. Wir definieren hierzu eine Abbildung $f : \mathbb{R} \to \mathbb{R}$ durch $f(\mu) = \|\mathbf{b}_2 - \mu\mathbf{b}_1\|^2$ wobei $\|\_\|$ die euklidische Norm bezeichnet.

AUFGABE 1:

(a) Zeigen Sie, dass $\mu^* = \frac{\langle \mathbf{b}_1, \mathbf{b}_2 \rangle}{\|\mathbf{b}_1\|^2}$ die Funktion f minimiert.

(b) Führen Sie den Gauß-Algorithmus für die Matrix

$$\mathbf{B} = \begin{pmatrix} 1 & 5 \\ 6 & 21 \end{pmatrix}$$

durch, d.h. $\mathbf{b}_1 = (1, 5)$ und $\mathbf{b}_2 = (6, 21)$. Wählen Sie μ^* gemäß Teil (a). Führen Sie das Verfahren durch, so loange $\mu^* > \frac{1}{2}$ gilt (wir werden in der Hausübung beweisen, dass $\mu^* \leq \frac{1}{2}$ stets eine reduzierte Basis garantiert).

(c) Geben Sie die unimodulare Transformationsmatrix $\mathbf{T}$ an, welche $\mathbf{B}$ in die minimale Basis überführt.

AUFGABE 2:

Betrachten Sie das Gitter

$$L := \{\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{Z}^3 : 2x_1 - 4x_2 - x_3 \equiv 0 \bmod 7\} \ .$$

Geben Sie eine Basismatrix $\mathbf{B}$ für L an und zeigen Sie $\text{span}(\mathbf{B}) = L$. Welche Dimension hat L? Berechnen Sie $\det(L)$.

AUFGABE 3:

Sei $N \in \mathbb{N}$ und $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Lösen Sie die Polynomgleichung $f(x) = 0 \bmod N$ mittels Linearisierung und Lösen eines SVPs. Welche Schranke erhalten Sie für die Größe der Lösung?

AUFGABE 4:

Seien $a_1, a_2, a_3 \in \mathbb{N}$ und sei $A := \max\{a_1, a_2, a_3\}$. Konstruieren Sie einen Algorithmus, der in Zeit $\mathcal{O}(\log^2 A)$ ganze Zahlen $u_1, u_2, u_3 \in \mathbb{Z}$ berechnet mit

$$\text{ggT}(a_1, a_2, a_3) = u_1a_1 + u_2a_2 + u_3a_3 \ .$$

Hinweis: Benutzen Sie $\text{ggT}(a_1, a_2, a_3) = \text{ggT}(\text{ggT}(a_1, a_2), a_3)$.