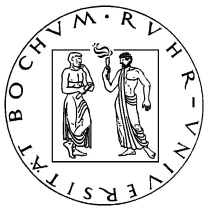
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Maike Ritzenhofen, Alexander Meurer



Präsenzübungen zur Vorlesung

Kryptanalyse

SS 2008

Blatt 4 / 05.Juni 2008

AUFGABE 1:
Sei $n \geq m$ und $a \in \mathbb{Z}^{m \times n}$ eine ganzzahlige $m \times n$-Matrix mit linear unabhängigen Zeilenvektoren. Zeigen Sie, dass die Menge

$$L = \{\mathbf{x} \in \mathbb{Z}^{n \times 1} \mid A\mathbf{x} = \mathbf{0}\}$$

ein Gitter L mit Gitterdimension $\dim(L) = n - m$ ist.

AUFGABE 2:
Gegeben sei ein Gitter L mit Basis

$$B = \begin{pmatrix} 24 & 14 \\ 9 & 5 \end{pmatrix}.$$

Berechnen Sie mit Hilfe des Gauß-Algorithmus eine reduzierte Basis. Was sind die sukzessiven Minima von L? Was ist die Determinante von L? Durch welche unimodulare Transformation kann B in die vom Gauß-Algorithmus berechnete Basis umgewandelt werden?

AUFGABE 3 (5 Punkte)**:**
Seien $a_1, a_2, \ldots, a_n, s \in \mathbb{N}$, wobei $\gcd(a_1, \ldots, a_n)$ ein Teiler von s ist. Zeigen Sie, dass man effizient $y_1, y_2, \ldots, y_n \in \mathbb{Z}$ konstruieren kann mit

$$\sum_{i=1}^{n} y_i a_i = s.$$

Bestimmen Sie die Laufzeit Ihres Algorithmus. Die Laufzeit sollte polynomiell in n und in der Bitgröße der a_i und s sein.

AUFGABE 4:
Sei $N \in \mathbb{N}$ und $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Lösen Sie die Polynomgleichung $f(x) = 0 \bmod N$ mittels Linearisierung und Lösen eines SVPs. Welche Schranke erhalten Sie für die Größe der Lösung?