Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Elena Kirshanova, Ilya Ozerov

Hausübungen zur Vorlesung

Kryptanalyse

SS 2014

Blatt 6 / 27. Mai 2014

Abgabe: 05. Juni 2014, 14.00 Uhr, Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

Sei

$$B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

eine Basis für ein Gitter L.

(a) Berechnen Sie mit Hilfe des Gauß-Algorithmus eine reduzierte Basis B' für L.

(b) Geben Sie ein $v \in L$ mit $\|v\| = 10$ an.

(c) Was sind die sukzessiven Minima von L?

(d) Durch welche unimodulare Transformation kann B in B' umgewandelt werden?

AUFGABE 2 (5 Punkte)**:**

Implementieren Sie den Angriff von Wiener aus der Vorlesung. Verwenden Sie dazu in Satz 50 die Schranken $Y_1 = \lfloor N^{3/4} \rfloor$ und $Y_2 = \lceil N^{1/4} \rceil$. In der Datei wiener.txt finden Sie einen öffentlichen RSA-Schlüssel (N, e). Finden Sie den zugehörigen geheimen Schlüssel d und faktorisieren Sie N. Geben Sie den Quellcode mit ab.

Hinweis: Verwenden Sie in sage den Befehl B.LLL() um eine reduzierte Basis zu bestimmen.