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

Präsenzübungen zur Vorlesung

Kryptanalyse

SS 2014

Blatt 6 / 26. Mai 2014

AUFGABE 1:

Sei $N = pq$ ein RSA-Modul. Zeigen Sie, dass man unter der Kenntnis von N und der Phi-Funktion $\varphi(N) = (p-1)(q-1)$ die Primfaktoren p und q in Zeit polynomiell in $\log N$ bestimmen kann.

AUFGABE 2:

Gegeben sei ein Gitter L mit Basis

$$B = \begin{pmatrix} 41 & 21 \\ 95 & 56 \end{pmatrix}.$$

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:

Die Menge

$$L = \{(x_1, x_2) \in \mathbb{Z}^2 \mid 2x_1 - 3x_2 = 0 \bmod 5\}$$

ist ein Gitter. Geben Sie eine Basis B für das Gitter L an und zeigen Sie, dass B eine Basis für L ist.

AUFGABE 4:

Seien p, q_1, q_2 prim, $r \in \mathbb{N}$ und $q_1 r \approx q_2 < p$. Wir betrachten eine Variante des "approximativen ggT-Problems": Gegeben sind $N_1 = p \cdot q_1$ und $N_2 = p \cdot q_2 + r$, gesucht ist die Faktorisierung von N_1. Beschreiben Sie einen Linearisierungsangriff, der das Problem in Zeit polynomiell in $\log N_1$ und $\log N_2$ löst. Lösen Sie das Problem für $N_1 = 161$, $N_2 = 301$ mit Hilfe Ihres Algorithmus.

Hinweis: Sie dürfen verwenden, dass

$$\begin{pmatrix} 41 & 22 \\ 95 & 51 \end{pmatrix} \cdot \begin{pmatrix} 1 & -161 \\ 0 & 301 \end{pmatrix} = \begin{pmatrix} 41 & 21 \\ 95 & 56 \end{pmatrix}.$$