RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Enrico Thomae

**Präsenzübungen zur Vorlesung**

# Kryptanalyse

**WS 2010/2011**

Blatt 7 / 24. November 2010

**AUFGABE 1:**
Sei $N = p^k$, $k \geq 2$. Zeigen Sie, dass $p$ und $k$ in Zeit polynomiell in $\log N$ berechnet werden können.

**AUFGABE 2:**
Faktorisieren Sie die Zahl $N = 77$ mit Hilfe von Satz 78 der Vorlesung, ohne eine Faktorbasis zu benutzen.
Faktorisieren Sie die Zahlen $N = 119$ und $N = 93$ mit Hilfe der Faktorbasis $F = \{2, 5, 7\}$ unter Verwendung von $a_i = \lfloor \sqrt{N} \rfloor + i, i \geq 0$.
Faktorisieren Sie die Zahl $N = 85$ mit Hilfe der Faktorbasis $F_2 = \{-1, 2\}$ unter Verwendung von $a_i = \lfloor \sqrt{N} \rfloor + i, i \geq 0$.

**AUFGABE 3:**
Berechnen Sie mit Hilfe des Index-Kalkulus Algorithmus den diskreten Logarithmus $\log_5(14)$ in $\mathbb{Z}_{23}^*$. Verwenden Sie dabei die Faktorbasis $F_3 = \{-1, 2, 3\}$ und die Wahl $r_i = i, i \geq 0$. Geben Sie die diskreten Logarithmen aller Elemente aus $F_3$ zur Basis 5 in $\mathbb{Z}_{23}^*$ an.