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 7 / 30. November 2011

AUFGABE 1:
Faktorisieren Sie die Zahl $N = 56$ mit Hilfe der Faktorbasis $F_2 = \{-1, 2, 3\}$ unter Verwendung von $a_i = \lfloor \sqrt{N} \rfloor + i, i \geq 1$.

AUFGABE 2:
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 $r_i = i, i \geq 1$. Geben Sie die diskreten Logarithmen aller Elemente aus F_3 zur Basis 5 in $\mathbb{Z}_{23}^*$ an.

AUFGABE 3:
Konstruieren Sie einen Algorithmus, der in Zeit $\tilde{\mathcal{O}}(B^2)$ eine Faktorbasis

$$F_B = \{p \in \mathbb{N} : p \leq B \text{ und } p \text{ prim}\} \cup \{-1\}$$

zur Schrnake $B \in \mathbb{N}$ konstruiert.

AUFGABE 4:
Sei $N = p^k$, $k \geq 2$ eine Primzahlpotenz. Zeigen Sie, dass p und k effizient, d.h. in Zeit polynomiell in $\log N$, berechnet werden können.