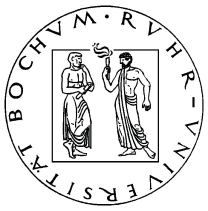
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Alexander Meurer



Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2009/2010

Blatt 7 / 20. Januar 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 $N = 85$ 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.