RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 5 / 13. November 2012

AUFGABE 1:
Sei $N \in \mathbb{N}$ und $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Lösen Sie die Polynomgleichung $f(x) = 0 \bmod N$ mittels Linearisierung und Lösen eines SVPs. Welche Schranke erhalten Sie für die Größe der Lösung?

AUFGABE 2:
Seien $N_1 < \ldots < N_5$ paarweise teilerfremde RSA Moduln. Geben Sie einen effizienten Algorithmus zum Lösen folgenden Gleichungssystems an:

$$\begin{aligned} c_1 &= m^3 \bmod N_1 \\ c_2 &= m^3 \bmod N_2 \\ c_3 &= m^5 \bmod N_3 \\ c_4 &= m^5 \bmod N_4 \\ c_5 &= m^5 \bmod N_5. \end{aligned}$$

AUFGABE 3:
Seien $c = m^3 \bmod N$ und $c' = (m + r)^3 \bmod N$ zwei RSA-verschlüsselte Nachrichten. Zeigen Sie, dass man m mit Hilfe von c, c', r und N effizient berechnen kann. Sie benötigen für die Lösung nur elementare Arithmetik (Addition, Subtraktion, Multiplikation, Division (mit Rest)) modulo N.