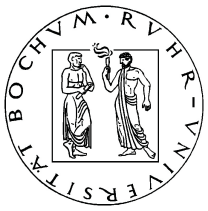
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Alexander Meurer



Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2009/2010

Blatt 5 / 9. Dezember 2009

AUFGABE 1:
Sei $N \in \mathbb{N}$ beliebig und $b = a^2 \bmod N$. Konstruieren Sie einen Algorithmus, der bei Eingabe b, N in Zeit $\tilde{\mathcal{O}}(N^{\frac{2}{3}})$ und Platz $\tilde{\mathcal{O}}(1)$ eine Quadratwurzel von b berechnet. Verwenden Sie dazu Linearisierung und das Lösen eines SVPs.
Anmerkung: Für prime N gibt es einen probabilistischen Algorithmus, der polynomielle Laufzeit hat. Ein deterministischer Algorithmus für Primzahlen ist ohne zusätzliche zahltheoretische Annahmen nicht bekannt.

AUFGABE 2:
Sei $f(x) = x^2 + ax + b$ und $m = 3$. Betrachten Sie den Beweis aus Satz 59, und geben Sie die Kollektion der Polynome $f_{i,j}(x)$ und die Basismatrix B explizit an.

AUFGABE 3:
Wir verwenden die stereotype Nachricht "... lautet das Passwort für den heutigen Tag". D.h. unser RSA-Chiffretext ist

$$c = (x2^k + S)^3 \bmod N,$$

für unbekanntes k und x. Zeigen Sie, dass man x effizient berechnen kann falls $|x| \leq N^{\frac{1}{3}}$, obwohl man nicht mit einem monischen Polynom startet.

AUFGABE 4:
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.
Hinweis: Die Lösung verwendet nur elementare Arithmetik (Addition, Subtraktion, Multiplikation, Division) modulo N.