RUHR UNIVERSITÄT BOCHUM

RUB

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

Hausübungen zur Vorlesung

Kryptanalyse

WS 2010/2011

Blatt 4 / 03. November 2010 / Abgabe bis spätestens 10. November 2010, 10 Uhr (vor der Übung)

AUFGABE 1 (5 Punkte)**:**
Betrachten Sie den Wiener-Angriff für unbalanciertes RSA. Sei dazu (N, e) ein öffentlicher RSA-Schlüssel mit $N = pq$, wobei $p \approx N^{\frac{1}{4}}$. Wie groß darf d höchstens sein, dass der Angriff von Wiener funktioniert? Ist das unbalancierte RSA sicherer als das Balancierte?

AUFGABE 2 (5 Punkte)**:**
Beweisen Sie für Satz 45 aus dem Skript die beiden Behauptungen:

(a) d ist ein nächster Gittervektor zum Targetvektor y'.

(b) Jeder Gittervektor in L, der Abstand exakt $\sqrt{n/4}$ zum Targetvektor y' hat, ist von der Form $(y_1 - x'_1, \ldots, y_n - x'_n)$ mit $s = \sum_{i=1}^{n} x'_i a_i$ und $x'_i \in \{0, 1\}$.

AUFGABE 3 (5 Punkte)**:**
Beweisen Sie ein Analogon von Satz 50 für inhomogene Gleichungen

$$a_1 x_1 + \ldots + a_n x_n = b \bmod N.$$

Dabei soll $|x_i| \leq X_i$ und $\prod_{i=1}^{n} X_i \leq N$ gelten.
Hinweis: Verwenden Sie ein $(n+1)$-dimensionales Gitter.

AUFGABE 4 (5 Punkte)**:**
Alice hat wieder mal Geburtstag und lädt ein. Da sie zu faul ist, neue Einladungen zu entwerfen, nimmt sie die alten Einladungen und ersetzt nur den Ort der Feier durch einen neuen geheimen Ort x. D.h. die Einladung m ist von der Form $m = \tilde{m} + x$. Sie verschlüsselt diese Nachricht mit einem RSA-Schlüssel (N, e) mit $e = 3$.
Eve fängt den Chiffretext $c = m^3 \bmod N$ ab. Da sie die letztes Jahr schon Alices Mails entschlüsselt hat, kennt sie den Text $\tilde{m}$ bereits. Zeigen Sie, dass Eve mit Hilfe eines Linearisierungsangriffs x bestimmen kann, sofern $x \leq N^{\frac{1}{6}}$.