RUHR
UNIVERSITÄT
BOCHUM

RUB

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

Hausübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 5 / 13. November 2012 / Abgabe bis spätestens 20. November 2012, 8:30 Uhr in dem Kasten auf NA 02

AUFGABE 1 (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 $x \leq N^{\frac{1}{6}}$.

AUFGABE 2 (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 3 (5 Punkte)**:**
Zeigen Sie, dass Aufgabe 2 der 5. Präsenzübung auch ohne Kenntnis von c_5, d.h. ohne die 5. Gleichung lösbar ist.

Hinweis: Benutzen Sie folgende Variante des CRT für Polynome: Seien $f_1(x), \ldots, f_k(x)$ Polynome $f_i(x) \in \mathbb{Z}_{N_i}[X]$ vom Grad n und $N_1, \ldots, N_k$ paarweise teilerfremde Moduln. Dann kann man effizient ein eindeutiges Polynom $f(x) \in \mathbb{Z}_M[x]$ vom Grad n mit $M = N_1 \cdot \ldots \cdot N_k$ bestimmen, so dass $f(x) \equiv f_i(x) \bmod N_i$ für $i = 1, \ldots, k$ gilt.

AUFGABE 4 (5 Punkte)**:**
Sei $N = pq$ ein RSA-Modul und $b = a^2 \bmod N$. Konstruieren Sie einen Algorithmus, der bei Eingabe b, N in Zeit $\tilde{\mathcal{O}}(N^{\frac{1}{2}})$ und Platz $\tilde{\mathcal{O}}(1)$ eine Quadratwurzel von b berechnet. Verwenden Sie dazu den Satz von Coppersmith (Satz 60).

Hinweis: Es kann hilfreich sein, zunächst die Existenz einer Approximation A von a einer gewissen Güte N^{δ} anzunehmen. Die Approximationen kann man dann per Brute-Force durchgehen.