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 6 / 17. November 2010 / Abgabe bis spätestens 24. November 2010, 10 Uhr (vor der Übung)

AUFGABE 1 (4 Punkte)**:**
Sei $k = (p, \alpha, \beta = \alpha^a)$ ein öffentlicher ElGamal Schlüssel mit geheimem Schlüssel a. Sei $e_k(m) = (\alpha^r, m\beta^r)$ ein ElGamal-Chiffretext. Weiterhin sei $\ell = \sqrt{\log p} + \log\log p$.
Sei A ein Algorithmus, der für beliebiges b bei Eingabe α^{a+b}, α^r und $m\beta^r$ die obersten ℓ Bits von $m \cdot (\alpha^{-r})^b$ berechnet. Zeigen Sie, dass es dann einen polynomiellen Algorithmus zur Berechnung von m gibt, d.h. dass ElGamal in polynomieller Zeit gebrochen werden kann.
Hinweis: Konstruieren Sie eine Instanz des Hidden Number Problems.

AUFGABE 2 (5 Punkte)**:**
Sei $M \in \mathbb{N}$ mit unbekanntem Teiler $b \geq M^{\frac{1}{2}}$ und $f(x) = x + a$.

(a) Geben Sie die komplette Basismatrix B des Gitters L aus Satz 66 für die Parameterwahl $m = 3$ an. Bestimmen Sie $\dim(L)$ und $\det(L)$.

(b) Sei $N = pq$ ein RSA Modul mit 1024-Bit Primzahlen p, q, wobei $p > q$. Gegeben ist eine Approximation $\tilde{p}$ von p mit $|p - \tilde{p}| \leq N^{0.225}$. Welchen Wert von m müssen Sie wählen, um den Modul faktorisieren zu können?

AUFGABE 3 (4 Punkte)**:**
Sei $M \in \mathbb{N}$ mit unbekanntem Teiler b und $f(x) \in \mathbb{Z}_M[x]$ mit Grad n. Sei A ein Algorithmus, der bei Eingabe M und $f(x)$ eine Nullstelle x_0 von $f(x)$ modulo b berechnet, die keine Nullstelle von $f(x)$ modulo M ist, d.h.

$$f(x_0) = 0 \bmod b \quad \text{und} \quad f(x_0) \neq 0 \bmod M.$$

Dann kann man einen nicht-trivialen Faktor von M in Zeit polynomiell in n und $\log M$ bestimmen.

AUFGABE 4 (4 Punkte)**:**
Sei $N = pq$ ein RSA-Modul mit $p > q$. Sei $k \in \mathbb{N}$ eine unbekannte Zahl, die kein Vielfaches von q ist. Weiterhin sei eine Approximation $\widetilde{kp}$ von kp gegeben mit

$$|kp - \widetilde{kp}\,| \leq N^{\frac{1}{4}}.$$

Zeigen Sie, dass die Faktorisierung von N in Zeit polynomiell in $\log N$ berechnet werden kann.