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 6 / 20. November 2012 / Abgabe bis spätestens 27. November 2012, 8:30 Uhr in dem Kasten auf NA 02

AUFGABE 1 (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 $\mathbf{B}$ des Gitters L aus Satz 66 für die Parameterwahl $m = 3$ an. Bestimmen Sie $\dim(L)$ und $\det(L)$. Welche obere Schranke an X erhalten sie (unter Vernachlässigung der LLL-Konstanten c und $\dim(L)$)?

(b) Sei $N = pq$ ein RSA Modul mit Primzahlen p, q, wobei $p > q$. Gegeben ist eine Approximation $\tilde{p}$ von p mit $|p - \tilde{p}| \leq N^{0.24}$. Welchen Wert von m müssen Sie wählen, um den Modul faktorisieren zu können?

AUFGABE 2 (5 Punkte)**:**
Sei $N = p^2 q$ ein modifizierter RSA-Modul mit $p > q$. Sei ferner eine Approximation $\tilde{p}$ von p gegeben mit $|p - \tilde{p}| \leq N^{\frac{2}{9}}$.

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

(b) Angenommen p und q haben gleiche Bitgröße. Welchen Bruchteil der Bits von p muss bei dieser Parameterwahl kennen, um N effizient faktorisieren zu können? Vergleichen Sie mit normalen RSA-Moduln $N = pq$.

AUFGABE 3 (5 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 $\mathcal{A}$ 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 und nutzen Sie Fakt 75 aus der Vorlesung.