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

AUFGABE 1 (4 Punkte)**:**
Zeigen Sie, dass Aufgabe 3 der 5. Präsenzübung auch ohne Kenntnis von c_5 lösbar ist.

AUFGABE 2 (4 Punkte)**:**
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 (6 Punkte)**:**
Sei $N = pq$ ein RSA-Modul und $b = a^2 \bmod N$.

(a) 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).

(b) Für Polynome vom Grad 2 liefert der Satz von Coppersmith die Schranke $|x_0| \leq N^{\frac{1}{2}}$. Angenommen man könnte die Schranke auf $|x_0| \leq N$ verbessern. Zeigen Sie, dass man dann N in Polynomialzeit faktorisieren kann.

AUFGABE 4 (4 Punkte)**:**
Beweisen Sie den Satz von Howgrave-Graham für bivariate Polynome, d.h. zeigen Sie:
Sei $g(x, y) = \sum_{i,j} b_{i,j} x^i y^i \in \mathbb{Z}[x, y]$ ein Polynom mit n Monomen. Es sei ferner

(1) $g(x_0, y_0) = 0 \bmod M^m$ für $|x_0| \leq X$, $|y_0| \leq Y$ und

(2) $\|g(xX, yY)\| < \frac{M^m}{\sqrt{n}}$.

Dann gilt $g(x_0, y_0) = 0$ über den ganzen Zahlen.

Hinweis: Wie bei univariate Polynomen ist die Norm von $g(x, y)$ als die Euklidische Norm des Koeffizientenvektors definiert.