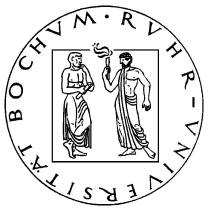
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Maike Ritzenhofen, Alexander Meurer



Hausübungen zur Vorlesung

Kryptanalyse

SS 2008

Blatt 5 / 19. Juni 2008 / Abgabe 03. Juli 2008 bis 12Uhr in den Kasten auf NA 02

AUFGABE 1 (5 Punkte)**:**
Gegeben sei ein RSA-Modul $N = pq$ mit $p > q$ und eine Approximation $\tilde{p}$ von p mit

$$|p - \tilde{p}| \leq N^{\frac{1}{6}}.$$

Zeigen Sie

(a) Man kann eine Approximation $\tilde{q}$ von q berechnen mit $|q - \tilde{q}| \leq N^{\frac{1}{6}}$.

(b) Bestimmen Sie mit Hilfe eines Linearisierungsangriffs die Faktorisierung von N.

AUFGABE 2 (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 3 (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.

AUFGABE 4 (5 Punkte)**:**
Sei $N \in \mathbb{N}$ und $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Verwenden Sie die Coppersmith-Methode mit $m = 1$ und der folgenden Kollektion von Polynomen

$$f_i(x) = x^i N \text{ für } i = 0, \ldots, n-1 \text{ und } f_n(x) = f(x).$$

Stellen Sie die Basismatrix aus den Koeffizientenvektoren der $f_i(xX)$ auf. Welche Schranke erhalten Sie? Vergleichen Sie mit der Schranke für Linearisierungsangriffe. Welche Vorteile bietet die Coppersmith-Methode?