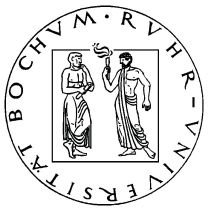
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Alexander Meurer



Hausübungen zur Vorlesung

Kryptanalyse

WS 2009/2010

Blatt 5 / 9. Dezember 2009 / Abgabe bis spätestens 23. Dezember 2009, 10 Uhr (vor der Übung)

AUFGABE 1 (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 2 (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 3 (10 Punkte)**:**
Bestimmen Sie mit einem Angriff nach Wiener den geheimen Schlüssel zu folgendem öffentlichen Schlüssel:

$N = 938300626597586498680866338901692155074169612925722624248438584118348822513156741269930773165733144614037042666304909846511691502353576698119405623123694165540876668426988865395164087166000618060710280315747350596615642883598922845027247637712211982470274940063197126643278336493622244308289512770008525487 41$

$e = 133573256543757753819391839704406237384503315239228218421366637457659341665631690496374404623977649738334738263062765914477256927194730545031422616617554545696546444367696373894008309145230056193770646885092464674035946338188693910094936706456532320257990800608310180128719790316898196028420425934037891061 83$

Können Sie ebenfalls die Faktorisierung von N bestimmen? (Kapitel 9.1.3)

Abgabe von lauffähigen Programmen oder Skripten an mathias.herrmann@rub.de .

Hinweis: Viele Computeralgebraprogramme verfügen über eine LLL Implementierung (z.B. pari/gp). Alternativ kann eine Implementierung in C/C++ verfügbare Bibliotheken (z.B. NTL) einbinden.