RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Ilya Ozerov

Hausübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 4 / 9. November 2011 / Abgabe bis spätestens 16. November 2011, 10 Uhr in dem Kasten auf NA 02

AUFGABE 1 (5 Punkte)**:**
Betrachten Sie den Wiener-Angriff für unbalanciertes RSA. Sei dazu (N, e) ein öffentlicher RSA-Schlüssel mit $N = pq$, wobei $p \approx N^{\frac{1}{4}}$. Wie groß darf d höchstens sein, dass der Angriff von Wiener funktioniert? Ist das unbalancierte RSA sicherer als das Balancierte?

AUFGABE 2 (5 Punkte)**:**
Beweisen Sie ein Analogon von Satz 50 für inhomogene Gleichungen

$$a_1 x_1 + \cdots + a_n x_n = b \bmod N.$$

Dabei soll $|x_i| \leq X_i$ und $\prod_{i=1}^{n} X_i \leq N$ gelten.

Hinweis: Verwenden Sie ein $(n+1)$-dimensionales Gitter und führen Sie auf das Lösen einer SVP-Instanz zurück.

AUFGABE 3 (10 Punkte)**:**

(a) Implementieren Sie den Gauss-Algorithmus entsprechend der Vorlage aus Hausübung 3 und berechnen Sie eine minimale Basis für

$$\mathbf{B} = \begin{pmatrix} 685 & 126101 \\ 697467 & 116726945 \end{pmatrix} .$$

Sie finden die Eingabematrix auch zum Download auf der Webseite in Datei `H4B.sobj`.

Hinweis: Die euklidische Norm $\|\mathbf{x}\|$ können Sie in sage mittels `norm(x)` berechnen. Das Skalarprodukt von `x` und `y` erhalten Sie durch `x.dot_product(y)`.

(b) Implementieren Sie den Wiener Angriff für N, e gemäß der Dateien `H4N.sobj` und `H4e.sobj` (oder alternativ `wiener.txt`) und finden Sie den geheimen Schlüssel d. Sie können entweder ihren eigenen Gauss-Algorithmus verwenden oder auf den LLL-Algorithmus von Sage zurückgreifen.

(c) Berechnen Sie die Faktorisierung von N wie im Beweis von Satz 52 beschrieben. Benutzen Sie hierzu auch Aufgabe 2 aus Präsenzübung 4.