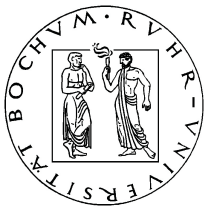
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Maike Ritzenhofen, Alexander Meurer



Hausübungen zur Vorlesung

Kryptanalyse

SS 2008

Blatt 6 / 03. Juli 2008 / Abgabe 17. Juli 2008 bis 12Uhr in den 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 B des Gitters L aus Satz 66 für die Parameterwahl $m = 3$ an. Bestimmen Sie $\dim(L)$ und $\det(L)$.

(b) Sei $N = pq$ ein RSA Modul mit 500-Bit Primzahlen p, q, wobei $p > q$. Verwenden Sie die Gitterbasis B aus Aufgabenteil (a), um N mit Hilfe einer Approximation $\tilde{p}$ von p zu faktorisieren. Wieviele Bits von p muss man bei dieser Parameterwahl kennen, um den Modul N effizient zu faktorisieren? Sie können bei Ihrer Analyse Terme niederer Ordnung vernachlässigen, d.h. Sie können die vereinfachte Determinantenbedingung aus Satz 66 verwenden.

AUFGABE 2 (5 Punkte)**:**
Seien $sig_k(x)$, $sig_k(x')$ zwei DSA-Unterschriften unterschiedlicher Nachrichten $x \neq x' \bmod q$ unter Verwendung desselben r. Zeigen Sie, dass dann a effizient berechnet werden kann, sofern $\gamma \neq 0$.

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 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.

AUFGABE 4 (5 Punkte)**:**
Sei $N = pq$ ein RSA-Modul mit $p > q$. Sei $k \in \mathbb{N}$ eine unbekannte Zahl, die kein Vielfaches von q ist. Weiterhin sei eine Approximation $\widetilde{kp}$ von kp gegeben mit

$$|kp - \widetilde{kp}| \leq N^{\frac{1}{4}}.$$

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