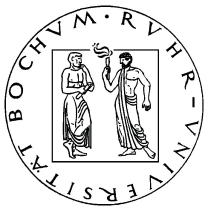
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Alexander Meurer



Hausübungen zur Vorlesung

Kryptanalyse

WS 2009/2010

Blatt 6 / 23. Dezember 2009 / Abgabe bis spätestens 20. Januar 2010, 10 Uhr (vor der Übung)

AUFGABE 1 (4 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 2 (6 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 512-Bit Primzahlen p, q, wobei $p > q$. Gegeben ist eine Approximation $\tilde{p}$ von p mit $|p - \tilde{p}| \leq N^{0.225}$. Implementieren Sie einen Gitterangriff für dieses Szenario. Welchen Wert von m müssen Sie wählen, um den Modul faktorisieren zu können?

Die Parameter N und $\tilde{p}$ stehen auf der Webseite zum Download bereit.

AUFGABE 3 (4 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.

AUFGABE 4 (6 Punkte)**:**
In dieser Aufgabe soll der Angriff von Nguyen auf das DSA Signaturverfahren implementiert werden. Dazu steht eine Liste von 30 Tupeln

$$(Nachricht, Signatur, teilweisebekannteZufallswerte)$$

auf der Webseite der Vorlesung zur Verfügung. Der Teil der Signatur besteht wiederum aus zwei Elementen γ, δ wie in der Vorlesung beschrieben. Die teilweise bekannten Zufallsbits sind gerade die niederwertigsten 11 Bits des für die jeweilige Signatur verwendeten r. (D.h. in der Notation des Skriptes : $\ell = 11$)
Können Sie den geheimen Schlüssel a rekonstruieren ?