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 6 / 23. November 2011 / Abgabe bis spätestens 30. November 2011, 10 Uhr in dem 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 $\mathbf{B}$ des Gitters L aus Satz 66 für die Parameterwahl $m = 3$ an. Bestimmen Sie $\dim(L)$ und $\det(L)$. Welche obere Schranke an X erhalten sie (unter Vernachlässigung der LLL-Konstanten c und $\dim(L)$)?

(b) Sei $N = pq$ ein RSA Modul mit 1024-Bit Primzahlen p, q, wobei $p > q$. Gegeben ist eine Approximation $\tilde{p}$ von p mit $|p - \tilde{p}| \leq N^{0.225}$. Welchen Wert von m müssen Sie wählen, um den Modul faktorisieren zu können?

AUFGABE 2 (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 und nutzen Sie Fakt 75 aus der Vorlesung.

AUFGABE 3 (10 Punkte)**:**
Implementieren Sie den Angriff zur Faktorisierung bei bekannten Bits von $d_p = d \bmod p - 1$ (siehe Satz 71). Berechnen Sie die Faktorisierung von

```
N=100058751642012180851382778935573208181172831282859086021181419998934675412877950217028689124541061857566783494581394199403858983063865215903319246266688541236721360856162284496659495545691545598127037811398152230119244798510128532627105942389272920855125265525214320333144778124167158770185859505636829596196716000449271313349809009920076453134430871299797134843537714475259390486276018020954069267483182275302624567263742391725639906407052553493138859020337938221439727624283671611984340764108114635982302630540179852391829275887212582287817425018100060508665545841929614197615831147697022352011563423413224025308 23
```

bei gegebenem

```
e=2125963540892179
```

und

```
dptil=106065845341213497426332573985368484400489218999488613024861985041880980238189307329529724261208701954403218002998598054683610287960649043659251650907827432252239075610867870586876781618163085013934492649743413618961344433443974946882479535242048127689593673579745459212313947997023872106502252698565910481085
```

gemäß der Dateien `H6N.sobj`, `H6e.sobj` und `H6dptil.sobj` auf der Webseite, d.h. $\tilde{d_p}$ ist die gegebene Approximation von d_p.
Benutzen Sie hierzu den Algorithmus aus Aufgabe 2 aus der Präsenzübung, d.h. bauen Sie ein Gitter gemäß Satz 66 zum Polynom $f(x) = x + \tilde{kp}$ auf, wobei Sie $\tilde{kp}$ geeignet berechnen müssen.
Beachten Sie, dass Sie zum Aufbau eines konkreten Gitters m bestimmen müssen, wofür Sie ϵ benötigen, was von der Güte der verwendeten Approximation $\tilde{kp}$ abhängt. Der Beweis von Satz 71 gibt hierzu aber keine Auskunft. Starten Sie daher den Algorithmus mit $\epsilon = \frac{1}{8}$ und halbieren Sie ϵ so lange, bis sie die Faktorisierung gefunden haben. Für welches ϵ ist der Algorithmus erfolgreich? Welche Gitterdimension haben Sie verwendet?