RUHR UNIVERSITÄT BOCHUM

RUB

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

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 5 / 16. November 2011

AUFGABE 1:
Betrachten Sie für $f(x) = x^2 + ax + b$ die quadratische Gleichung $f(x) = 0 \bmod M$.

(a) Stellen Sie die zugehörige Gitterbasis gemäß dem Beweis von Satz 59 auf. Benutzen Sie als Kollektion von Polynomen lediglich

$$f_0(x) := f(x) \ , \ \ f_1(x) := Mx \ \text{ und } \ f_2(x) := M \ .$$

Welche Schranke $|x_0| \leq X$ für die Größe einer Nullstelle $f(x_0) = 0$ erhalten Sie?

(b) Geben Sie eine Gitterbasis für $f(x) = x^2 + 1008x + 781$ und $M = 2801$ an. Verwenden Sie die obere Schranke $X = 4$. Nehmen Sie an, nach der LLL-Reduktion erhalten Sie die Basis

$$\mathbf{B} = \begin{pmatrix} 82 & 36 & -400 \\ -188 & 464 & -176 \\ 2261 & 856 & 448 \end{pmatrix} \ .$$

Berechnen Sie $g(x)$. Erfüllt $g(xX)$ Bedingung (2) aus dem Lemma von Hastad / Howgrave-Graham? Berechnen Sie die ganzzahlige(n) Nullstelle(n) von g.

AUFGABE 2:
Sei $f(x)$ ein monisches Polynom vom Grad n. Konstruieren Sie eine Variante des Coppersmith-Algorithmus, der effizient alle Nullstellen $f(x_0) = 0 \bmod M$ im Intervall $[a, b]$ mit

$$|a - b| \leq 2M^{\frac{1}{n}}$$

bestimmt.

AUFGABE 3:
Sei $N_1 < \ldots < N_5$ RSA Moduln. Geben Sie mittels Satz 59 einen effizienten Algorithmus zum Lösen folgenden Gleichungssystems an.

$$\begin{aligned} c_1 &= m^3 \bmod N_1 \\ c_2 &= m^3 \bmod N_2 \\ c_3 &= m^5 \bmod N_3 \\ c_4 &= m^5 \bmod N_4 \\ c_5 &= m^5 \bmod N_5 \end{aligned}$$

Hinweis: Benutzen Sie folgende Variante des CRT für Polynome: Seien $f_1(x), \ldots, f_k(x)$ Polynome $f_i(x) \in \mathbb{Z}[X]$ vom Grad δ und $N_1, \ldots, N_k$ paarweise teilerfremde Moduli. Dann kann man effizient ein eindeutiges Polynom $f(x) \in \mathbb{Z}_M[x]$ vom Grad δ mit $M = N_1 \cdot \ldots \cdot N_k$ bestimmen, so dass $f(x) \equiv f_i(x) \bmod N_i$ für $i = 1, \ldots, k$ gilt. Kombinieren Sie dies mit dem Algorithmus von Coppersmith.