



Hausübungen zur Vorlesung

Kryptanalyse

WS 2009/2010

Blatt 4 / 25. November 2009 / Abgabe bis spätestens 8. Dezember 2009, 10
Uhr (vor der Übung)

AUFGABE 1 (5 Punkte):

Seien $a_1, a_2, \dots, a_n, s \in \mathbb{N}$, wobei $\gcd(a_1, \dots, a_n)$ ein Teiler von s ist. Zeigen Sie, dass man effizient $y_1, y_2, \dots, y_n \in \mathbb{Z}$ konstruieren kann mit

$$\sum_{i=1}^n y_i a_i = s.$$

Bestimmen Sie die Laufzeit Ihres Algorithmus. Die Laufzeit sollte polynomiell in n und in der Bitgröße der a_i und s sein.

AUFGABE 2 (5 Punkte):

Beweisen Sie für Satz 45 aus dem Skript die beiden Behauptungen:

- (a) d ist ein nächster Gittervektor zum Targetvektor y' .
- (b) Jeder Gittervektor in L , der Abstand exakt $\sqrt{n}/4$ zum Targetvektor y' hat, ist von der Form $(y_1 - x'_1, \dots, y_n - x'_n)$ mit $s = \sum_{i=1}^n x'_i a_i$ und $x'_i \in \{0, 1\}$.

AUFGABE 3 (5 Punkte):

Beweisen Sie ein Analogon von Satz 50 für inhomogene Gleichungen

$$a_1 x_1 + \dots + a_n x_n = b \pmod{N}.$$

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.

AUFGABE 4 (5 Punkte):

Alice hat wieder mal Geburtstag und lädt ein. Da sie zu faul ist, neue Einladungen zu entwerfen, nimmt sie die alten Einladungen und ersetzt nur den Ort der Feier durch einen neuen geheimen Ort x . D.h. die Einladung m ist von der Form $m = \tilde{m} + x$. Sie verschlüsselt diese Nachricht mit einem RSA-Schlüssel (N, e) mit $e = 3$.

Eve fängt den Chiffretext $c = m^3 \bmod N$ ab. Da sie die letztes Jahr schon Alices Mails entschlüsselt hat, kennt sie den Text \tilde{m} bereits. Zeigen Sie, dass Eve mit Hilfe eines Linearisierungsangriffs x bestimmen kann, sofern $x \leq N^{\frac{1}{6}}$.