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 4 / 9. November 2011

AUFGABE 1:
Betrachten Sie den Wiener-Angriff.

(a) Geben Sie eine Gitterbasis $\mathbf{B}$ für das zur Gleichung $ex_1 + x_2 = 0 \bmod N$ gehörige Gitter an.

(b) Welche Linearkombination von Basisvektoren von $\mathbf{B}$ liefert die gesuchte Lösung $(x_1, x_2) = (d, k(p+q-1)-1)$?

(c) Wie erhält man aus einer Lösung $\mathbf{x}'$ für das mit $Y_i = \frac{N}{X_i}$ skalierte Gitter die eigentliche Lösung $(x_1, x_2) = (d, k(p+q-1)-1)$?

AUFGABE 2:
Zeigen Sie, dass man aus N und $\varphi(N)$ die Faktorisierung $N = p \cdot q$ von N berechnen kann.

Hinweis: Die Lösung ist elementar und benötigt keinerlei Hilfsmittel aus der Vorlesung.

AUFGABE 3:
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 $x \leq N^{\frac{1}{6}}$.