RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Enrico Thomae

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2010/2011

Blatt 5 / 10. November 2010

AUFGABE 1:
Geben Sie eine Basis für das im Wiener Angriff verwendete Gitter an. Welche Linearkombination von Gittervektoren liefert die gesuchte Lösung $(d, k(p+q-1)-1$?

AUFGABE 2:
Seien $c = m^3 \bmod N$ und $c' = (m+r)^3 \bmod N$ zwei RSA-verschlüsselte Nachrichten. Zeigen Sie, dass man m mit Hilfe von c, c', r und N effizient berechnen kann.
Hinweis: Die Lösung verwendet nur elementare Arithmetik (Addition, Subtraktion, Multiplikation, Division) modulo N.

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

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

AUFGABE 4:
Wir kennen für die in c verschlüsselte Nachricht m die Begrüßungs- und Abschiedstext S_1 und S_2. Damit ist auch k und k' bekannt. Angenommen S_1 und S_2 haben die gleiche Länge. Ab welcher Größe von S_1 kann man x effizient berechnen?

$$c = (S_2 2^{k'} + x 2^k + S_1)^3 \bmod N,$$