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 2 / 20. Oktober 2010

AUFGABE 1:
Sei $c = m^e \bmod N$ ein RSA-Chiffretext. Zeigen Sie, dass m effizient aus c berechnet werden kann, falls $m < N^{\frac{1}{e}}$.

AUFGABE 2:
Zeigen Sie: Für einen bekannten RSA-Modul N gilt:

$$\varphi(N) \text{ ist effizient berechenbar } \Leftrightarrow p, q \text{ sind effizient berechenbar}$$

AUFGABE 3:
Sei (N, e) ein öffentlicher RSA-Schlüssel und (N, d) der zugehörige geheime Schlüssel. Zeigen Sie, dass auch für Nachrichten $m \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$ die Entschlüsselung korrekt ist.
(Der Satz von Euler sagt *nur* $a^{\varphi(N)} = 1 \bmod N$, falls $\gcd(a, N) = 1$.)

AUFGABE 4:
Sei (N, e) ein öffentlicher RSA Schlüssel mit zugehörigen CRT-Exponenten $d_p \neq d_q$. Zeigen Sie, dass dann die Faktorisierung von N in Zeit $\tilde{\mathcal{O}}(\min\{d_p, d_q\})$ und Platz $\tilde{\mathcal{O}}(1)$ berechnet werden kann.