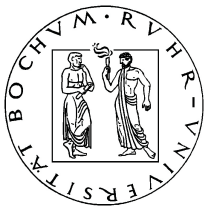
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Alexander Meurer




**Präsenzübungen zur Vorlesung**

# Kryptanalyse

**WS 2009/2010**

Blatt 2 / 28. Oktober 2009

**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:**
Seien $a, b, k, n, p \in \mathbb{N}$, $p$ prim.
Zeigen Sie die folgenden Eigenschaften der Eulerschen $\varphi$-Funktion:

(a) $\varphi(p^k) = p^k(1 - \frac{1}{p})$

(b) $\varphi(ab) = \varphi(a)\varphi(b)$, falls $\gcd(a, b) = 1$.

(c) $\varphi(n) = n \prod_{p|n}(1 - \frac{1}{p})$, falls $n = \prod_{p|n} p^{k_p}$ die Primfaktorzerlegung von $n$ ist.

**AUFGABE 4:**
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.

**AUFGABE 5:**
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 $\mathcal{O}(1)$ berechnet werden kann.