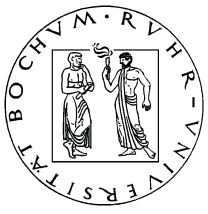
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Maike Ritzenhofen




**Präsenzübungen zur Vorlesung**

# Kryptanalyse

**SS 2008**

Blatt 2 / 02. Mai 2008

**AUFGABE 1:**
Sei $c = m^e \mod N$ 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 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.

**AUFGABE 4:**
Angenommen wir haben einen Algorithmus ELGAMAL, der bei Eingabe einer ElGamal verschlüsselten Nachrichten den Klartext ausgibt, d.h. $\text{ELGAMAL}(p, \alpha, \beta, \alpha^r, m\beta^r) = m$.
Zeigen Sie, dass man daraus einen Algorithmus DH konstruieren kann, der das Diffie-Hellman Problem löst, d.h. $\text{DH}(p, \alpha, \alpha^a, \alpha^b) = \alpha^{ab}$.

**AUFGABE 5:**
Wir betrachten das DL-Problem: Sei $\beta = \alpha^a \in Z_p^*$, wobei $n = \text{ord}(\alpha)$ gegeben ist und $a$ ermittelt werden soll. Beschreiben Sie einen Meet-in-the-Middle Angriff auf $a$ mit Zeit und Platz $\tilde{\mathcal{O}}(\sqrt{n})$.
Verwenden Sie Ihren Algorithmus, um $\log_5(10)$ in $\mathbb{Z}_{17}^*$ zu berechnen.