



Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2009

Blatt 2 / 06. Mai 2009

**AUFGABE 1:**

Betrachten Sie den Beweis zur Sicherheit mehrfacher Verschlüsselungen.  
Zeigen Sie dass es eine vernachlässigbare Funktion *negl* gibt, so dass

$$\frac{1}{2}Pr[\mathcal{A}(Enc_{pk}(m_0^1), Enc_{pk}(m_1^2)) = 0] + \frac{1}{2}Pr[\mathcal{A}(Enc_{pk}(m_1^1), Enc_{pk}(m_1^2)) = 1] \leq \frac{1}{2} + negl.$$

**AUFGABE 2:**

Sei  $N = pq$  ein Produkt von zwei verschiedenen Primzahlen. Zeigen Sie, dass mit Kenntnis von  $N$  und  $\phi(N)$  die Primfaktoren  $p$  und  $q$  in Polynomialzeit berechenbar sind.

**AUFGABE 3:**

**Common Modulus Attack**

Seien  $pk_1 = (N, e_1)$  und  $pk_2 = (N, e_2)$  zwei öffentliche Schlüssel von Textbook RSA mit  $\gcd(e_1, e_2) = 1$ . Ein Angreifer erfährt die Verschlüsselungen der gleichen Nachricht  $m$  unter den beiden Public Keys, d.h. er kennt

$$c_1 = m^{e_1} \bmod N \quad \text{und} \quad c_2 = m^{e_2} \bmod N$$

1. Erklären Sie, wie der Angreifer die Nachricht  $m$  berechnen kann.
2. Führen Sie den Angriff für die Werte  $N = 143, e_1 = 3, e_2 = 5, c_1 = 8, c_2 = 54$  durch.