Prof. J. Rothe Düsseldorf, 17.11.2009

# Übung zur Vorlesung
# Kryptologie 2

Blatt 6, Abgabe: 26.11.2009 bis 15:00 Uhr

**Aufgabe 1 (10 Punkte):** Betrachten Sie das ElGamal-Protokoll für digitale Signaturen. Angenommen, Erich kennt $p = 401$, $\gamma = 6$, $\beta = 216$, $m_1 = 15$, $m_2 = 17$, $(\sigma_1, \varrho_1) = (67, 186)$ und $(\sigma_2, \varrho_2) = (67, 184)$. Dabei seien $(\sigma_1, \varrho_1)$ eine Signatur zu $m_1$ und $(\sigma_2, \varrho_2)$ eine Signatur zu $m_2$, die beide mit dem selben $s$ erzeugt wurden.
Bestimmen Sie Bobs geheimen Exponenten $b$, ohne dabei explizit einen diskreten Logarithmus zu berechnen.

**Aufgabe 2 (15 Punkte):** Betrachten Sie Rabins Kryptosystem mit $p = 43$ und $q = 47$.

**(a)** Verschlüsseln Sie die Nachrichten $m_1 = 234$, $m_2 = 1789$ und $m_3 = 1989$.

**(b)** Betrachten Sie die Ciphertexte, die Sie in Aufgabenteil (a) erhalten und berechnen Sie jeweils alle möglichen Klartexte.

**Aufgabe 3 (5 Punkte):** Faktorisieren Sie $n = 13081$ mit Hilfe eines Chosen-Ciphertext-Angriffs. Benutzen Sie dazu $x = 12$ und $c = x^2 = 144$.
*Die Orakel-Antwort auf* $\langle 13081, 144 \rangle$ *ist* $m = 115$.

**Aufgabe 4 (freiwillig):** Betrachten Sie das Rabin-Kryptosystem mit $n = 713$.
Angenommen, Erich kennt die Klartexte $m_1 = 17$, $m_2 = 293$, $m_3 = 420$, $m_4 = 696$ zum Schlüsseltext $c = 289$.
Faktorisieren Sie $n$ durch einen Known-Plaintext-Angriff.
*Hinweis: Dies funktioniert ähnlich dem Random-Factor-Algorithmus.*