Gregor Leander
30.06.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Übungsblatt 11

Aufgabe 1 *Secret Sharing* 10 Punkte

Zeigen Sie, dass bei Shamir's (t, n)-Secret Sharing Protokoll weniger als t Parteien keinerlei Informationen über das gemeinsame Geheimnis haben.

Aufgabe 2 *RSA und CCA* 5 Punkte

Zeigen Sie, dass das standard RSA Verfahren nicht sicher gegen Chosen Ciphertext Attacken sicher ist. Sei $PK = (n, e)$ ein öffentlicher RSA Schlüssel und d der entsprechende geheime Exponent. Finden Sie also eine Attacke auf RSA im folgenden Model.

1. Der Angreifer bekommt einen öffentlichen RSA Schlüssel (n, e) und eine Ciphertext $c = m^e \bmod n$.
2. Der Angreifer hat Zugriff auf ein Entschlüsselungs-Orakel und kann sich alle Ciphertexte $c' \neq c$ entschlüsseln lassen. Das Orakel berechnet also $m' = (c')^d \bmod n$
3. Am Ende muss der Angreifer die Nachricht m zu dem Ciphertext c ausgeben.

Aufgabe 3 *Deterministische Verfahren* 5 Punkte

Zeigen Sie, dass ein deterministisches Public Key Verschlüsselungs-Verfahren niemals semantisch sicher sein kann. Finden Sie also für jedes solche Verfahren einen Angriff im folgenden Model.

1. Der Angreifer wählt zwei (gleich lange) Nachricht m_0 und m_1 und schickt m_0 und m_1 an das Orakel.
2. Das Orakel wählt zufällig ein Bit b und schickt dem Angreifer die Verschlüsselung von m_b.
3. Der Angreifer gibt ein Bit b' aus und gewinnt, wenn $b = b'$ gilt.

Abgabe: Freitag, 4.07.2008 bis 12:00 Uhr im Kasten im Gebäude NA Ebene 02 oder Samstag, 5.07.2008 bis 12:00 Uhr per Mail an `mansour.alsawadi@rub.de`.