Gregor Leander
7.07.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Übungsblatt 12

Aufgabe 1 *ElGamal ist semantisch sicher* 10 Punkte

Zeigen Sie, dass das ElGamal Verschlüsselungs-Verfahren semantisch sicher ist unter der Annahme das DDH schwer ist.

Aufgabe 2 *ElGamal ist unsicher gegen adaptive Angriffe* 10 Punkte

Zeigen Sie, dass das ElGamal Verschlüsselungs-Verfahren unsicher gegen CCA-2 Angriffe ist.

Das ElGamal Verfahren:
Sei G eine zyklische Gruppe primer Ordnung p und g ein Erzeuger gegeben.

1. Schlüsselerzeugung
   (a) Wähle eine Zufallszahl $a \in_R \mathbb{Z}_p$.
   (b) Der öffentliche Schlüssel ist $A = g^a$.
   (c) Der private Schlüssel ist a.
2. Verschlüsselung
   (a) Wähle zufällig $b \in_R \mathbb{Z}_p$.
   (b) Die Verschlüsselung von $m \in G$ ist
   $$\mathrm{Enc}_A = (g^b, mA^b)$$
3. Entschlüsselung
   (a) Sei ein Ciphertext (B, C) gegeben. Berechne
   $$\mathrm{Dec}_a(B, C) = \frac{C}{B^a}$$

Abgabe: Freitag, 11.07.2008 bis 12:00 Uhr im Kasten im Gebäude NA Ebene 02 oder Samstag, 12.07.2008 bis 12:00 Uhr per Mail an `mansour.alsawadi@rub.de`.