3. Übungsblatt

SS 2015
Rechnersicherheit
Ausgegeben am 30.04.2015
Abgabe 07.05.2015

Marian Margraf
Inst. für Informatik
Freie Universität Berlin

Aufgabe 1 (RSA)

Zeigen Sie, dass das RSA-Verfahren mit OAEP IND-CPA sicher ist,wenn H und G Einwegfunktionen sind.

Aufgabe 2. (Elgamal)

(*a*) Zeigen Sie, dass Elgamal IND-CPA sicher ist.

(*b*) Zeigen Sie, dass die mehrmahlige Verwendung derselben Zufallszahl k im Elgamal-Verfahren unsicher ist.

Aufgabe 3. (Hashfunktionen I)

Sei $f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n$ eine Kompressionsfunktion und H eine wie in der Vorlesung konstruierte Hashfunktion, die auf f basiert. Zeigen Sie: Wenn f eine Einwegfunktion ist, dann auch H.

Aufgabe 4. (Hashfunktionen II)

Wie groß ist die Wahrscheinlichkeit dafür, dass 20 zufällige Personen am selben Tag Geburtstag haben wie Sie (Jahrgang spielt keine Rolle)?