Spezielle Aspekte: Kryptographie *SoSe 2011*
Barbara Baumeister

11. Präsenzübungsblatt

Aufgabe 1 Berechnen Sie die folgenden geheimen Schlüssel im RSA-Verfahren zu den folgenden öffentlichen Schlüsseln:

(a) $(n, e) = (323, 5)$;

(b) $(n, e) = (493, 13)$.

Aufgabe 2 Für eine Hashfunktion $h : P \to \mathbb{Z}_2^r$ soll eine Kollision mithilfe des Geburtstagsparadoxon konstruiert werden. Man spricht von der *Geburtstagsattacke*.

Wieviele Versuche braucht man, um mit einer Wahrscheinlichkeit $\approx 1/2$ eine Kollision zu finden, wenn $r = 64$, $r = 128$ ist?

Aufgabe 3 Es ist $\alpha = 3$ eine erzeugendes Element von $\mathbb{Z}_{2011}^*$ ($p = 2011$ ist eine Primzahl). Der geheime Schlüssel von Alice ist 101. Das zu signierende Dokument ist $x = 1111$. Bestimmen Sie die ElGamal-Signatur mit $k = 31$ und verifizieren Sie diese.