Spezielle Aspekte: Kryptographie *SoSe 2011*
PD Dr. Barbara Baumeister
Tutoren: Patrick Wegener, Philipp Neumann, Patrick Odenbach

10. Übungsblatt

Abgabe: Mittwoch, 15.6.11

Aufgabe 1 *Sei $n = 5609$. Fakorisieren Sie n in seine Primfaktoren*

(a) mit Hilfe von Pollards $(p-1)$-Methode;

(b) mit dem Verfahren von Fermat.

Aufgabe 2 *Sei $p = 83$ (eine sichere Primzahl). Es ist $\alpha = 2$ ein erzeugendes Element von $\mathbb{Z}_{83}^*$. Seien Sie zuerst Alice. Wählen Sie ein $a \in \{2, \ldots, 81\}$ und bestimmen Sie den öffentlichen Schlüssel. Danach seien Sie Bob und schicken die Nachricht $x = 61$ mit dem ElGamal-Verfahren an Alice.*

Aufgabe 3 *Die Buchstaben $a, \ldots, z$ seien mit 1 startend durchnummeriert. Sei $(107, 2, 80)$ der öffentliche und $a = 51$ Ihr privater Schlüssel des ElGamal-Verfahrens. Bob hat Ihnen die folgende Nachricht*

$$(60, 3), (21, 49), (15, 9), (8, 25), (16, 69), (42, 27)$$

geschickt, die er mit dem ElGamal-Verfahren verschlüsselt hat. Was besagt sie?

Aufgabe 4 *ZUSATZAUFGABE: Schreiben Sie in Ihrer Lieblingsprogrammierspache ein Programm, was bei Eingabe einer Primzahl p ein α und a wählt und dann die ElGamal-Verschlüsselung durchführt. Verschlüsseln Sie die Nachricht $x = 17$, wobei $p = 107,1171$ sei.*