TECHNISCHE UNIVERSITÄT BERLIN WS09/10
Fakultät II – Institut für Mathematik
Dozent: Tobias Finis
Assistent: Gerriet Möhlmann
www.math.tu-berlin.de/~kant/kryptows09

9. Übung Kryptographie

1. Aufgabe

Ist p eine Primzahl und g ein Erzeuger der multiplikativen Gruppe $G := (\mathbb{Z}/p\mathbb{Z})^\times$, so berechnet man für ein $x \in \{0, 1, \ldots, p-2\}$ das Element $y = g^x$. Dieses y ist öffentlich wohingegen x privat ist. Ist nun $m \in G$ eine zu verschlüsselnde Nachricht, so wählt man $r \in \mathbb{Z}$ zufällig und bildet $u := g^r$ und $v := my^r$. Der Chiffretext ist dann (u, v). Zum Entschlüsseln berechnet man $vu^{-x} = my^r g^{-rx} = mg^{rx}g^{-rx} = m$. Dieses Kryptosystem heißt ELGamal Kryptosystem.

(a) Bestimmt alle Erzeuger von $(\mathbb{Z}/43\mathbb{Z})^\times$.

(b) Alice erhält den ElGamal-Chiffretext $(u = 37, v = 24)$. Ihr öffentlicher Schlüssel ist $(p = 43, g = 3)$. Bestimmt den zugehörigen Klartext, wenn $x = 9$ ist.

(c) Der öffentliche Schlüssel von Bob sei $(p = 53, g = 2, y = 30)$. Allice erzeugt damit den Chiffretext $(24, 37)$. Wie lautet der Klartext?

(5 Punkte)

2. Aufgabe

Sei (e, n) ein öffentlicher RSA-Schlüssel. Für einen Klartext $m \in \{1, \ldots, n-1\}$ sei $c \equiv m^e \mod n$ der zugehörige Chiffretext. Zeigt, dass es eine natürliche Zahl k gibt mit

$$m^{(e^k)} \equiv m \mod n.$$

Beweist, dass für ein solches k gilt:

$$c^{(e^{k-1})} \equiv m \mod n.$$

(5 Punkte)

3. Aufgabe

Implementiert die Ver- und Entschlüsselung mit ElGamal in einer Untergruppe der Einheitengruppe eines Primkörpers. Ihr könnt dazu die Methode zum Berechnen eines Erzeugers der Einheitengruppe aus $el\_g.g$ verwenden.

(5 Punkte)

4. Aufgabe

Implementiert einen Baby-Step-Giant-Step Algorithmus, berechnet damit zu einem von eurem ElGamal erzeugten Chiffretext den Klartext ohne den geheimen Schlüssel zu nutzen und skizziert ein Baby und einen Giant.

(5 Punkte)