TECHNISCHE UNIVERSITÄT BERLIN Sommersemester 2004
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. Heß
WM: Dipl.-Math. M. Wagner
www.math.tu-berlin.de/~hess/krypto

9. Übung Kryptographie

1. Aufgabe ElGamal für $\mathbb{Z}/p\mathbb{Z}$ (4 Punkte)

Ist p eine Primzahl und g ein Erzeuger der multiplikativen Gruppe $G := (\mathbb{Z}/p\mathbb{Z})^\times$, so berechnet man für ein $x \in \{0, 1, ..., p-2\}$ 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 dann $vu^{-x} = my^r g^{-rx} = mg^{rx}g^{-rx} = m$.

(i) Bestimmen sie alle Erzeuger der multiplikativen Untergruppe von $\mathbb{Z}/43\mathbb{Z}$.

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

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

2. Aufgabe Faktorisierung ganzer Zahlen (4 Punkte)

(i) Finden Sie einen echten Teiler von $n = 11111$ mit dem quadratischen Sieb.

(ii) Faktorisieren Sie $n = 138277151$ mit der $p-1$-Methode.

3. Aufgabe Rabin-Kryptosystem (3 Punkte)

Sei $n = 713$ ein öffentlicher Rabin-Schlüssel und sei $c = 289$ ein Schlüsseltext den man durch Rabin-Verschlüsselung mit diesem Modul erhält. Bestimmen Sie alle möglichen Klartexte.

4. Aufgabe Praktische Aufgabe - ElGamal (9 Punkte)

Es sei $p = 31847, g = 5, x = 7899$ und $y = 18074$. Jedes Element von $\mathbb{Z}/p\mathbb{Z}$ besitzt eine 26-adische Darstellung wobei man im Restklassenring $\mathbb{Z}/p\mathbb{Z}$ als Repräsentanten immer die kleinste positive Zahl einer Nebenklasse nimmt. Diese Darstellung ist die selbe wie in Aufgabe 3 auf dem 5. Übungsblatt. Auf der Kryptographie-Homepage befindet sich eine Datei **ElGamal**. Entschlüsseln Sie den sich dort befindenden Chiffretext. Wie lautet der Klartext?

Gesamt: 20 Punkte