TECHNISCHE UNIVERSITÄT BERLIN WS08/09
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. Heß
Assistent: G. Möhlmann
Abgabe: 27.1.09
www.math.tu-berlin.de/~hess/krypto-ws2008

12. Übung Kryptographie

1. Aufgabe

Beweisen oder widerlegen Sie die folgenden Aussagen:

(a) Für alle $n \in \mathbb{N}$ gibt es $k, a, b \in \mathbb{Z}$, so dass gilt:

$$a^2 - b^2 = kn$$

(b) Für alle $n \in \mathbb{N}$ gibt es $a, b \in \mathbb{Z}$, so dass gilt:

$$a^2 - b^2 = n$$

Hat diese Aufgabe etwas mit dem quadratischen Sieb zutun?

(5 Punkte)

2. Aufgabe

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

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

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

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

(5 Punkte)

3. Aufgabe

Implementieren Sie eine Probedivision und versuchen Sie $n \in \mathbb{N}$ zu finden, so dass bei geeigneten Parametern ihr quadratisches Sieb schneller als die Probedivision einen Teiler findet.

(3 Punkte)

4. Aufgabe

Implementieren Sie die fehlenden Teile ihres quadratischen Siebs. Bei dem LinA-Schritt kann man die Methode *KernelMatrix()* verwenden. Die Faktorbasis darf unter Benutzung von *NextPrime()* konstruiert werden.

(7 Punkte)