Gregor Leander
21.04.2008

Fakultät für Mathematik
Ruhr-Universität Bochum

Kryptographie II – Übungsblatt 4

Aufgabe 1: *Quadratwurzeln modulo p* (7 Punkte)

Finde beide Quadratwurzeln von 4792 modulo 9941 mittels des in der Vorlesung erläuterten Verfahrens.
Hinweis: man muss ein richtiges (also quadratischer Nichtrest modulo 9941) n erst finden.

Aufgabe 2: *Quadratwurzeln modulo n* (7 Punkte)

Sei $n = 137238091$.

1. Die Zahl n ist das Produkt zweier Primzahlen p und q. Bestimme diese.
2. Bestimme alle Quadratwurzeln von $a = 113050492$ modulo n mittels des in der Vorlesung erläuterten Verfahrens.

Aufgabe 3: *Quadratwurzeln modulo p^t* (7 Punkte)

In der Vorlesung haben wir ein Verfahren besprochen, wie man effizient Quadratwurzeln modulo einer Primzahl $p \neq 2$ ziehen kann.
Überlege Dir nun ein Verfahren um effizient Quadratwurzeln modulo p^t für ein $t \geq 1$ zu bestimmen. Finde also ein Verfahren um f"ur gegebenes a einen Wert x so zu bestimmen, dass

$$x^2 \equiv a \bmod p^t$$

gilt.
Hinweis: Schreibe x in der *p-adischen Entwicklung*, d.h. $x = x_0 + x_1 p + \ldots x_{t-1} p^{t-1}$, und bestimme x in mehreren Schritten.

Abgabe: Freitag, 9.05.2008 bis 12:00 Uhr im Kasten im Gebäude NA Ebene 02 oder Samstag, 10.05.2008 bis 12:00 Uhr per Mail an `mansour.alsawadi@rub.de`.