Universität Tübingen, WS 13/14

Bernd Borchert

Übungen Kryptologie

Blatt 6

Aufgabe 6.1. Wiederholung Rechnen

(a) Berechnen Sie den ggT von 493 und 459. Prüfen Sie das Ergebnis, d.h. die zwei Teilbarkeiten.

(b) Berechnen Sie das multiplikative Inverse von 8 modulo 53, d.h. finden ein e, so dass gilt 8e = 1 mod 53. Falls Ihr e nicht zwischen 0 und 53 liegt, wandeln Sie e in ein solches um. Prüfen Sie das Ergebnis, d.h. die Eigenschaft 8e = 1 mod 53.

(c) Berechnen Sie 5^{66} mod 17.

Aufgabe 6.2. Rabin Kryptosystem

(a) Prüfen Sie mit den Euler Kriterium, ob die Zahlen 2 und 3 Quadratzahlen modulo 7 sind.

(b) Verschlüsseln Sie die Nachricht 42 im Rabin Kryptosystem mit dem Public Key 77.

(c) Entschlüsseln Sie diese chiffrierte Nachricht mit dem Private Key (7,11). Ist die Originalnachricht unter den 4 Ergebnissen?

Aufgabe 6.3. Elgamal Kryptosystem

(a) Generieren Sie ein Elgamal Schlüsselpaar mit p= 23, q=11, g = 5 und a = 13.

(b) Verschlüsseln Sie die Nachricht 15 mit dem Public Key, mit b = 20.

(c) Entschlüsseln Sie die chiffrierte Nachricht mit dem Private Key.

Aufgabe 6.4. Chinesischer Restsatz

Finden Sie ein x, für das alle drei folgenden Gleichungen gelten:

x = 5 mod 8
x = 6 mod 11
x = 7 mod 13