Hochschule für
Technik und Wirtschaft
des Saarlandes
University of Applied Sciences

Studiengang Kommunikationsinformatik (Master)
Prof. Dr.–Ing. Damian Weber

Sicherheit und Kryptographie – Übung 1

Aufgabe 1 (GP/PARI und RSA)

Erzeugen Sie ein in der Praxis verwendbares Beispiel von RSA Parametern. In Klammern sind die in `gp` aufzurufenden Funktionen angegeben. Schauen Sie sich dabei für jede Funktion (z.B. `func()`) den zugehörigen Hilfetext an (mittels `?func`). Zahlen z mod n stellen Sie als $Mod(z, n)$ dar, damit während der Arithmetik die Zwischenergebnisse klein gehalten werden können.

a) Wählen Sie zufällige 500-bit-Primzahlen p, q (`random()`, `nextprime()`).

b) Berechnen Sie n.

c) Berechnen Sie $\varphi(n)$. (nicht `eulerphi()` benutzen, nur deren Beschreibung lesen (warum?))

d) Wählen Sie $e = 2^{16} + 1$ und berechnen Sie d.

e) Verschlüsseln Sie die Nachricht $m = 111 \ldots 1$ (100 Einsen).

f) Entschlüsseln Sie die verschlüsselte Nachricht und überprüfen Sie das Ergebnis.