Hochschule für
Technik und Wirtschaft
des Saarlandes
University of Applied Sciences

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

Sicherheit und Kryptographie – Übung 2

Aufgabe 1 (ElGamal–Kryptosystem)

Erzeugen Sie mit Hilfe von GP/PARI eine Konfiguration eines ElGamal–Kryptosystems.

a) Wählen Sie als Primzahl q die nächste Primzahl größer als $10^{250} \cdot \pi$ (siehe `default(realprecision, 300)`, `Pi`, `floor()`, `nextprime()`, `truncate()`) für die auch $p = 2q + 1$ eine Primzahl ist. Die Zahl p ist dann eine ,,sichere" Primzahl für DL–Kryptosysteme. GP/PARI hat auch eine `for`–Schleife (siehe auch `print()`), mit der man für diesen Zweck automatisiert `isprime()` aufrufen kann.

b) Finden Sie einen möglichst kleinen Erzeuger g modulo p.

c) Wählen Sie als geheimen Schlüssel $a = (10^{250} - 1)/9$ und geben Sie den resultierenden Public Key y aus.

d) Verschlüsseln Sie den Text `Kryptovorlesung` als Paar (c, d) durch Umwandlung des Textes in eine Zahl und benutzen Sie dabei die ,,Zufallszahl" $k = (10^{250} - 1)/3$.

e) Entschlüsseln sie den Chiffretext (c, d).