Hochschule für Technik und Wirtschaft
Studiengang Kommunikationsinformatik
Studiengang Praktische Informatik
Prof. Dr.–Ing. Damian Weber

Kryptographie – Übung 4

Aufgabe 1 (RSA–Kryptosystem)

Implementieren Sie das RSA–Kryptosystem. Hierzu definiere man eine Klasse RSA, die als Attribute die `BigInteger`–Werte n, p, q, e, d, phi und die im folgenden beschriebenen Methoden enthält.

a) *setup* erzeuge für vorgegebene Bitlänge alle Parameter.

b) *encrypt* verschlüssle ein Element aus $\mathbf{Z}/n\mathbf{Z}$.

c) *decrypt* entschlüssle ein Element aus $\mathbf{Z}/n\mathbf{Z}$.

d) *sign* signiere ein Element aus $\mathbf{Z}/n\mathbf{Z}$.

e) *verify* verifiziere die Signatur für ein Element aus $\mathbf{Z}/n\mathbf{Z}$.

Für eine vorgegebene Bitlänge b sollten Sie die Parameter folgendermaßen wählen:

- wähle Primzahlen p, q der Bitlänge $b/2$
- n und $\varphi(n)$ ausrechnen
- setze $e = 2^{16} + 1$
- berechne d

Testen Sie

- mit Hilfe der *decrypt*–Methode, ob die *encrypt*–Methode
- mit Hilfe der *verify*–Methode, ob die *sign*–Methode

korrekt arbeitet.