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

Angewandte Kryptographie – Übung 3

Aufgabe 1 (RSA Grundlagen)

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

a) *setup* erzeuge für vorgegebene Bitlänge die 5 Parameter.

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

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

Sie dürfen eine Zahl als Primzahl annehmen, wenn die `isProbablePrime(7)` Methode den Wert *true* zurückliefert.

Zum Testen der Korrektheit Ihres Codes deklarieren Sie ein Random–Objekt

```
Random r=new Random(987654321L);
```

und erzeugen daraus zwei BigInteger–Werte (BigInteger–Konstruktor für 128 Bit und Random–Variable), die Sie als Parameter für Ihre *next_prime* Funktion übergeben.

a) welche Werte treten für p und q auf?

i) 234028873424310926862032544425673971781
ii) 234028873424310926862032544425673971783
iii) 234028873424310926862032544425673971787
iv) 234028873424310926862032544425673971789
v) 288949718778966808255592086333653197141
vi) 288949718778966808255592086333653197143
vii) 288949718778966808255592086333653197147
viii) 288949718778966808255592086333653197149

b) welcher Wert für $\varphi(n)$

i) 676225771621130612320903689366939883832262288555258267967274708209024061170 46

ii) 676225771621130612320903689366939883832262288555258267967274708209024061170 48

iii) 676225771621130612320903689366939883832262288555258267967274708209024061170 50

iv) 676225771621130612320903689366939883832262288555258267967274708209024061170 52

c) wie sieht für $e = 2^{16} + 1$ der Parameter d aus?

i) 404784122262187068699346197321590119211127295726426016637261192960312707626 3

ii) 404784122262187068699346197321590119211127295726426016637261192960312707626 5

iii) 404784122262187068699346197321590119211127295726426016637261192960312707626 7

iv) 404784122262187068699346197321590119211127295726426016637261192960312707627 1

d) verschlüsseln Sie die Nachricht $m = 1234567890$, was ist das Ergebnis m'?

i) 109936802951286845349546068739278357124269024300733906785046657107968797700 01

ii) 109936802951286845349546068739278357124269024300733906785046657107968797700 03

iii) 109936802951286845349546068739278357124269024300733906785046657107968797700 05

iv) 109936802951286845349546068739278357124269024300733906785046657107968797700 07

e) Testen Sie durch das Entschlüsseln, ob das ursprüngliche m als Klartext sichtbar wird.

Aufgabe 2 (Umwandlung von Text in Integers)

Erweitern Sie Ihre RSA–Implementierung dadurch, daß statt Zahlen Texte verschlüsselt werden können.