

Aufgabe 14: (8 Punkte)

Betrachten Sie folgende Variante der RSA-Schlüsselerzeugung:

- (1) Wähle eine große Primzahl n und eine natürliche Zahl e mit $\text{ggT}(e, n) = 1$.
- (2) Berechne $d = e^{-1}$ in \mathbb{Z}_n als Lösung der Gleichung $ed \bmod n = 1$.
- (3) Halte das Paar (d, n) als privaten Schlüssel geheim.
- (4) Gib das Paar (e, n) als öffentlichen Schlüssel bekannt.

Beurteilen Sie den RSA-Verschlüsselungsalgorithmus mit der auf diese Weise modifizierten Schlüsselerzeugung bzgl. der Aspekte Korrektheit, Durchführbarkeit und Sicherheit (mit Begründungen!).

Programmieraufgabe P4: (12 Punkte)

(a) Implementieren Sie den RSA-Algorithmus! Beachten Sie dabei folgende Hinweise:

- Verwenden Sie die über die Veranstaltungswebsite verfügbaren Quelldateien RSA.java und RSAKey.java als Vorlage (Einträge „// TODO: ...“ beachten)
- Es sollen Methoden zur Schlüsselerzeugung, Verschlüsselung und Entschlüsselung implementiert werden.
- Schlüsselerzeugung: Der Benutzer soll die Bitlänge des RSA-Moduls n vorgeben können. Alle anderen Parameter sind im Programm selbst (zufällig) zu generieren. Methoden zur Speicherung der generierten Schlüssel in Dateiform sind schon in den Vorlagedateien enthalten.

Testen Sie Ihre Implementierung an Beispiel 3.2 aus dem Skript und an weiteren selbstgewählten Beispielen.

(b) Entschlüsseln Sie folgende Texte, die mit dem RSA-Algorithmus verschlüsselt wurden. Geben Sie jeweils den zugehörigen privaten Schlüssel an.

(i) öffentlicher Schlüssel: $n = 902801$, $e = 65537$

337399 | 714856 | 026644 | 167710 | 570828 | 040248 | 653930 |
122513 | 714856 | 167710 | 167710 | 714856 | 653930 | 832186 |
217060 | 133641 | 465012 | 570828 | 040248 | 342970 | 217060 |
725410 | 187722 | 465012 | 167710 | 167710 | 712499

(ii) öffentlicher Schlüssel: $n = 902801$, $e = 65537$

443971 | 755299 | 640320 | 591219 | 198515 | 364196 | 131390 |
477933 | 704075 | 491944 | 890194 | 692686 | 173080 | 404345 |
308040 | 477933 | 390879 | 552292 | 277094 | 716033 | 197691

(iii) öffentlicher Schlüssel: $n = 182271469$, $e = 65537$

054787027 | 143188524 | 008028162 | 078128714 | 127863274 |
130225691 | 006129563 | 096160985 | 008028162 | 143188524 |
127863274 | 097393629 | 059509204 | 052542987 | 006216099 |
078128714 | 078568844 | 005560808