

## KRY: Wahlfach Kryptologie

### Serie 1: Einführung, RSA

**Bemerkung:** (P) steht für Programmieraufgabe, (T) steht für Theorieaufgabe.

#### Aufgabe 1 (P)

Um in der Kryptographie häufig vorkommende Operationen (modulare Arithmetik, Analyse von Gruppen, Rechnungen in speziellen Körpern etc) durchzuführen, werden wir das Tool PARI/GP verwenden.

- (a) Laden Sie sich PARI/GP auf Ihren Rechner.  
(Das zugehörige File ist z.B. unter <https://pari.math.u-bordeaux.fr/download.html> zu finden.)
- (b) Berechnen Sie zur Angewöhnung die folgenden Werte:  
(Ein Tutorial gibts z.B. hier: <http://www.math.uiuc.edu/~r-ash/GPTutorial.pdf>)
  - (i)  $4 + 7$
  - (ii) den grössten gemeinsamen Teiler von 98 und 280
  - (iii) den Rest von  $9746:17$ .

**Hinweis:** Benutzen Sie in den folgenden Aufgaben PARI/GP für die Berechnungen von Operationen innerhalb von Gruppen (Addition, Multiplikation, Exponentiation etc).

#### Aufgabe 2 (T)

Wir nehmen an, dass Bob für das RSA-Verfahren die Parameter  $N = 143$ ,  $e = 23$  und  $d = 47$  verwendet. Verschlüsseln Sie die Nachricht  $m = 9$  und führen Sie anschliessend die Entschlüsselungsoperation durch.

#### Aufgabe 3 (T)

- (a) Bestimmen Sie für  $\mathbb{Z}_{17}^*$  die von 2 erzeugte Untergruppe.
- (b) Berechnen Sie  $2^{-5}$  (in  $\mathbb{Z}_{17}^*$ )
- (c)
  - (i) Bestimmen Sie eine Primitivwurzel in  $\mathbb{Z}_{1237}^*$ .
  - (ii) Wie lässt sich aus der Primitivwurzel aus (i) ein Element der Ordnung 103 bilden?

$$2. \quad N = 143; e = 23; d = 47;$$

$$m = 9$$

Verschlüsselung:

$$c := m^e \bmod N \Rightarrow 9^{23} \bmod 143 = 3$$

Entschlüsselung:

$$m := c^d \bmod N \Rightarrow 3^{47} \bmod 143 = 9$$

$$3. \quad a) \quad \mathbb{Z}_{17}^* \quad \langle 2 \rangle = \{2, 4, 8, 16, 15, 13, 9, 1\}$$

$$b) \quad 2^{-5} \text{ in } \mathbb{Z}_{17}^*$$

$$(2^{-1})^5$$

$$2^{-1} \bmod 17 = 9 \rightarrow 9^5 \bmod 17 = 8$$

$$c) \quad i) \quad |\mathbb{Z}_{1737}^*| = 1736 = 2^2 \cdot 3 \cdot 103$$

**Aufgabe 4 (T)**

- (a) Berechnen Sie in  $\mathbb{Z}_{17}^*$ :  $\frac{1}{3} \cdot 5^{-7}$
- (b) Lösen Sie modulo 19:  $\frac{1}{2} \left( 4x + \frac{1}{3} \right) = \frac{1}{4} \cdot (12x + 1)$

**Aufgabe 5 (T)**

- (a) Bestimmen Sie die Anzahl aller für den RSA-Modul  $N = 437$  möglichen Verschlüsselungsexponenten  $e$ .
- (b) Alice verschlüsselt die Nachricht  $m$  mit Bobs öffentlichem RSA-Schlüssel  $(N, e) = (899, 11)$ . Der verschlüsselte Text ist 400. Bestimmen Sie den Klartext.