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. $N = 143$; $e = 23$; $d = 47$; $m = 9$

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

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

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

c) i) $|\mathbb{Z}_{1237}^*| = 1236 = 2^2 \cdot 3 \cdot 103$

$$2^{\frac{1236}{2}} \bmod 1237 \neq 1$$

$$2^{\frac{1236}{3}} \bmod 1237 \neq 1$$

$$2^{\frac{1236}{103}} \bmod 1237 \neq 1$$

ii) $2^{\frac{1236}{2}} = 2^{12}$

$$2^{12} \bmod 1237 = 385$$

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.

4. a) $3^{-1} \cdot 5^{-7} \bmod 17 = 4$

$3^{-1} \bmod 17 = 6$

$5^{-7} \bmod 17 = 12$

$6 \cdot 12 \bmod 17 = 4$

b) $2^{-1} \bmod 19 = 10$

$3^{-1} \bmod 19 = 13$

$4^{-1} \bmod 19 = 5$

$10 \cdot (4x + 13) = 5 \cdot (12x + 1) \quad // T$

$40x + 130 = 60x + 5 \quad // - 40x; -5$

$125 = 20x \quad // : 20$

$125 \bmod 19 = 11$

$20 \bmod 19 = 1$

$11 = x$

5. a) $N = 437 = 19 \cdot 23$

$|\mathbb{Z}_{19}^*| = 18 \; ; \; |\mathbb{Z}_{23}^*| = 22 \rightarrow 18 \cdot 22 = 396$

$e \cdot d \bmod 396 = 1$

Pari/gp $\rightarrow$ eulerphi(396) = 120

b) $N = 899 \; ; \; e = 11 \; ; \; c = 400$

eulerphi(899) = 840

$d = 11^{-1} \bmod 840 = 611$

$m = 400^d = 400^{611} \bmod 899 = 297$