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: `https://www.math.mcgill.ca/darmon/courses/12-13/nt/GPTutorial.pdf`)

(i) $4 + 7$ gp > 4+7

(ii) den grössten gemeinsamen Teiler von 98 und 280 gp > gcd(98,280)

(iii) den Rest von 9746:17. gp > 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.

Verschlüsselung: c = m^(e) mod N = 9 ^ (23) mod 143 = 3 -> c = 3!

Entschlüsselung: c^(d) mod N = 3 ^ (47) mod 143 = 9

Aufgabe 3 (T)

(a) Bestimmen Sie für $\mathbb{Z}_{17}^*$ die von 2 erzeugte Untergruppe. 1,2,4,8,16,15,13,9

(b) Berechnen Sie 2^{-5} (in $\mathbb{Z}_{17}^*$) 2^5 mod 17 = 15 -> 15^-1 mod 17
Mod(15,17)^-1 = 8

(c) (i) Bestimmen Sie eine Primitivwurzel in $\mathbb{Z}_{1237}^*$. znprimroot(1237) -> g = 2

(ii) Wie lässt sich aus der Primitivwurzel aus (i) ein Element der Ordnung 103 bilden?

2 ^ 12 mod 1237 = 385

Aufgabe 4 (T)

(a) Berechnen Sie in $\mathbb{Z}_{17}^*$: $\frac{1}{3} \cdot 5^{-7}$

1. 5^7 % 7 = 10
2. Mod(10,17)^-1 = Mod(12,17)
3. 12/3 = 4

(b) Lösen Sie modulo 19: $\frac{1}{2}\left(4x + \frac{1}{3}\right) = \frac{1}{4} \cdot (12x + 1)$

> 2^-1 * (4x + 3^-1) = 4^-1 * (12x+1)
> 10 * (4x + 13) = 5 * (12x + 1)
> 40x + 130 = 60x + 5
> 20x mod 19 = 125 mod 19
> x = 11

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.

a) factor(437) = 19 * 23

(19 -1) * (23-1) = 396

factor(396) = 2^2 * 3^2 * 11^1

2^2 - 2 * 3^2-3 * 11^1-1= 2*6*10=120 -> 120 Möglichkeiten

b) factor(899) = 29, 31

28*30= 840

Mod(11,840)^-1 = 611 mod 840

Mod(400,899)^611 = 297 mod 899