

Aufgaben 2

1. Führe den RSA-Algorithmus aus. Wähle dazu zunächst zwei Primzahlen p und q zwischen 3 und 11 aus. Wähle d und e entsprechend den Bedingungen (falls Du sie zu groß wählst, kann es sein, daß Dein Taschenrechner die nötigen Berechnungen nicht mehr ausführen kann. In dem Fall wähle erneut kleineres d und e . Beachte aber die Multiplikativität von mod!). Nun besitzt Du einen öffentlichen und einen privaten Schlüssel.

Dann wähle eine Zahl x zwischen 2 und 10. Verschlüssele x mit Deinem öffentlichen Schlüssel, und entschlüssele das Ergebnis mit Deinem privaten Schlüssel. Erhältst Du wieder x ?

2. Führe den ElGamal-Algorithmus aus. Wähle dazu die Gruppe (\mathbb{F}_7, \cdot) (Achtung: $0 \notin (\mathbb{F}_7, \cdot)$, also $\#F_7 = 6$). Da jedes Element außer 1 die Gruppe erzeugt, wähle $g = 2$. Wähle ferner ein $r \in \mathbb{Z}$ (je kleiner r ist, desto weniger mußt Du rechnen), und versuche dann, Elemente von \mathbb{F}_7 zu ver- und wieder zu entschlüsseln.

Beachte: Du mußt immer mod 7 rechnen! Um a^{-b} zu berechnen, beachte $a^{-b} = (a^b)^{-1}$ und suche das multiplikative Inverse von a^b in \mathbb{F}_7 (z.B. $4^{-1} = 4$ in \mathbb{F}_5 , da $4 \cdot 4 = 16 \equiv 1 \pmod{5}$).