SMS1 für MC, FHS Hagenberg
6. Übungsblatt für den 17. November 2005

Verwenden Sie Mathematica. Eventuell nützliche Funktionen sind `ExtendedGCD`, `Mod, PowerMod, Prime, FactorInteger`.

1. Bestimmen Sie jeweils das multiplikative Inverse von x in $\mathbb{Z}_n$:
   (a) $x = 17, n = 24$ (b) $x = 57, n = 459$ (c) $x = 353, n = 2005$

2. Für das RSA-Verfahren wählen wir $p = 5, q = 11$ und $e = 13$. Chiffrieren Sie $(1, 3, 22, 8)$ und dechiffrieren Sie das Ergebnis.

3. Entschlüsseln Sie die Nachricht $(1234, 56789)$, die mit dem öffentlichen Schlüssel $e = 13$ und $pq = 1334323339$ verschlüsselt wurde.

4. (a) Wählen Sie geeignete Zahlen p, q, e, d, um 2-stellige Zahlen mit dem RSA-Verfahren verschlüsseln zu können.
   (b) Verschlüsseln Sie 17 und 97.
   (c) Entschlüsseln Sie die Nachrichten aus (b).

5. Wählen Sie ein mathematisches Softwarepaket (Mathematica, Matlab, ...) oder ein Faktorisierungsprogramm im Web und testen Sie, bis zu welcher Größenordnung von ganzen Zahlen eine Primfaktorenzerlegung in "vernünftiger" Zeit möglich ist.