SMS1 für MC, FHS Hagenberg
4. Übungsblatt für den 28. Oktober 2004

1. Bestimmen Sie jeweils das multiplikative Inverse von x in $\mathbb{Z}_n$:
   (a) $x = 16, n = 35$ (b) $x = 56, n = 459$ (c) $x = 353, n = 2004$

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

3. Alice sendet Bob mit dem RSA-Verfahren die Nachricht $\{3, 8, 5, 5, 18, 19\}$. Bob weiß, dass Alice das RSA-Verfahren mit $(n = 35, k = 5)$ verwendet hat. Entschlüsseln Sie die Nachricht (A=1, B = 2, ..., Z=26)!

4. Entschlüsseln Sie die Nachricht $(5, 7, 11, 13)$, die mit $k = 13$ und $pq = 1334323339$ verschlüsselt wurde.

5. (a) Verschlüsseln Sie das Wort FHS $(A = 1, B = 2, \ldots, Z = 26)$ mit dem RSA-Verfahren $p = 3, q = 11$ und geeignetem k.
   (b) Entschlüsseln Sie die Nachricht aus (a).

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