



## 5. Übungsblatt

### ÜBUNGEN

#### **G1 (RSA).**

Bestimmen Sie alle möglichen Verschlüsselungsexponenten  $e$ , die für das RSA-Modul  $n = 35$  möglich sind.

#### **G2 (Primzahltest).**

Zum generieren von RSA-Modulen werden (meist) probabilistische Primzahltests verwendet. Also ist es nicht zu 100% sicher, dass  $p$  und  $q$  wirklich Primzahlen sind. Ist das gefährlich?

#### **G3 (Schnelle Exponentiation).**

Sie kennen einen Algorithmus zur schnellen Exponentiation, der die Bits des Exponenten vom niederwertigsten zum höchstwertigsten Bit verarbeitet. Entwerfen Sie einen Algorithmus, der die Bits in anderer Reihenfolge (vom höchstwertigsten zum niederwertigsten) durchgeht und verarbeitet.

Vergleichen sie beide Verfahren und finden sie Vor- bzw. Nachteile.