Aufgaben zur RSA-Verschlüsselung

Diese Aufgaben setzten voraus, dass man sich mit der RSA-Verschlüsselung z. B. über das passende Modul des Matheprisma `http://www.matheprisma.uni-wuppertal.de/Module/RSA/` auseinander gesetzt hat.

Aufgabe 1

Beschreiben Sie, wie die Verschlüsselung mit einem privaten und einem öffentlichen Schlüssel funktioniert.

Aufgabe 2

Geben Sie an, warum bei der RSA-Verschlüsselung eine Einwegfunktion mit einer sogenannten Falltür vorhanden sein muss.

Aufgabe 3

Zerlegen Sie die Zahl 589 in ihre beiden Primfaktoren.

Aufgabe 4

Erklären Sie, warum die Primfaktorzerlegung in der Regel schwierig ist, aber für die größere Zahl 299577 dennoch sehr einfach ist.

Aufgabe 5

Verschlüsseln Sie den Buchstaben J (ASCII-Code: 74) mit $N = 187, e = 7$ durch die Formel $C = M^e \mod N$.

Hinweis: Für $8^5 \mod 15$ ergibt sich mit $64/15 = 4,267$ und $8 \cdot 8 \mod 15 = 64 - 4 \cdot 15 = 4$ folgende Möglichkeit: $(8 \cdot 8 \mod 15) \cdot (8 \cdot 8 \mod 15) \cdot 8 \mod 15 = 4 \cdot 4 \cdot 8 \mod 15 = 4^2 \cdot 8 \mod 15$.

Aufgabe 6

Erklären Sie, weshalb man eine Nachricht bei der RSA-Verschlüsselung in Blöcke unterteilen muss, die einzeln verschlüsselt werden.

Aufgabe 7

Geben Sie an, welche Eigenschaften d haben muss, damit die Verschlüsselung und anschließende Entschlüsselung mit $M = C^d \mod N$ funktioniert.

Aufgabe 8

Weisen Sie nach, dass die Bedingung $(d \cdot e) \mod ((p-1)(q-1)) = 1$ für $N = 187, e = 7$ und $d = 23$ erfüllt ist.