Aufgaben zur RSA-Verschlüsselung

Diese Aufgaben setzten voraus, dass man sich mit der RSA-Verschlüsselung z. B. über das passende Modul des Matheprisma `https://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.

Lösungen zu den Aufgaben

Lösung 1

Eine Nachricht wird mit einem öffentlichen Schlüssel verschlossen. Anschließend kann sie auch nur mit dem dazugehörigen privaten Schlüssel wieder geöffnet werden. Bei RSA ist auch der umgekehrte Weg möglich, jedoch nicht, dass eine Nachricht mit dem gleichen Schlüssel ver- und entschlüsselt werden kann.

Lösung 2

Durch die Falltür wird es erst möglich, auf einfachem Wege wieder an die ursprünglichen Eingaben in die Funktion zu gelangen. Diese Eingabe ist bei der Verschlüsselung der Klartext.

Lösung 3

$31 \cdot 19 = 589$

Lösung 4

Die Primzahlen, aus denen sich ein Produkt zusammensetzt können nicht einfach erschlossen werden, sondern müssen aufwendig berechnet werden. Für die Zahl 299577 ist es aber sehr einfach, da mit $3 \cdot 99859 = 299577$ einer der beiden Primfaktoren sehr klein ist.

Lösung 5

$C = 74^7 \mod 187 = 167$

Lösung 6

Es muss stets gelten, dass $M < N$ ist, da sonst dass Ergebnis der Verschlüsselung bzw. Entschlüsselung nicht eindeutig ist.

Lösung 7

Es muss gelten, dass $(M^e)^d \mod N = M$ ist. Dazu muss e das modulare Inverse von d sein.

Lösung 8

Dazu müssen die Primfaktoren berechnet werden zu $p = 11$ und $q = 17$.