Aufgaben zu Kapitel 4: RSA-Verschlüsselung

Aufgabe 4.1 (Asymmetrische Verschlüsselung)

a) Welche Vorzüge besitzen asymmetrische Kryptosysteme im Vergleich zu symmetrischen Kryptosystemen?

b) Falls 10 Kommunikationsteilnehmer untereinander verschlüsselt Nachrichten austauschen möchten, wie viele Schlüssel werden insgesamt benötigt, falls symmetrische bzw. asymmetrische Verschlüsselung verwendet wird?

c) Welche Zahlen ergeben sich, falls sich die Teilnehmerzahl verzehnfacht?

Aufgabe 4.2 (Square-and-Multiply) Berechnen Sie mit dem Square-and-Multiply-Algorithmus (Potenzieren durch wiederholtes Quadrieren) $37^{58} \bmod 143$. Geben Sie die Zwischenschritte Ihrer Berechnung an.

Aufgabe 4.3 (RSA 1) Für das RSA-Verfahren werden folgende Werte gewählt: $p = 17$, $q = 19$ und $e = 35$.

a) Ermitteln Sie den öffentlichen und privaten Schlüssel. Geben Sie die Zwischenschritte Ihrer Berechnung an.

b) Verschlüsseln Sie die Nachricht $m = 250$. Erläutern Sie Ihren Rechenweg.

Aufgabe 4.4 (RSA 2)

a) Alice verwendet zur Verschlüsselung das RSA-Verfahren, hat für die Schlüsselgenerierung aber leider sehr kleine Primzahlen verwendet. Ihr öffentlicher Schlüssel ist $(3551, 35)$. Wie lautet ihr geheimer Schlüssel?

b) Bob wählt bei der Schlüsselgenerierung $p = 31$ und $q = 53$. Nun muss er e wählen. Welches ist das kleinstmögliche e, das er verwenden kann? Nutzen Sie dieses e, um die Nachricht 24 zu verschlüsseln. Welcher Geheimtext entsteht?

Aufgabe 4.5 (RSA 3)

a) Erläutern Sie, warum das Potenzieren der Nachricht m mit e und das anschließende Potenzieren des Geheimtextes mit d wieder die Nachricht m liefert.

b) Würde das Verfahren auch funktionieren, wenn zuerst mit d und anschließend mit e potenziert wird? Begründen Sie Ihre Antwort.

c) Erklären Sie, warum das RSA-Verfahren schwer zu brechen ist.