

RSA-Kryptosystem

Aufgabe 1. Bob will seinen privaten Schlüssel (p, q, d) und seinen öffentlichen Schlüssel (n, e) für den RSA-Umtausch konstruieren. Dafür wählt er $p = 5, q = 7$. Zählen Sie alle möglichen Varianten für beide Schlüssel nach.

Aufgabe 2. Sei $(p, q, d) = (7, 11, 43)$ der private Schlüssel von Bob.

(a) Berechnen Sie seinen öffentlichen Schlüssel (n, e) .

(b) Alice will Klartext $t = 19$ mit RSA-Verfahren chiffrieren und an Bob schicken. Wie sieht der Chiffretext $s = s(t)$ aus.

(c) Bob erhält den Chiffretext $s = 3$ von Claudia. Wie sieht ihr Klartext t aus?

Aufgabe 3. Bob hat einen öffentlichen Schlüssel $(n, e) = (3053, 23)$ und erhält einen Chiffretext $s = 1000$. Wie sieht der Klartext t aus?

Aufgabe 4. Identifizieren wir die Buchstaben a, b, \dots, z mit der Zahlen $1, 2, \dots, 26$. Dann können wir ein Block aus zwei Buchstaben mit einer Zahl identifizieren. Zum Beispiel $b := 2, p := 16$ und $bp := 2 \cdot 26 + 16$.

Sei $(n, e) = (3053, 23)$ der öffentlichen Schlüssel von Bob. Alice will das Wort Hallo mit RSA-Verfahren an Bob schicken. Dafür teilt sie das Wort in drei Blöcke : $|Ha||l||o|$, und kalkuliert entsprechende Zahlen n_1, n_2, n_3 . Danach chiffriert sie die Zahlen mit RSA-Verfahren und erhält die Zahlen m_1, m_2, m_3 . Die neuen Zahlen schickt sie mit dem offenen Kanal an Bob. Der Computer von Bob erhält die Zahlen und wandelt sie in Blöcke um (die Blöcke können Länge 1,2 oder 3 haben). Welchen Text wird Bob sehen?