

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. Finden Sie alle natürlichen Zahlen n mit $\phi(n) = 12$.

Aufgabe 4. Es ist bekannt, daß $n = 64777$ ein Produkt von zwei Primzahlen ist und $\phi(n) = 64260$. Finden Sie diese Primzahlen mit Hilfe des Kalkulators.