

Attacken auf das RSA-Kryptosystem

Aufgabe 1. Finden Sie alle natürlichen Zahlen n mit $\phi(n) = 24$.

Aufgabe 2. Es ist bekannt, daß $n = 64777$ ein Produkt von zwei Primzahlen ist und $\phi(n) = 64260$. Finden Sie diese Primzahlen mit Hilfe des Kalkulators.

Aufgabe 3. Finden Sie alle $a \in \mathbb{Z}_{21}^*$, so daß $\text{ord}_3(a^3) \neq \text{ord}_7(a^3)$ ist.

Aufgabe 4. (Weiner-Attacke) Bob benutzt das RSA-Kryptosystem. Sein öffentlicher Schlüssel (n, e) ist $(61093, 36353)$. Es ist bekannt, daß für die Primzahl-Zerlegung $n = pq$ gilt $q < p < 2q$. Beweisen Sie, daß sein privater Schlüssel d nicht weniger als 5 ist. Finden Sie (p, q, d) mit Hilfe des Kalkulators.

Aufgabe 5. Die öffentlichen Schlüssel von Alice, Bob und Claudia sind $(143, 3)$, $(391, 3)$ und $(899, 3)$. Eine Bank schickt ihnen denselben Klartext m mit Hilfe des RSA-Verfahrens. Sie erhalten die Chiffretexte 60, 203 und 711 entsprechend. Finden Sie m .

Aufgabe 6. Alice und Bob haben öffentliche Schlüssel (n_a, e_a) und (n_b, e_b) , wobei die Zahlen e_a, e_b teilerfremd sind **und** $n_a = n_b$ ist. Eine Bank schickt ihnen denselben Klartext. Sie erhalten die Chiffretexte t_a und t_b . Wie sieht der Klartext aus?