Übungszettel 10

RSA-Kryptosystem

Aufgabe 1. Finden Sie alle $a \in \mathbb{Z}_{21}^*$, so daß $\mathrm{ord}_3(a^3) \neq \mathrm{ord}_7(a^3)$ ist.

Aufgabe 2. (Weiner-Attacke) Bob benutzt das RSA-Kryptosystem. Sein öffentlicher Schlüssel (n, e) ist $(7387, 2405)$. Finden Sie den geheimen Schlüssel (p, q, d) mit Hilfe des Kalkulators.

Aufgabe 3. Der öffentliche Schlüssel von Bob ist $(899, 117)$. Eine Bank schickt ihm einen Klartext m mit Hilfe des RSA-Verfahrens. Er erhält den Chiffretext 5. Finden Sie m.

Aufgabe 4. 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?