7. Präsenzübungsblatt

Aufgabe 1 Sei $p = 5$, $q = 13$.
Dann ist $\varphi(pq) = ?$ Daher kann als öffentlicher Schlüssel $e = 5$ gewählt werden (Begründung!). Verschlüssele $m = 17$.
Dem Ergebnis sieht man nun nicht an, welche 5-Potenz es ist! Bestimme mit dem erweiterten euklidischen Algorithmus den geheimen Schlüssel d.

Aufgabe 2 Die Botschaft m wurde drei mal mit dem Schlüssel $e = 3$ verschlüsselt, aber mit verschiedenem n:

Mit $(n_1, e) = (55, 3)$ zu c_1;

Mit $(n_2, e) = (51, 3)$ zu c_2;

Mit $(n_3, e) = (46, 3)$ zu c_3.

Empfangen wurde $c_1 = 17, c_2 = 2, c_3 = 6$.
Finden Sie heraus, was die Botschaft m war.