

Übungen zur Vorlesung Panorama der Mathematik und Informatik**Blatt 13****Aufgabe 37: (Erweiterter euklidischer Algorithmus)**

Bestimmen Sie $\text{ggt}(1234, 4321)$. Finden Sie $a, b \in \mathbb{Z}$, so dass gilt

$$a \cdot 1234 + b \cdot 4321 = \text{ggt}(1234, 4321).$$

Aufgabe 38: (RSA)

Folgende Botschaft ist mit dem RSA-Verfahren verschlüsselt: 239845 075302 198960. Der öffentliche Schlüssel ist $N = pq = 262699$, $e = 207099$. Entschlüsseln Sie die Botschaft.

Jeder Block steht für drei Buchstaben. Wie üblich bedeutet 01: A, 02: B, ..., 26: Z, sowie diesmal ausnahmsweise 00: ! (Ausrufezeichen).

Aufgabe 39: (PGP)

Schicken Sie mir eine mit PGP (oder gpg) verschlüsselte Email, mit meinem Public Key codiert und mit Ihrer Signatur. Der Text soll Ihren Vor- und Nachnamen enthalten.

Rätsel der Woche:

Ein 3 km langer Demonstrationszug bewegt sich mit konstanter Geschwindigkeit vorwärts. Ein Polizist auf einem Motorrad am Ende des Zuges fährt (zum Zeitpunkt 0 los und) mit konstanter Geschwindigkeit (bzgl. des Bodens, nicht bezgl. des Demonstrationszugs) bis an die Spitze des Zuges, dreht unverzüglich (Verzögerung 0) und fährt mit derselben Geschwindigkeit zurück ans Ende des Zuges. In dieser Zeit hat der Demonstrationszug 4 km zurückgelegt. Welche Strecke hat der Polizist zurückgelegt?
