

Datensicherheit und Kryptografie

2. Übung

Abgabe: Lösen Sie Aufgaben **1** und **4**. Ihre Lösungen geben Sie bitte entweder

- bis zum 27.04.2022 um 20:00 Uhr per Mail
an `julian.pape-lange@informatik.tu-chemnitz.de`
mit *Betreff:* DuK Hausaufgaben oder
- nach der Vorlesung am 26.04.2022.

ab.

1. Aufgabe: ((3+4)P)

Seien $a = 96$ und $b = 252$. Bestimmen Sie den größten gemeinsamen Teiler von a und b

- mit den Primfaktorzerlegungen $96 = 2^5 \cdot 3^1$ und $252 = 2^2 \cdot 3^2 \cdot 7^1$ und
- mit dem Euklidischen Algorithmus.

2. Aufgabe:

Seien $a = 5$ und $M = 11$. Bestimmen Sie das Inverse von a modulo M durch durchsuchen aller Möglichkeiten. Erklären Sie, warum das Verfahren in $\mathcal{O}(M \log M)$ Zeit durchführbar ist.

3. Aufgabe:

Zeigen Sie, dass für alle natürlichen Zahlen a und b die Gleichung

$$\text{ggT}(a, b) \text{ kgV}(a, b) = a \cdot b$$

gilt.

4. Aufgabe: 3P

Geben Sie für den Euklidischen Algorithmus eine obere Schranke für die Anzahl der Runden an.