Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2023
13.04.2023

Datensicherheit und Kryptografie

2. Übung

Abgabe: Lösen Sie Aufgabe **2**. Ihre Lösungen geben Sie bitte entweder

- bis zum 20.04.2023 um 20:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`
  mit *Betreff:* `DuK Hausaufgaben` oder
- nach der Vorlesung am 18.04.2023

ab.

1. Aufgabe:
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: (2+4+4)P
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.
Finden Sie das Inverse von $a = 64$ modulo $M = 81$ mit Hilfe des erweiterten Euklidischen Algorithmus.

3. Aufgabe:
Zeigen Sie, dass für alle natürlichen Zahlen a und b die Gleichung

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

gilt.

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