Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2022
01.07.2022

Datensicherheit und Kryptografie

11. Übung

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

- bis zum 06.07.2022 um 20:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`
  mit *Betreff:* `DuK Hausaufgaben` oder
- nach der Vorlesung am 05.07.2022

ab.

1. Aufgabe:
Sei G eine endliche kommutative Gruppe mit Untergruppe U.

(a) Zeigen Sie, dass $|G|$ ein Vielfaches von $|U|$ ist.

(b) Sei G' eine weitere endliche kommutative Gruppe mit Homomorphismen $f : G \to G'$ und $g : G' \to G$. Zeigen Sie, dass das Bild von U bezüglich f und das Urbild von U bezüglich g Untergruppen von G' sind.

2. Aufgabe: (7+3)P
Schreiben Sie in einer Programmiersprache Ihrer Wahl ein möglichst effizientes Programm, das (echte) Potenzen erkennt. Wenn eine natürliche Zahl m eingegeben wird, soll also genau dann True ausgegeben werden, wenn es natürliche Zahlen b, e mit $e \geq 2$ gibt, sodass $m = b^e$ gilt.
Geben Sie auch die Laufzeit des Programms an.

3. Aufgabe:
Sei a eine Einheitswurzel modulo m und e eine ungerade Zahl. Zeigen Sie die Gleichung $a^e \equiv a \pmod{m}$.

4. Aufgabe:
Wir betrachten die Zahl $m = 8911 = 7 \cdot 19 \cdot 67$. Führen Sie den Primzahltest von Miller-Rabin aus der Vorlesung mit den Werten $a = 2$ und $a = 3$ aus.

5. Aufgabe:
Wir betrachten das Feistelchiffre. Verschlüsseln Sie die Nachricht `101001010110` mit der Funktion $f(K_i, R_i) = (R_i)^2 + K_i \pmod{2^6}$ in zwei Runden mit den Werten $K_1 = 7$ und $K_2 = 3$. Entschlüsseln Sie die Nachricht hinterher wieder.