Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2022
01.05.2022

Datensicherheit und Kryptografie

3. Übung

Abgabe: Lösen Sie Aufgaben **3** und **5**. Ihre Lösungen geben Sie bitte entweder

- bis zum 04.05.2022 um 20:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`
  mit *Betreff:* `DuK Hausaufgaben` oder
- nach der Vorlesung am 03.05.2022.

ab.

1. Aufgabe:
Finden Sie das inverse von $a = 64$ modulo $M = 81$ mit Hilfe des erweiterten Euklidischen Algorithmus.

2. Aufgabe:
In der Vorlesung vom 26.10.2022 wurden ab Minute 15 die Variablen q_i und q'_i eingeführt. Zeigen Sie, dass

(a) für gerade i die Ungleichung $q'_i > 0$ gilt,

(b) für ungerade i die Ungleichung $q'_i < 0$ gilt und

(c) für ungerade i die Ungleichung $|q'_{i+1}| \geq |q'_i|$ gilt.

3. Aufgabe: 6P
Berechnen Sie 4^{250} modulo 29.

4. Aufgabe:
Zeigen Sie den kleinen Satz des Fermat für festes p mit Induktion über a.
Hinweis: Benutzen Sie dazu den binomischen Lehrsatz.

5. Aufgabe: 4P
Sei $M = 17$. Wir verschlüsseln Werte $a (\mathrm{mod}\, M)$ als $a^V (\mathrm{mod}\, M)$ mit $V = 4$.
Finden Sie ein E, sodass für alle Nachrichten $a \equiv (a^V)^E (\mathrm{mod}\, M)$ gilt.
Begründen Sie, warum Ihr E richtig ist.