Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2023
20.04.2023

Datensicherheit und Kryptografie

3. Übung

Abgabe: Lösen Sie die Aufgaben **1** und **2**. Ihre Lösungen geben Sie bitte entweder

- bis zum 27.04.2023 um 20:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`
  mit *Betreff:* `DuK Hausaufgaben` oder
- nach der Vorlesung am 25.04.2023

ab.

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

2. Aufgabe: 4P
Sei $M = 23$. Wir verschlüsseln Werte $a (\mathrm{mod}\, M)$ als $a^V (\mathrm{mod}\, M)$ mit $V = 5$.
Finden Sie ein E, sodass für alle Nachrichten $a \equiv (a^V)^E (\mathrm{mod}\, M)$ gilt.
Begründen Sie, warum Ihr E richtig ist.

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

4. Aufgabe:
Seien m und n zwei teilerfremde Zahlen. Sei $\varphi(k)$ die Anzahl der Zahlen von 1 bis k (inklusive), die teilerfremd zu k sind.

(a) Geben Sie mit Hilfe der φ-Funktion die Anzahl der Zahlen von 1 bis m (inklusive) an, die nicht teilerfremd zu m sind.

(b) Geben Sie die Anzahl der Zahlen von 1 bis mn (inklusive) an, die nicht teilerfremd zu m sind.

(c) Geben Sie die Anzahl der Zahlen von 1 bis mn (inklusive) an, die weder teilerfremd zu m noch zu n sind.

(d) Geben Sie die Anzahl der Zahlen von 1 bis mn (inklusive) an, die zu mindestens einer der beiden Zahlen m und n teilerfremd sind.

(e) Zeigen Sie, dass $\varphi(mn) = \varphi(m)\varphi(n)$ gilt.

(f) Zeigen Sie, dass die Gleichung aus dem letzten Aufgabenteil für nicht teilerfremde Zahlen m, n (im Allgemeinen) nicht gilt.