Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2023
09.07.2023

Datensicherheit und Kryptografie

14. Übung

Abgabe: Lösen Sie die Aufgabe **1**. Ihre Lösungen geben Sie bitte

- bis zum 14.07.2023 um 13:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`

ab.

1. Aufgabe: $5 \cdot 2P$
Bestimmen Sie, ob die folgenden Zahlen Primzahlen sind.

- $m = 8481$,
- $m = 8911$,
- $m = 15841$,
- $m = 17377$ und
- $m = 41041$.

Hinweis: Pomerance et al. haben in „The pseudoprimes to $25 \cdot 10^9$" gezeigt, dass es für Zahlen $m < 1373653$ ausreicht, den Miller-Rabin-Primzahltest mit $a = 2$ und $a = 3$ auszuführen.

2. Aufgabe:
Wir wollen zeigen, wie das Finden von Ordnungen und das Faktorisieren zusammenhängen.
Finden Sie die Primfaktorzerlegung von 221. Verwenden Sie hierbei, dass die Ordnung von 2 modulo 221 gleich 24 ist.
Finden Sie die Ordnung von 4 modulo 323. Verwenden Sie hierbei, dass $323 = 17 \cdot 19$ gilt.