Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2023
27.04.2023

Datensicherheit und Kryptografie

4. Übung

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

- bis zum 04.05.2023 um 20:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`
  mit *Betreff:* `DuK Hausaufgaben` oder
- nach der Vorlesung am 02.05.2023

ab.

1. Aufgabe: 4P
Sei $M = 55 = 5 \cdot 11$. Wir verschlüsseln Werte $a (\mathrm{mod}\, M)$ als $a^V (\mathrm{mod}\, M)$ mit $V = 7$.
Finden Sie ein E, sodass für alle zu M teilerfremden Nachrichten a, die Gleichung

$$a \equiv (a^V)^E (\mathrm{mod}\, M)$$

gilt.
Begründen Sie, warum Ihr E richtig ist.

2. Aufgabe: 6P
Am Ende der Vorlesung vom 25.04.2023 wurde der RSA-Algorithmus beschrieben.
Rechnen Sie den Algorithmus mit folgenden Parametern durch:

(a) p und q sollen zwischen 10 und 20 sein,

(b) der Verschlüsselungsschlüssel ist V ist 3 und

(c) die Nachricht ist 10.

Geben Sie dabei an, welche Werte Alice und Bob berechnen und welche Werte die beiden senden.

3. Aufgabe:
Seien $p \neq q$ Primzahlen. Zeigen Sie mit Hilfe des kleinen Fermat, dass für alle $0 \leq a < pq$ (also auch nicht teilerfremde a), die Gleichung

$$a^{1+(p-1)(q-1)} \equiv a(\mathrm{mod}\, pq)$$

gilt.
Folgern Sie, dass für $e \equiv 1(\mathrm{mod}(p-1)(q-1))$ die Gleichung

$$a^e \equiv a(\mathrm{mod}\, pq)$$

folgt.

4. Aufgabe:
Wir haben in der letzten Übung gesehen, dass φ für teilerfremde Zahlen multiplikativ ist. Wir wollen in dieser Übung zeigen, dass für eine Zahl n mit Primfaktorzerlegung $n = \prod_{i=1}^{k} p_i^{e_i}$ (mit $i \neq j \Rightarrow p_i \neq p_j$ und $e_i \neq 0$) die Gleichung

$$\varphi(n) = \prod_{i=1}^{k} p_i^{e_i-1}(p_i - 1)$$

gilt.
Zeigen Sie dazu zunächst $\varphi(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1)$.