Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2022
05.05.2022

Datensicherheit und Kryptografie

4. Übung

Abgabe: Lösen Sie Aufgaben **1**, **3** und **4**. Ihre Lösungen geben Sie bitte entweder

- bis zum 11.05.2022 um 20:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`
  mit *Betreff:* `DuK Hausaufgaben` oder
- nach der Vorlesung am 10.05.2022.

ab.

1. 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 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:
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.

3. Aufgabe: 4P
Es sind die beiden Kongruenzen

$$x \equiv 3 (\mathrm{mod}\, 11)$$

und

$$x \equiv 5 (\mathrm{mod}\, 13)$$

gegeben.
Geben Sie ein x zwischen 0 und $142 = 11 \cdot 13 - 1$ an, dass die beiden Kongruenzen löst.

4. Aufgabe: 6P
In der Vorlesung vom 03.05.2022 wurde ab Minute 41 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.

5. Aufgabe:
Seien m und n zwei teilerfremde Zahlen.

(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.