Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2022
12.05.2022

Datensicherheit und Kryptografie

5. Übung

Abgabe: Lösen Sie die Aufgabe **5**. Ihre Lösungen geben Sie bitte entweder

- bis zum 18.05.2022 um 20:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`
  mit *Betreff:* `DuK Hausaufgaben` oder
- nach der Vorlesung am 17.05.2022

ab.

1. Aufgabe:
Nutzen Sie den Chinesischen Restsatz, um alle Zahlen x zu finden, die $0 \leq x < 187 = 11 \cdot 17$ und $x^2 \equiv 1 \pmod{187}$ erfüllen.

2. Aufgabe:
Geben Sie für die Funktion

$$\begin{aligned} \mathbb{Z}/15\mathbb{Z} &\to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ x &\mapsto (x \mod 3, x \mod 5) \end{aligned}$$

für $0 \leq x < 15$ alle Funktionswerte an.

3. Aufgabe:
Zeigen Sie, dass für alle $0 \leq a < 561 = 3 \cdot 11 \cdot 17$ die Äquivalenz $a^{561} \equiv a \pmod{561}$ gilt.
Hinweis: Benutzen Sie zwei mal den Chinesischen Restsatz und verwenden Sie, dass die Abbildung aus dem Chinesischen Restsatz die Gleichung $f(h \cdot jh') = f(h) \cdot f(h')$ erfüllt.

4. Aufgabe:
Seien p, q und q' Primzahlen. Geben Sie an, wann die simultane Kongruenz

$$\begin{aligned} x &\equiv a \pmod{pq} \\ x &\equiv b \pmod{pq'} \end{aligned}$$

eine Lösung hat und beschreiben Sie, wie Sie die Lösung algorithmisch ermitteln können.

5. Aufgabe: (5·2)P
Die folgenden Verschlüsselungen sind nicht sicher!
Brechen Sie die Verschlüsselungen, indem Sie entweder den Entschlüsselungsschlüssel E, die Zusatzinformation $\varphi(M)$ oder die Nachricht a angeben. Einer der drei Werte reicht, Sie müssen keine Rechnung angeben.
Jede der 5 in der am Ende der Vorlesung vom 10.05.2022 angegebenen Schwachstellen ist mindestens ein Mal vorhanden.

(a) $V = 3$, $M = 449485$, $a^V \equiv 123456 \pmod{M}$

(b) $V = 3$, $M = 1727782939$, $a^V \equiv 125 \pmod{M}$

(c) $V = 1482460227$, $M = 2223784657$, $a^V \equiv 314159265 \pmod{M}$

(d) $V = 3$, $M = 42071 \cdot 42083$, $a^V \equiv 42 \pmod{M}$

(e) $V = 3$, $M = 1241611573$, $a^V \equiv 243709603 \pmod{M}$