Institut für Informatik
Prof. Dr. J. Rothe

Sommersemester 2024
Übungsblatt 1

Übung zur Vorlesung

Kryptokomplexität II

Bearbeitungszeit: 9. April bis 26. April
Verantwortlich: Roman Zorn

Begründen Sie Ihre Antworten und bereiten Sie sie so vor, dass Sie sie in der Übung präsentieren können.

Aufgabe 1: Wiederholung: Chinesischer Restsatz

► Lösen Sie das folgende Kongruenzsystem für x, $0 \leq x \leq 27$,

$$\begin{aligned} x &\equiv 3 \mod 4, \\ x &\equiv 1 \mod 7. \end{aligned}$$

Aufgabe 2: Wiederholung: RSA

(a) Gegeben sei der RSA-Modul $n = 91$.
► Sind $e_1 = 1, e_2 = 3$, und $e_3 = 13$ jeweils gültige öffentliche Exponenten? Begründen Sie Ihre Antwort.

(b) ► Berechnen Sie für jeden gültigen Exponenten aus Aufgabenteil (a) den zugehörigen privaten Exponenten d. Verwenden Sie den erweiterten Euklidischen Algorithmus.

(c) ► Berechnen Sie mit Hilfe von Fermats kleinem Satz

$$127^{247} \mod 83.$$

(d) ► Wie viele gültige öffentliche Exponenten gibt es für den RSA-Modul $n = 4141$?

Aufgabe 3: Wiederholung: Zahlentheoretische Grundlagen

▶ Beweisen Sie, dass es unendlich viele Primzahlen gibt.