Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2023
11.05.2023

Datensicherheit und Kryptografie

6. Übung

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

- bis zum 18.05.2023 um 20:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`
  mit *Betreff:* `DuK Hausaufgaben` oder
- nach der Vorlesung am 16.05.2023

ab.
Sie dürfen für elementare Rechnungen wie $a^b \bmod c$ technische Hilfsmittel verwenden. Sie brauchen für diese Rechnungen keine Zwischenschritte mehr angeben.

1. Aufgabe: (3+3+4)P
Wir betrachten die RSA-Signatur und die RSA-Verschlüsselung.
Alice hat als Schlüsselpaar

$$\text{den privaten Schlüssel } (1387, 2173) \text{ und}$$
$$\text{den öffentlichen Schlüssel } (3, 2173).$$

Bob hat als Schlüsselpaar

$$\text{den privaten Schlüssel } (859, 1363) \text{ und}$$
$$\text{den öffentlichen Schlüssel } (3, 1363).$$

Alice möchte mit Hilfe von RSA die Nachricht $N = 127$

(a) verschlüsselt,

(b) signiert und

(c) verschlüsselt und signiert

an Bob senden. Bob möchte die Nachricht (wenn möglich) entschlüsseln und die Echtheit der Nachricht verifizieren.
Geben Sie alle dafür nötigen Berechnungen und Übertragungen von Alice und Bob an.

2. Aufgabe:
Erklären Sie, warum Alice für die Signatur normalerweise lange vor der zu signierenden Nachricht erstellt und verteilt.
Finden Sie heraus, wie Sie die öffentlichen Schlüssel der von Ihnen besuchten Internetseiten bekommen haben.

3. Aufgabe:
In der Vorlesung haben wir gelernt, dass die Anzahl $\pi(x)$ der Primzahlen kleiner als x mit $\pi(x) = \frac{x}{\log(x)}(1 + o(1))$ abgeschätzt werden kann. Daher gilt für hinreichend große x die Abschätzung $0{,}9\frac{x}{\log(x)} < \pi(x) < 1{,}1\frac{x}{\log(x)}$.

(a) Geben Sie mit dieser Abschätzung für hinreichend großes n Schranken für die Anzahl der Primzahlen zwischen 2^n und 2^{n+1} an.

(b) Schätzen Sie die Wahrscheinlichkeit ab, dass eine zufälig gezogene Zahl zwischen 2^n und 2^{n+1} eine Primzahl ist.

4. Aufgabe:
Wenn p eine Primzahl ist, gilt für alle a mit $\text{ggt}(a, p) = 1$ die Äquivalenz

$$a^{p-1} \equiv 1 \pmod{p}.$$

Zeigen Sie, dass es ein a gibt, sodass für alle $1 \leq 1 < p - 1$

$$a^i \not\equiv p \pmod{p}$$

gilt.