Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2022
20.05.2022

Datensicherheit und Kryptografie

6. Übung

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

- bis zum 25.05.2022 um 20:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`
  mit *Betreff:* `DuK Hausaufgaben` oder
- nach der Vorlesung am 24.05.2022

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:
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.

2. Aufgabe:

(a) Finden Sie ein x mit $3^x \equiv 20 \pmod{29}$.

(b) Berechnen Sie $3^{16} \bmod 31$.

(c) Geben Sie für beide Probleme die Laufzeitkomplexität an.

3. Aufgabe: (3+3)P

(a) Wir betrachten den Diffie-Hellman-Schlüsselaustausch aus der Vorlesung vom 17.05.2022.

Alice und Bob wählen als Modul $M = 37$ und als Basis $g = 2$. Alice wählt als geheimen Exponenten $S_A = 6$ und Bob wählt $S_B = 9$.

Geben Sie an, sämtliche Berechnungen und Übertragungen von Alice und Bob für den Diffie-Hellman-Schlüsselaustausch an.

(b) Wir betrachten nun die El-Gamal-Verschlüsselung aus der Vorlesung vom 17.05.2022.

Alice und Bob wählen wieder als Modul $M = 37$ und als Basis $g = 2$. Alice wählt als geheimen Exponenten $S_A = 6$ und Bob wählt als Sitzungsschlüssel $S_B = 11$ und als Nachricht $N = 7$.

Geben Sie an, sämtliche Berechnungen und Übertragungen von Alice und Bob für die Ver- und Entschlüsselung mit El-Gamal an.

4. Aufgabe: 4P

Wir betrachten die RSA-Signatur aus der Vorlesung vom 17.05.2022 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 $N = 127$ verschlüsselt und signiert an Bob senden. Bob möchte die Nachricht entschlüsseln und die Echtheit der Nachricht verifizieren.
Geben Sie alle dafür nötigen Berechnungen und Übertragungen von Alice und Bob an.