Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2023
03.05.2023

Datensicherheit und Kryptografie

5. Übung

Abgabe: Lösen Sie die Aufgaben **2** und **3**. Ihre Lösungen geben Sie bitte entweder

- bis zum 11.05.2023 um 20:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`
  mit *Betreff:* `DuK Hausaufgaben` oder
- nach der Vorlesung am 09.05.2023

ab.

1. Aufgabe:
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.

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

2. Aufgabe: (3+3)P

(a) Wir betrachten den Diffie-Hellman-Schlüsselaustausch aus der Vorlesung vom 02.05.2023.

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 Elgamal an.

3. Aufgabe: 4P

(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.

4. Aufgabe:
Bei dem Diffie-Hellman-Schlüsselaustausch müssen sich Alice und Bob zuerst auf geeignete Werte für g und M einigen.
Erklären Sie, warum es vorteilhaft ist, wenn M eine Primzahl ist und $\varphi(M)$ eine bekannte Primfaktorzerlegung mit möglichst wenigen Teilern hat.
Geben Sie ein Verfahren an, um ein geeignetes g zu bestimmen.