Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2022
02.06.2022

Datensicherheit und Kryptografie

8. Übung

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

- bis zum 15.06.2022 um 20:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`
  mit *Betreff:* `DuK Hausaufgaben` oder
- nach der Vorlesung am 14.06.2022

ab.

1. Aufgabe:
Wir betrachten noch einmal die (richtige) Elgamal-Signatur aus der Vorlesung vom 24.05.2022 mit $M = 37$ und $g = 2$.

(a) Finden Sie ein Beispiel, in der die Formel

$$g^{S_{AI} g^k + ks} \equiv g^N \qquad (\mathrm{mod}\, M)$$

erfüllt ist und $k = M - 1$ gilt.

Hinweis: Wählen Sie die Variable N als letztes.

(b) Finden Sie ein Beispiel, in der die Formel

$$g^{S_{AI} g^k + ks} \equiv g^N \qquad (\mathrm{mod}\, M)$$

erfüllt ist und $1 < \mathrm{ggT}(k, M-1) < M - 1$ gilt.

(c) Wie kann mit Hilfe der Primfaktorzerlegung von $M - 1 = 2 \cdot 2 \cdot 3 \cdot 3$ effizient entschieden werden, ob für ein gegebenes g^k die Ungleichung $\mathrm{ggT}(k, M-1) > 1$ gilt?

Hinweis: g wurde so gewählt, dass

$$g^i \equiv 1 \qquad (\mathrm{mod}\, M) \qquad \Leftrightarrow \qquad i \equiv 0 \qquad (\mathrm{mod}\, M-1)$$

gilt.

(d) Welches Problem tritt auf, wenn $\mathrm{ggT}(k, M-1)$ groß ist?

2. Aufgabe:
Wir betrachten das bitweise exklusive Oder „$\oplus$“.

(a) Begründen Sie, warum $\oplus$ kommutativ ist.

(b) Zeigen Sie, warum $\oplus$ assoziativ ist.

(c) Zeigen Sie, dass für alle Zahlen a die Gleichungen $a \oplus a = 0$ und $a \oplus 0 = a$ gelten.

(d) Gegeben sind zwei unterschiedliche Variablen a und b. Tauschen Sie den Inhalt von a und b ohne zusätzliche Variablen zu verwenden.

3. Aufgabe:
Wir betrachten One-Time-Pad.

(a) Alice hat den Schlüssel $S =$ `101011111000` und möchte die Nachrichten $N_1 =$ `1011` und $N_2 =$ `01110` verschlüsseln. Berechnen Sie die verschlüsselten Nachrichten und zeigen Sie, wie die Entschlüsselung funktioniert.

(b) Aufgrund von Verlustbehafteten Übertragungskanälen kann es sein, dass die Verschlüsselte Nachricht von N_1 nicht bei Bob ankommt. Wie kann Alice sicherstellen, dass Bob trotzdem N_2 entschlüsseln kann, falls zumindest die Verschlüsselte Nachricht von N_2 ankommt?

4. Aufgabe:
Wir können Texte durch Vertauschen der Zeichen verschlüsseln. Dafür ist eine Permutation, zum Beispiel $A = [3, 1, 2, 4]$ gegeben und ein Text $T =$ `abcd` wird durch vertauschen der Zeichen mit der Vorschrift $T'[i] = T[A[i]]$ verschlüsselt. In diesem Fall gilt also $T' =$ `bcad`.
Ich habe einen einfachen Text mit der Permutation

$$A = [1, 6, 11, 16, 2, 7, 12, 17, 3, 8, 13, 18, 4, 9, 14, 19, 5, 10, 15, 20]$$

verschlüsselt und

$$T' = \texttt{e\_a\_iectniheenexnfnt}$$

erhalten. Entschlüsseln Sie T'.