Institut für Informatik
Prof. Dr. J. Rothe

Sommersemester 2024
Übungsblatt 5

Übung zur Vorlesung

Kryptokomplexität II

Bearbeitungszeit: 7. Mai bis 17. Mai
Verantwortlich: Roman Zorn

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

Aufgabe 1: Algorithmus von Pohlig und Hellman

► Berechnen Sie $a = \log_2 26$ in $\mathbb{Z}_{37}^*$ mit dem Algorithmus von Pohlig und Hellman.

Aufgabe 2: ElGamals Public-Key-Kryptosystem

(a) Alice und Bob einigen sich auf $p = 367$ und das primitive Element $\gamma = 17$ in $\mathbb{Z}_{367}^*$. Alice möchte die Nachricht $m = 103$ an Bob verschicken und wählt dafür die private Zahl $a = 97$. Bob wählt die private Zahl $b = 129$.
► Führen Sie das Protokoll für das Kryptosystem von ElGamal durch. Geben Sie dabei alle benötigten Zwischenschritte an.

(b) Alice möchte die Nachrichten m_1 und m_2 verschlüsseln. Sie wählt bei beiden Verschlüsselungen die gleiche zufällige Zahl a. $\alpha_{2,i}$ bezeichne für $i \in \{1, 2\}$ das von Alice berechnete α_2 der i-ten Nachricht.
► Zeigen Sie, dass sich bei bekannter Nachricht m_2 die Nachricht m_1 durch die Gleichung $m_1 = \alpha_{2,1} \cdot \alpha_{2,2}^{-1} \cdot m_2$ berechnen lässt.

Aufgabe 3: ElGamal – Signaturen

Betrachten Sie das digitale Signatur-Schema von ElGamal mit den bekannten Werten $p = 383$ und $\gamma = 5$.

(a) ► Für die Signatur einer Nachricht muss Bob eine geheime Zahl s wählen. Begründen Sie, welche der folgenden s_i gültig sind.

- $s_1 = 1$
- $s_2 = 29$
- $s_3 = 38$

(b) ▶ Bob wählt den privaten Exponenten $b = 15$. Signieren Sie die Nachricht $m = 23$ mit $s = 29$.

(c) ▶ Ist folgende Signatur gültig bei $p = 383$ und $\gamma = 5$?

$$\langle 24, 25, (163, 69) \rangle$$

Aufgabe 4: ElGamal – Key-only-Angriff

Betrachten Sie erneut das digitale Signatur-Schema von ElGamal mit den bekannten Werten $p = 383,\ \gamma = 5$. Diesmal ist $\beta = 68$.

(a) ▶ Welche Nachricht m kann ein Angreifer signieren, wenn er für einen Key-only-Angriff die Zahlen $x = 33$ und $y = 7$ wählt? Geben Sie auch die Signatur an.

(b) ▶ Zeigen Sie, dass Ihre in (a) berechnete Signatur tatsächlich gültig ist.

(c) ▶ Bewerten Sie, wie geeignet der Angriff ist, um gezielt eine bestimmte Nachricht in falschem Namen zu signieren.