Institut für Informatik
Prof. Dr. J. Rothe

Sommersemester 2024
Übungsblatt 4

Übung zur Vorlesung
Kryptokomplexität II

Bearbeitungszeit: 30. April bis 10. Mai
Verantwortlich: Roman Zorn

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

Aufgabe 1: Primitive Elemente III
Es sei p eine ungerade Primzahl und γ ein primitives Element in $\mathbb{Z}_p^*$.
► Zeigen Sie:

$$\textit{Es gilt } \gamma^{(p-1)/2} \equiv -1 \mod p.$$

Aufgabe 2: Schlüsselvereinbarung von Diffie und Hellman

(a) ► Zeigen Sie, dass $\gamma = 17$ ein primitives Element in $\mathbb{Z}_{487}^*$ ist.

(b) ► Führen Sie das Schlüsselvereinbarungsprotokoll von Diffie und Hellman für $p = 487$, $\gamma = 17$, $a = 112$ und $b = 72$ durch. Geben Sie dabei alle relevanten Zwischenschritte an.

Aufgabe 3: Man-in-the-Middle-Angriff
Seien $p = 37$ und $\gamma = 18$ für eine Schlüsselvereinbarung nach dem Protokoll von Diffie und Hellman gegeben. Alice und Bob wählen die privaten Zahlen $a = 103$ bzw. $b = 97$. Allerdings fängt ein *Man in the Middle* die öffentlichen Zahlen α und β ab und führt mit der Zahl $e = 7$ einen *Man-in-the-Middle*-Angriff durch.

(a) ► Welchen Schlüssel $k_{A,E}$ teilt er sich mit Alice und welchen Schlüssel $k_{B,E}$ teilt er sich mit Bob?

(b) ► Welche Schlüssel $k_{E,A}$ und $k_{E,B}$ berechnet der *Man in the Middle*?

(c) ► Welchen Schlüssel hätten sich Alice und Bob ohne den Angriff geteilt?

Aufgabe 4: Algorithmus von Shanks
► Berechnen Sie $a = \log_3 101$ in $\mathbb{Z}_{127}^*$ mit dem Algorithmus von Shanks.