Übung zur Vorlesung Kryptokomplexität II

Bearbeitungszeit: 4. Juni bis 14. Juni
Verantwortlich: Roman Zorn

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

Aufgabe 1: Merkle-Hellman-Kryptosystem

Führen Sie das Kryptosystem von Merkle und Hellman mit $\vec{s} = (2, 5, 9, 20, 38)$, $p = 101$, $b = 13$ und $\vec{m} = (1, 1, 0, 1, 0)$ durch. Testen Sie dabei, ob die gegebenen Werte gültig sind und geben Sie alle relevanten Zwischenschritte an.

Aufgabe 2: Einwegfunktion

► Zeigen Sie, dass keine totale, assoziative Einwegfunktion $\sigma : \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$ injektiv sein kann.

Aufgabe 3: Shamirs No-Key-Protokoll

Betrachten Sie Shamirs No-Key-Protokoll mit der Primzahl p . Ella wählt e und Paula wählt d . Ella möchte die Nachricht m an Paula senden.

► Konstruieren Sie eine Man-In-The-Middle-Attack, mit der die Eltern die Nachricht unbemerkt mitlesen können. Geben Sie dabei den Ablauf des Protokolls vollständig an.

Aufgabe 4: Wiederholung: Aussagen der Komplexitätstheorie

Zeigen Sie die folgenden Aussagen:

- (a) ► P ist eine Teilmenge von NP .
- (b) ► Ist $A \leq_m^p B$ und $B \in P$, so ist $A \in P$.
- (c) ► Ist B NP -vollständig, $B \leq_m^p C$ und $C \in NP$, so ist C NP -vollständig.
- (d) ► Ist B NP -vollständig und $B \in P$, so ist $P = NP$.