Institut für Informatik
Prof. Dr. J. Rothe

Sommersemester 2024
Übungsblatt 9

Lösungsvorschläge

Kryptokomplexität II

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

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.

Lösungsvorschlag: Voraussetzungen prüfen:

- $2, 5, 9, 20, 38$ ist eine superwachsende Folge, da $2 < 5$, $2 + 5 < 9$, $2 + 5 + 9 < 20$ und $2 + 5 + 9 + 20 < 38$.
- $p = 101$ ist eine Primzahl mit $p > 2 + 5 + 9 + 20 + 38 = 74$
- $b = 13$ ist Teilerfremd zu p.

Nun berechnen wir den öffentlichen Schlüssel $\vec{t} = (b \cdot s_1 \mod p, ..., b \cdot s_n \mod p) = (26, 65, 16, 58, 90)$.

Alice		Bob
		$\vec{s} = (2, 5, 9, 20, 38), p = 101, b = 13$,
	$\xleftarrow{\vec{t}}$	$\vec{t} = (26, 65, 16, 58, 90)$
$\vec{m} = (1, 1, 0, 1, 0)$ $c = \sum_{i=1}^{5} m_i \cdot t_i$ $= 26 + 65 + 58 = 149$	$\xrightarrow{c}$	
		$T = b^{-1} \cdot c \equiv 70 \cdot 149 \equiv 27 \mod 101$ Suche Lösung für die SOS-Instanz $\langle \vec{s}, T \rangle = \langle 2, 5, 9, 20, 38, T = 27 \rangle$ (z. B. mit Algorithmus von Blatt 8): Es gilt $27 = 2 + 5 + 20 = s_1 + s_2 + s_4$, also ist $m = (1, 1, 0, 1, 0)$ die entschlüsselte Nachricht.

Aufgabe 2: Einwegfunktion

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

Lösungsvorschlag: [a] Angenommen die Funktion $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$ ist injektiv, assoziativ und total. Wähle beliebige $x, y \in \Sigma^*$. Weil σ total ist, ist $\sigma(y,y), \sigma(y,x), \sigma(x,y)$ und $\sigma(x,x)$ immer definiert.

- Wegen der Assoziativität gilt $\sigma(\sigma(x,y),x) = \sigma(x,\sigma(y,x))$.
- Wegen der Injektivität muss gelten, dass $\sigma(\sigma(x,y),x) = \sigma(x,\sigma(y,x))$ genau dann wenn $(\sigma(x,y),x) = (x,\sigma(y,x))$.
- Das wiederum bedeutet, dass $\sigma(x,y) = \sigma(y,x) = x$.
- Dann hat aber x zwei Urbilder, was ein Widerspruch zur Annahme der Injektivität ist.

[a] Rabi, M; Sherman, A. *An Observation on Associative One-Way Functions in Complexity Theory.* Information Processing Letters, Elsevier Science B. V., 64(5):239–244, 1997.

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.

Lösungsvorschlag:
Die Eltern müssen auch eine geheime Zahl s mit $\mathrm{ggT}\,(s, p-1) = 1$ wählen. Gegenüber Ella werden sie so tun, als wären sie Paula, gegenüber Paula werden sie sich als Ella ausgeben.

Ella	Eltern	Paula
Ella und Paula einigen sich auf die Primzahl p.		
Berechnet $x_1 = m^e \mod p$		
	$\xrightarrow{x_1}$	
	Berechnen $y_1 = x_1^s \mod p$	
	$\xleftarrow{y_1}$	
Berechnet $z_1 = y_1^{e^{-1}} \mod p$		
	$\xrightarrow{z_1}$	
	Berechnen $m = z_1^{s^{-1}} \mod p$	
Nun geben sich die Eltern gegenüber Paula als Ella aus und übermitteln m.		
	Berechnen $x_2 = m^s \mod p$	
		$\xrightarrow{x_2}$
		Berechnet $y_2 = x_2^d \mod p$
		$\xleftarrow{y_2}$
	Berechnet $z_2 = y_2^{s^{-1}} \mod p$	
		$\xrightarrow{z_2}$
		Berechnet $m = z_2^{d^{-1}} \mod p$

Aufgabe 4: Wiederholung: Aussagen der Komplexitätstheorie

Zeigen Sie die folgenden Aussagen:

(a) ▶ P ist eine Teilmenge von NP.

(b) ▶ Ist $A \leq_{\mathrm{m}}^{\mathrm{p}} B$ und $B \in \mathrm{P}$, so ist $A \in \mathrm{P}$.

(c) ▶ Ist B NP-vollständig, $B \leq_{\mathrm{m}}^{\mathrm{p}} C$ und $C \in \mathrm{NP}$, so ist C NP-vollständig.

(d) ▶ Ist B NP-vollständig und $B \in \mathrm{P}$, so ist $\mathrm{P} = \mathrm{NP}$.

Lösungsvorschlag:

(a) Für Probleme in NP gilt, dass man sie mit einer nichtdeterministischen Turingmaschine in Polynomialzeit entscheiden kann. Probleme in P können von einer deterministischen Turingmaschine in Polynomialzeit entschieden werden.

Da jede deterministische Turingmaschine nur eine nichtdeterministische Turingmaschine ist, die von ihrem Nichtdeterminismus keinen Gebrauch macht, kann jedes Problem aus P auch von einer nichtdeterministischen Turingmaschine in Polynomialzeit entschieden werden, ist also auch in NP.

(b) Da $B \in \mathrm{P}$, existiert ein Polynomialzeit-Algorithmus M, der B entscheidet. Da $A \leq_{\mathrm{m}}^{\mathrm{p}} B$ gilt, existiert auch eine in Polynomialzeit berechenbare Funktion f, die A auf B reduziert, d.h. I ist eine JA-Instanz für A, genau dann wenn $f(I)$ eine JA-Instanz für B ist.

Um zu zeigen, dass $A \in \mathrm{P}$ genügt es, einen Polynomialzeit-Algorithmus anzugeben, der A entscheidet:

- Eingabe I
- Bestimme $I' = f(I)$
- Gebe JA zurück, falls $M(I')$ JA zurück gibt. Ansonsten gib NEIN zurück.

Wegen den oben beschriebenen Eigenschaften von M und f ist der Algorithmus in Polynomialzeit berechenbar und entscheidet A.

(c) Um zu zeigen, dass C tatsächlich NP-vollständig ist, müssen wir zwei Dinge zeigen:

1) C ist in NP.
2) Jedes $A \in \text{NP}$ ist polynomialzeit-reduzierbar auf C.

Nummer 1 haben wir nach Voraussetzung bereits gegeben.

Da B NP-vollständig ist, ist jedes $A \in \text{NP}$ in Polynomialzeit reduzierbar auf B, dh. es gibt eine polynomialzeit-berechenbare Funktion f_A, die A auf B reduziert.

Wir wissen, dass B ebenfalls in Polynomialzeit auf C reduzierbar ist. Sei f_B eine polynomialzeit-berechenbare Funktion, die B auf C reduziert. Dann ist für jedes $A \in \text{NP}$ die Funktion $g_A(I) = f_B(f_A(I))$ ebenfalls in Polynomialzeit berechenbar. Offensichtlich reduziert g_A das Problem A auf C. Damit haben wir die zweite Eigenschaft gezeigt.

(d) B ist NP-vollständig, also gilt

1) B ist in NP.
2) Jedes $A \in \text{NP}$ ist polynomialzeit-reduzierbar auf B, d.h. $A \leq_{\text{m}}^{\text{p}} B$ für alle $A \in \text{NP}$.

Wenn nun $B \in \text{P}$, dann können wir wie in Aufgabenteil (b) zeigen, dass alle Probleme $A \in \text{NP}$ ebenfalls in P sind. Weil umgekehrt auch alle Probleme aus P ebenfalls in NP liegen (siehe Aufgabenteil (a)), folgt $\text{P} = \text{NP}$.