Aufgabe 9 (10 Punkte)

Alice und Bob möchten einen symmetrischen Schlüssel im Geheimen austauschen. Dazu verwenden Sie das Diffie-Hellman-Key-Exchange-Verfahren. Beide einigen sich auf $p = 43$ und $g = 3$.

(9.1) (1 Punkt) Welche Eigenschaft muss g erfüllen, damit dieses Verfahren funktioniert?

(9.2) (2 Punkte) Alice wählt im Geheimen $a = 11$ und verschickt $x = 30$ an Bob. Bob wiederum verschickt $y = 32$ an Alice. Wie lautet ihr gemeinsamer Schlüssel?

(9.3) (7 Punkte) Berechnen Sie die geheime Zahl b von Bob mit Hilfe des Baby-Step-Giant-Step Algorithmus. Geben Sie alle Zwischenschritte Ihrer Berechnung an.

Hinweis: Ein Repräsentant des multiplikativ Inversen von $[g]_p$ ist 29.

Brzezinski, Christiansen,
Ullmann, Zimmermann

NORDAKADEMIE

30. September 2019

Aufgabe 1 (8 Punkte)

In den folgenden Multiple Choice Aufgaben sind je 3 Antworten richtig.

Tipp: Nehmen Sie sich für das Lesen und Verstehen der Aufgabenstellung viel Zeit, ansonsten verlieren Sie unnötig viele Punkte.

Bewertungshinweis:

- Es gibt maximal vier Punkte pro Teilaufgabe.
- Wenn Sie mehr als drei Kreuze pro Teilaufgabe ankreuzen, erhalten Sie keine Punkte.
- Haben Sie ein Kreuz in einer Teilaufgabe falsch gesetzt, erhalten Sie die halbe Punktzahl.
- Haben Sie mehr als ein Kreuz in einer Teilaufgabe falsch gesetzt, erhalten Sie keine Punkte.

(1.1) (4 Punkte) Kreuzen Sie die drei richtigen Antworten an:

- [x] Auf der Menge $M := \{1, 2, 3\}$ gibt es $2^3 = 8$ Relationen.
- [ ] Es gibt keine Relation, die asymmetrisch aber nicht antisymmetrisch ist.
- [x] Eine transitive und symmetrische Relation ist immer reflexiv.
- [ ] Die Vereinigung zweier asymmetrischer Relationen ist wieder asymmetrisch.
- [ ] Eine Ordnungsrelation auf einer nichtleeren Menge kann nie irreflexiv sein.
- [x] Es gibt Äquivalenzrelationen, die gleichzeitig Ordnungsrelationen sind.

2

(1.2) (4 Punkte) Kreuzen Sie die drei richtigen Antworten an:

- [ ] $(\mathbb{N}_0, +)$ erfüllt nicht den Eindeutigkeitssatz.
- [ ] $(\mathbb{N}_0, +)$ erfüllt nicht den Existenzsatz.
- [x] Es sei $(G, \circ)$ eine endliche Gruppe. Dann gilt $x \circ y = y \circ x$ für alle $x, y \in G$.
- [ ] Es sei $(G, \circ)$ eine Gruppe mit neutralem Element e. Sind $a, b \in G$ mit $a \circ b = a$, so folgt $b = e$.
- [ ] $(\mathbb{Z}_5, \otimes)$ ist keine Gruppe.
- [ ] $(\mathbb{Z}_n, \oplus)$ ist nur dann eine Gruppe, wenn n eine Primzahl ist.

Aufgabe 2 (8 Punkte)

Prüfen Sie für die folgenden Relationen R auf $M := \{1, 2, 3, 4\}$ jeweils, ob es eine Ordnungsrelation S gibt, die R umfasst. Falls ja, geben Sie die (bzgl. der Teilmengenordnung) kleinste solche Ordnungsrelation an.

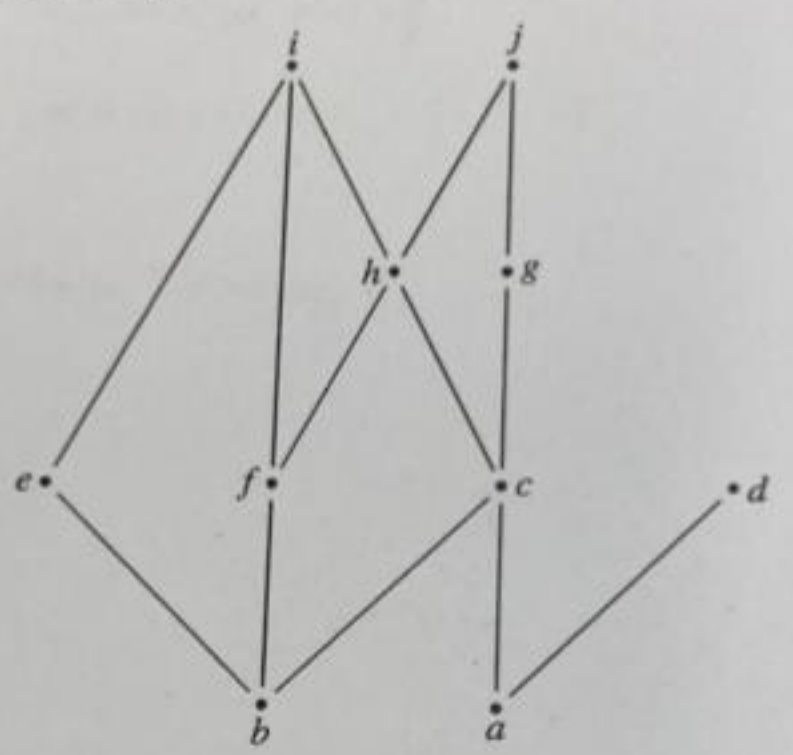
(2.1) $R := \{(1, 2), (2, 3), (3, 2)\}$

(2.2) $R := \{(1, 2), (2, 3), (3, 1)\}$

(2.3) $R := \{(1, 2), (3, 1)\}$

Aufgabe 3 (18 Punkte)

(3.1) (10 Punkte) Gegeben sei das folgende Hasse-Diagramm der zehn-elementigen Menge $M := \{a, b, c, d, e, f, g, h, i, j\}$:



Geben Sie größte/ kleinste und maximale/ minimale Elemente sowie obere/ untere Scharanken, obere/ untere Grenzen und Supremum/ Infimum von $\{c, g, h\}$ und $\{a, b, f\}$ an, falls existent.

	$\{c, g, h\}$	$\{a, b, f\}$		$\{c, g, h\}$	$\{a, b, f\}$
größte Elemente			kleinste Elemente		
maximale Elemente			minimale Elemente		
obere Schranken			untere Schranken		
obere Grenzen			untere Grenzen		
Supremum			Infimum		

(3.2) (8 Punkte) Es sei $\sqsubseteq$ eine Ordnungsrelation auf der Menge M und $A \subseteq M$. Zeigen Sie: Jedes kleinste Element von A ist auch minimales Element von A.

Aufgabe 4 (20 Punkte)

(4.1) (3 Punkte) Notieren Sie die Definition einer Äquivalenzrelation $\equiv$ auf einer Menge M mithilfe von Quantoren.

Nun sei X eine Menge und $M := P(X) = \{A \mid A \subseteq X\}$ die Potenzmenge von X. Für alle $A, B \in M$ definiere

$$A \equiv B :\Leftrightarrow \textit{Es gibt eine bijektive Abbildung } f : A \to B.$$

Hinweis: Eine Abbildung $f : A \to B$ ist bijektiv, wenn f injektiv und surjektiv ist, bzw. wenn f als Relation rechts- und linkseindeutig und rechts- und linkstotal ist.

(4.2) (8 Punkte) Zeigen Sie, dass $\equiv$ eine Äquivalenzrelation auf M ist.

Ab jetzt sei $X := \{1, 2, 3\}$.

(4.3) (2 Punkte) Zeigen Sie $\{1\} \equiv \{2\}$ und $\{1, 2\} \equiv \{2, 3\}$, indem Sie (explizit oder mit Pfeildiagramm) Bijektionen zwischen den jeweiligen Mengen angeben.

(4.4) (4 Punkte) Geben Sie die Äquivalenzklassen $[\{1\}]_{\equiv}$ und $[\{2, 3\}]_{\equiv}$ explizit an.

(4.5) (3 Punkte) Zeigen Sie, dass $[A]_{\equiv} \oplus [B]_{\equiv} := [A \cup B]_{\equiv}$ für $A, B \in M$ nicht wohldefiniert bzw. nicht unabhängig vom Repräsentaten ist.

Hinweis: Nutzen Sie dazu die Äquivalenzklassen $[\{1\}]_{\equiv}$ und $[\{2\}]_{\equiv}$.

Brzezinski, Christiansen,
Ullmann, Zimmermann

30. September 2019

Aufgabe 6 (6 Punkte)

Geben Sie an, ob folgende Aussagen wahr oder falsch sind.

Hinweis: Inkorrekte Antworten führen nicht zu Abzügen. Punkte werden ab vier korrekten Antworten vergeben.

	Aussage	wahr	falsch
1.	Das Schutzziel „Vertraulichkeit" besagt, dass die Nachricht nicht unbemerkt verändert werden kann		
2.	Bei asymmetrischen Verschlüsselungsverfahren kann der Sender die von ihm verschlüsselte Nachricht auch wieder entschlüsseln.		
3.	Das Kerckhoffs'sche Prinzip besagt, dass die Sicherheit des Verschlüsselungsverfahrens nicht von der Geheimhaltung des Schlüssels abhängen darf.		
4.	Permutations-Chiffren sind bei einer sehr großen Schlüsselmenge nicht anfällig gegenüber Häufigkeitsanalysen.		
5.	Bei asymmetrischen Verschlüsselungsverfahren werden insgesamt doppelt so viele Schlüssel benötigt wie bei symmetrischen Verfahren.		
6.	Das Ergebnis des Miller-Rabin-Tests lautet entweder „n ist eine Primzahl" oder „n ist wahrscheinlich keine Primzahl".		

Aufgabe 7 (6 Punkte)

(7.1) (3 Punkte) Geben Sie für $n = 625$ und $n = 360$ jeweils die Anzahl der teilerfremden natürlichen Zahlen kleiner als n an. Geben Sie die Zwischenschritte Ihrer Berechnung an.

(7.2) (3 Punkte) Es wurde das Caesar-Chiffre-Verfahren verwendet um den Klartext

GESCHAFFT

zu verschlüsseln. Welche der folgenden Geheimtexte kann dabei entstehen und geben Sie ggf. den Schlüssel dazu an. Begründen Sie Ihre Antwort.

IGUEJCHHV, HGTDIBGGU, USGQVOTHH.

Aufgabe 8 (13 Punkte)

Für das RSA-Verfahren werden folgende Werte gewählt: $p = 17$, $q = 19$ und $e = 11$.
Geben Sie in den folgenden Teilaufgaben stets einen nachvollziehbaren Rechenweg an:

(8.1) (6 Punkte) Bestimmen Sie den öffentlichen und den privaten Schlüssel.

(8.2) (2 Punkte) Verschlüsseln Sie die Nachricht $m = 38$.

(8.3) (5 Punkte) Entschlüsseln Sie die Nachricht $c = 21$ mithilfe des Square-and-Multiply-Algorithmus.