

Übung Diskrete Strukturen

Einführungsveranstaltung

WS 2018/19

Prof. Stefan Lucks, Nathalie Jolanthe Dittrich
<first>.<middle>.<lastname>(at)uni-weimar.de

Bauhaus-Universität Weimar

October 15, 2018

Willkommen zur Übung der Vorlesung **Diskrete Strukturen!**

Mein Name ist Nathalie und ihr
findet mich hier: B11 R217

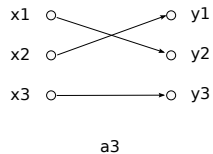
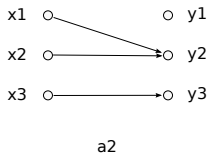
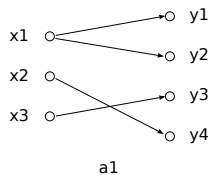


Allgemein:

- Diskrete Strukturen = Fundamentale Aspekte der Zahlen- und Wahrscheinlichkeitstheorie
- In der Kryptographie unverzichtbar:
Alle Kurse unseres Lehrstuhls bauen auf den hier vermittelten Grundlagen auf
- Schulung Ihres abstrakten Denk- und Schlussfolgerungsvermögens

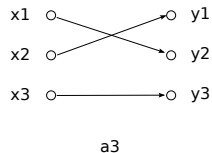
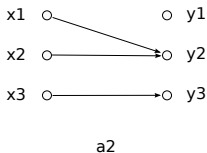
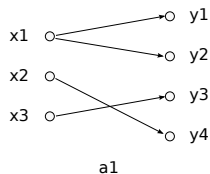
Relevanz-Beispiel

Funktion vs. Permutation



Relevanz-Beispiel

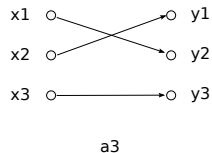
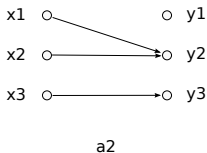
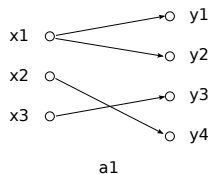
Funktion vs. Permutation



- Funktionen $F : \mathcal{X} \rightarrow \mathcal{Y}$ = deterministische Abbildungen von Eingaben $x \in \mathcal{X}$ auf Ausgaben $y \in \mathcal{Y}$

Relevanz-Beispiel

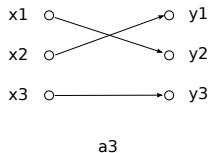
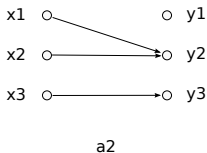
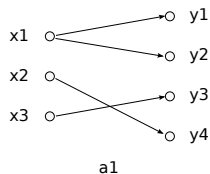
Funktion vs. Permutation



- Funktionen $F : \mathcal{X} \rightarrow \mathcal{Y}$ = deterministische Abbildungen von Eingaben $x \in \mathcal{X}$ auf Ausgaben $y \in \mathcal{Y}$
- Funktionen sind nicht notwendigerweise eindeutig umkehrbar

Relevanz-Beispiel

Funktion vs. Permutation



- Funktionen $F : \mathcal{X} \rightarrow \mathcal{Y}$ = deterministische Abbildungen von Eingaben $x \in \mathcal{X}$ auf Ausgaben $y \in \mathcal{Y}$
- Funktionen sind nicht notwendigerweise eindeutig umkehrbar
- Permutationen sind invertierbare Funktionen:
Aus einer Verschlüsselung $y = F(x)$ kann der Klartext x eindeutig wieder entschlüsselt werden durch $x = F^{-1}(y)$

- Voraussichtlich 7 Übungsblätter
- 14-Tage-Intervall (abwechselnd mit Tutorium)
- Das aktuelle ist spätestens 1-2 Tage nach der vorherigen Übung zu finden auf:

<https://www.uni-weimar.de/de/medien/professuren/medieninformatik/mediensicherheit/teaching/ws-2018/diskrete-strukturen-uebung/>

- Hinweise zur Bearbeitung auch nochmal auf der Webseite und auf den Blättern
 - Alle Gruppenmitglieder die daran gearbeitet haben müssen erwähnt werden
 - Abgabetermin (strikt) vor der Übung die das Blatt bespricht (per E-Mail 15:15 Uhr oder auf Papier im Fach/vor der Übung)

Motivation der Übung

- Sie lernen weniger wenn Sie die Übungsaufgaben nicht bearbeiten
- Darum: Pflicht zur Erstzulassung zur Klausur
- Bilden Sie Gruppen von 2-3 Studenten

Zulassung:

- Lösen Sie alle n Übungsblätter mit $\geq 25\%$ oder
- Lösen Sie $n - 1$ Übungsblätter mit $\geq 25\%$ und ≥ 2 mit $\geq 50\%$

Wie lernt man?

- Die Veranstaltung ist nicht einfach
- Arbeiten Sie die Vorlesungsinhalte regelmäßig nach (am Besten zeitnah nach den Vorlesungen)
- Bilden Sie Übungsgruppen von 2-3 Studenten und treffen Sie sich zur Bearbeitung
- Bilden Sie Lerngruppen
- Fragen Sie rechtzeitig (erst in Gruppen, dann die Tutoren, dann den Dozenten) was Sie nicht verstanden haben
- Bearbeiten Sie die Aufgaben des Handouts (auch auf der Übungsseite)

- Ihre Dozenten und Tutoren sind auch nur Menschen
- Wenn Sie Fehler entdecken sollten oder eine Aufgabe nicht verstanden haben, auch nachdem
 - Sie können uns gerne darauf hinweisen
 - Wir werden versuchen Unklarheiten zu beseitigen, gerne auch per Mail
- Was wir voraussetzen:
 - Dass Sie Fragen selbständig zu klären versuchen
 - Dass Sie bestehende Fragen auch in Ihrer Gruppe und mit Mitstudenten selbständig zu klären versuchen
 - Dass Sie Ihre Lösungen pünktlich abgeben
 - Dass Sie Ihre Lösungen nachvollziehbar aufschreiben
 - Dass Sie Ihre Lösungen in ordentlicher Form aufbereiten (Keine Bleistiftabgaben, keine Kaffeeflecken, keine Hamsterbisse etc.)
 - Dass Sie fair selbständig arbeiten und lernen und NICHT plagieren

Bei guter Bearbeitung der Übungen durch das gesamte Semester können Sie sich einen Bonus auf Ihre Prüfungsnote erarbeiten.

Voraussetzung:

- Bestandene Klausur

1/3 Notenbonus:

- Alle n Übungsblätter mit $\geq 25\%$ der Punkte gelöst **UND**
 ≥ 3 Übungsblätter mit $\geq 50\%$ der Punkte gelöst

2/3 Notenbonus:

- Alle n Übungsblätter mit $\geq 25\%$ der Punkte gelöst **UND**
 $\geq n - 1$ Übungsblätter mit $\geq 50\%$ der Punkte gelöst

1. Übungsblatt und weiterer Verlauf

Inhalte:

- Grundlagen aus dem Handout
- Induktive Beweise und Fallbetrachtungen

Nächste Termine?

Fragen?