Kryptologie

Prof. Dr. Christoph Krauß

SS 2020

h_da

HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

fbi

FACHBEREICH INFORMATIK

Organisation

Kontakt

- Name — Prof. Dr. Christoph Krauß
- Fachgebiete — Netzwerksicherheit
Grundlagen der Informatik
- E-Mail — christoph.krauss@h-da.de
- Büro — Gebäude D 19, Raum 03.07
- Sprechstunde — per Jitsi-Konferenz (Terminvereinbarung per Email)
- Weitere Tätigkeit — Fraunhofer-Institut SIT
Abteilungsleiter Cyber-Physical Systems Security

Fraunhofer SIT

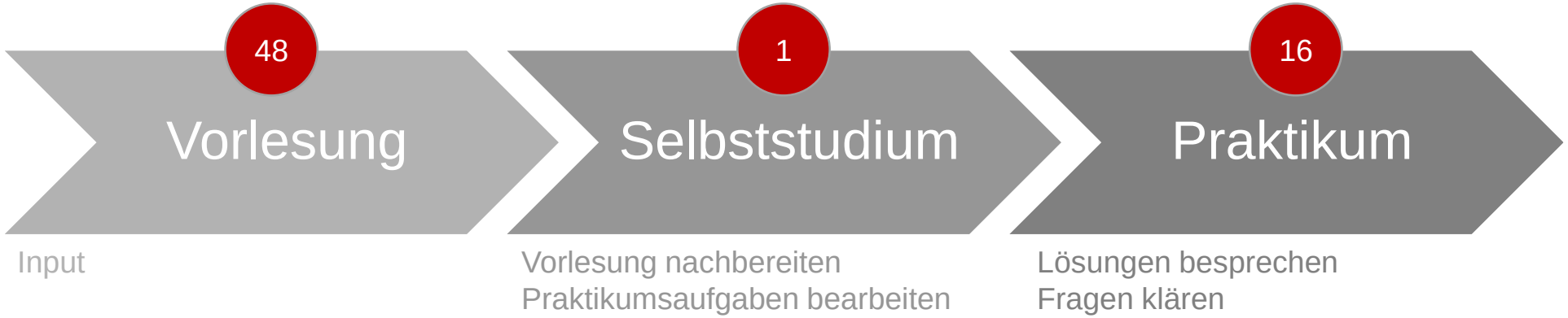
- Rheinstr. 75
  64295 Darmstadt
- Mitarbeiter: ca. 180
- Themen
  - IT-Sicherheitstests
  - Netzwerksicherheit
  - Embedded Security
  - Automotive Security
  - Industrie 4.0
  - …
- Angebote
  - Hiwi-Tätigkeiten, Mitarbeit in Forschungsprojekten
  - Studentische Abschlussarbeiten
  - Partnerunternehmen im kooperativen Studiengang

Organisatorisches

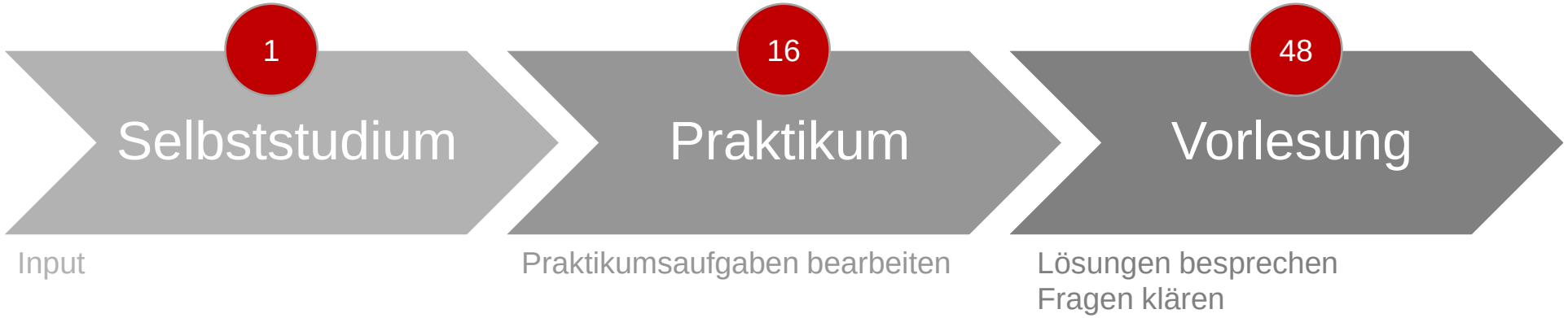
- Vorlesung 3 SWS, Praktikum 1 SWS, 5 CP
- Präsenzfreies Semester
  - Nutzung der **Corona eLearning Infrastruktur**
    - Jitsi (für kleine Gruppen): https://meet.fbi.h-da.de/
    - BigBlueButton (für große Gruppen): https://rooms.fbi.h-da.de/
    - Adobe Connect (für große Gruppen): Backup-Lösung
    - Moodle (Materialen, Diskussionsforum): https://lernen.h-da.de/course/view.php?id=10694
  - Ansatz: Präsenzfreier **Inverted Classroom / Flipped Classroom**
    - Unterrichtsmethode angepasst an das präsenzfreie Semester
    - Details s. nachfolgende Folien
- Alle **Materialen zur Veranstaltung**
  - Moodle: https://lernen.h-da.de/course/view.php?id=10694
  - Einschreibeschlüssel: DsPsswort4KryptohtkeinA.
- Prüfungsleistung: Klausur
- Prüfungsvorleistung: erfolgreiche Teilnahme am Praktikum

„Klassische“ Vorlesung vs. Inverted Classroom

- “Klassische Vorlesung”



- Inverted Classroom



Präsenzfreier Inverted Classroom für Kryptologie

- Grundsätzlicher Ablauf

Selbststudium	Online Lerngruppe	Plenum	Online Lerngruppe
Input • Lehrbuchkapitel • Vorlesungsvideos • Praktikumsaufgaben	Praktikumsaufgaben bearbeiten	Lösungen besprechen Fragen klären	Praktikumsaufgaben überbearbeiten und abgeben

- Tools

Selbststudium	Online Lerngruppe	Plenum	Online Lerngruppe
• Moodle • YouTube • Google	• Jitsi • E-Mail • Moodle-Forum	• BigBlueButton • (Adobe Connect)	• Jitsi • E-Mail • Moodle (Abgabe)

Zeitlicher Ablauf und Tools

Freitag

- Freischaltung Lehrmaterialen
- Moodle

Donnerstag

- Plenum
- BigBlueButton

Freitag

- Abgabe Praktikum
- Moodle

Hinweis: Lehrmaterialen werden ggf. auch früher freigeschaltet

Informationen zum Plenum

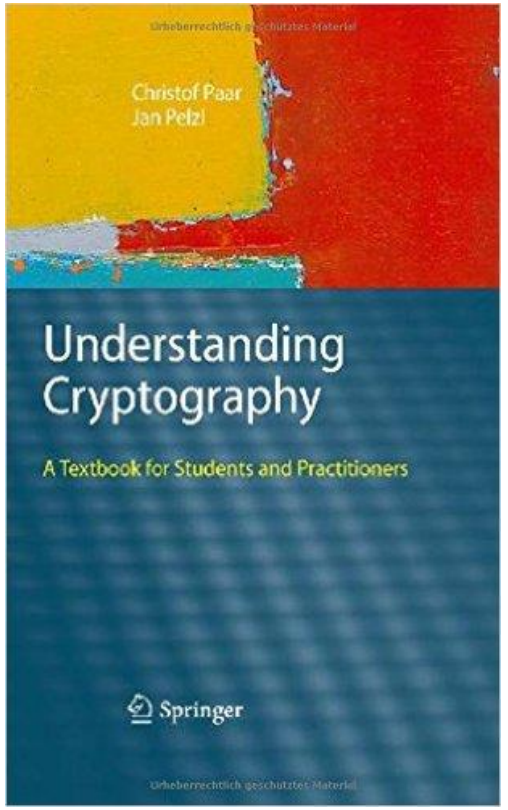
- Grundsätzliches
  - Keine Vorlesung
  - Keine Wiederholung von Inhalten
  - Beantwortung von offenen Fragen zum Lehrbuch, zu den Vorlesungsvideos und zum Praktikum
  - Teilnahme nur sinnvoll, wenn man sich vorbereitet hat
- Termine
  - Do1 08:30 – 10:00 Uhr, BigBlueButton D14/01.03
  - Do2x 10:15 – 11:45 Uhr, BigBlueButton D14/01.03 (14-tägig)
- Virtueller Raum
  - BigBlueButton D14/01.03: https://rooms.fbi.h-da.de/r/D14/01.03

Informationen zum Praktikum

- Grundsätzliches
  - Es ist kein expliziter Termin für das Praktikum geplant
  - Fragen zum Praktikum werden im Plenum besprochen
  - Anstatt alle zwei Wochen ein Praktikum mit vielen Aufgaben gibt es jede Woche kleinere Praktika zum jeweiligen Thema
- Praktikumsaufgaben
  - Werden spätestens Freitags veröffentlicht
  - Sollen in Gruppen von *4 Studierenden* bearbeitet werden
  - Unterteilt in *Training Exercises* und *Exercises for Review*
  - Abgabe nur der *Exercises for Review* notwendig
    - Abgabe am Freitag nach dem Plenum bis spätestens 23:55 Uhr (s. auch Aufgabenblatt)
    - Eine Abgabe für die gesamte Gruppe über Moodle
- Unbenotete Prüfungsvorleistung
  - Bei jedem Praktikum müssen die *Exercises for Review* abgegeben werden
  - Bei jeder Abgabe müssen mindestens 50% korrekt bearbeitet werden

Lehrmaterialen

- Lehrbuch
  - Christof Paar, Jan Pelzl: **Understanding Cryptography**
    A Textbook for Students and Practitioners, Springer, 2010
    - https://link.springer.com/book/10.1007/978-3-642-04101-3
  - Als eBook über Shibboleth an der HDA verfügbar
    - https://link.springer.com/athens-shibboleth-login
  - Errata
    - http://wiki.crypto.rub.de/Buch/download/Errata.pdf
  - Webseite der Autoren
    - http://www.crypto-textbook.com/
  - Deutsche Version des Buchs
    - Christof Paar, Jan Pelzl: **Kryptografie verständlich**
      Ein Lehrbuch für Studierende und Anwender, Springer, 2016
    - Veranstaltung basiert auf dem englischsprachigen Buch



- Ausgewählte Videos zur Vorlesung **Introduction to Cryptography** von Christof Paar
  - https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNuQg/videos

Ziele der Vorlesung

- Kennlernen ausgewählter kryptographischer Verfahren
- Verständnis von Prinzipien zum Entwurf kryptographischer Verfahren
- Fähigkeit zur Analyse kryptographische Verfahren in Bezug auf ihre Sicherheit
- Kennenlernen ausgewählter kryptoanalytischer Methoden und Fähigkeit diese anwenden zu können
- Fähigkeit kryptographische Verfahren für unterschiedliche Schutzziele auswählen und einsetzen zu können
- …

Inhalte

- Einführung
- Stromchiffren und Blockchiffren
- DES
- AES
- Blockchiffremodi
- Public Key Kryptographie
- RSA
- Elliptic Curve Kryptographie
- Digitale Signaturen
- Hash Funktionen
- MACs
- Schlüsselvereinbarung