

Einführung in die Kryptographie



TECHNISCHE
UNIVERSITÄT
DARMSTADT



0011011100010111 **Cryptoplexity**

Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Wintersemester 2014/15

Marc Fischlin

Team

Dozent: Marc Fischlin

Assistenz: Victoria Fehr

Tutorien: 6 Gruppen

(ab nächste Woche)

3 Sprechstunden pro Woche

(Diskussionsforum D120)

Homepage www.cryptoplexity.de

Fachprüfung (hier: Klausur)

- Do, 12. Februar 2015, 17:00h-19:00h
- S1|01, A1 („Audimax“)
- Hilfsmittel:
1 DIN-A4-Blatt, handgeschrieben,
beidseitig (oder zwei Blätter einseitig) beschrieben,
keine elektronischen Hilfsmittel
- Inhaltlich: gesamte Veranstaltung

Übungen

- neue Übung in der Regel Freitags nachmittags
- Besprechung der Präsenz-Übung in der entsprechenden Woche
- plus freiwillige Hausübungen
(ohne Korrektur und ohne Wertung)

Ferienübung

- vorlesungsbegleitenden Leistung: „Ferienübung“
- Ausgabe:
spätestens Fr, 19.Dezember 2014, 12:00h, per Homepage
- Abgabe:
 - in Übungen, Mo-Do, 12.-15.Januar 2015
 - oder bis Do, 15.Januar 2015, 16:15h, in S4|14, 3.1.02

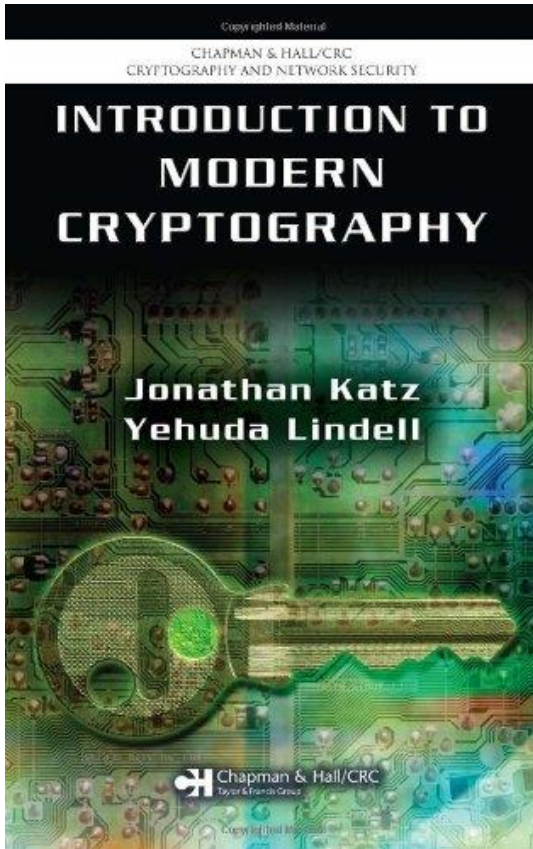
Bonussystem

- maximal 10 Bonuspunkte durch Ferienübung
- Umrechnung Bonuspunkte B in Klausurpunkte K
- bestenfalls Verbesserung um eine Notenstufe (bis zu 0,4)
(Beispiel: 3,3→3,0 oder 2,7→2,3)
- kein „Bestehen dank Bonus“:
Bonus wird nur angerechnet, wenn Fachprüfung ohne Bonus bestanden
- Bonus nicht über Semester hinaus übertragbar
insbesondere auch keine Anrechnung alter Boni

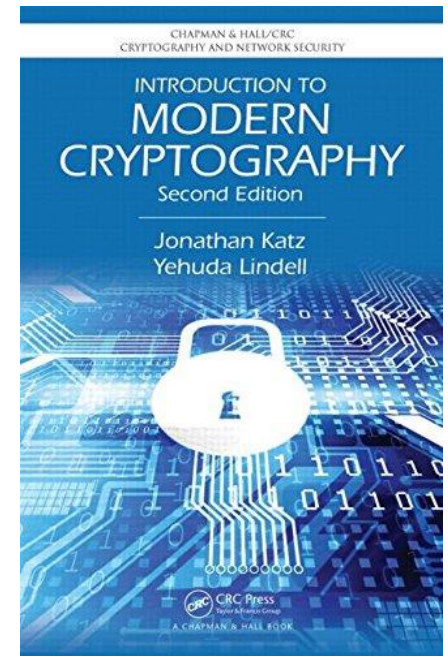
Wen fragen?

- Inhaltliche Angelegenheiten:
Tutoren, (D120-)Foren, Victoria Fehr, Marc Fischlin
- Organisatorische Angelegenheiten TUCaN:
<http://www.info.tucan.tu-darmstadt.de>
- Organisatorische Angelegenheiten Prüfungen:
Ihr Studienbüro
- Organisatorische Angelegenheiten Einführung Krypto:
(D120-)Foren, Victoria Fehr, Marc Fischlin

Literatur (außer Skript + Co)



Introduction to Modern Cryptography,
Katz, Lindell
Chapman & Hall CRC, 2007



2.Auflage ab Dezember 2014