Introduction to Modern Cryptography
E-Learning Course

Stefan Lucks, Eik List, Jakob Wenzel

Bauhaus-Universität Weimar
Chair of Media Security

21 April 2017
Welcome to the E-Learning Course
Introduction to Modern Cryptography!
We give three interesting master courses on advanced topics of cryptography:

- Cryptographic Hash Functions* (Summer Term 2017)
- Secure Channels* (Summer Term 2018)
- Safe and Secure Software (Winter Term 2018/2019)

* = requires successful pass of introduction to cryptography

Students from the Bachelor Medieninformatik have the course Kryptographie und Mediensicherheit

Maybe a problem for beginning master students from other universities

- Not every Bachelor program considers cryptography
- We must offer our Bachelor courses in German
This Course

- Provides an introduction to cryptography for master students from external universities

- Wraps the Stanford online course **Cryptography I** by Prof Boneh
  
  https://www.coursera.org/learn/crypto/
  
  - Should start April 2017
  - Requires (free) registration at the Coursera platform
  - Currently, no active session available, but all videos and talks are on the “Preview” section of the course

- Allows you to learn the foundations of cryptography at your own pace
  - We accompany your learning

- Yields 3 ECTS for the electives module
Course Objectives

You can learn...

- basic cryptographic goals,
- textbook versions of cryptographic algorithms,
- security and adversarial models,
- vulnerabilities of the textbook versions, and
- how to use them securely.
Video lectures in small chunks
Slides
Assignments
Programming assignments
Final exam
Approx. 5-7 hours of work/two weeks
Contents

1. Introduction
2. Stream ciphers
3. Block ciphers
4. Using block ciphers
5. Message integrity
6. Hash functions and collision resistance
7. Authentication and authenticated encryption
8. Odds and Ends: applications (KDF, tweakable encryption, . . .)
9. Basic key exchange
10. Introduction to number theory
11. Public-key encryption from trapdoor permutations
12. Public-key encryption from Diffie-Hellman
Rough Schedule

- We can not control your points at Coursera
- We will add two bigger problem sets (at mid-term and at the end)
  - 40% of the points of each necessary to be admitted to the exam
- Presumably 4 appointments:
  - 21 Apr: Introduction
  - Mid of June: discussing 1st problem set
  - Mid of July: discussing 2nd problem set
  - Before the exams: FAQ session
- Problem sets will be announced when they are published
- Will be returned corrected in the next problem session
- Exam at the end of the term (most probably oral exam)
Organizational – You Can Find

- The slides on the course webpage
  
  http://www.uni-weimar.de/en/media/chairs/media-security/teaching

- The problem sets on the problem-session website

- Slides, videos, and Prof Boneh’s problem sessions also on the coursera site
  
  https://class.coursera.org/crypto
Problem Sets

- Always explain your solutions
- You can work in groups of up to 3 students
- A LaTeX template can be found on the website of the problem session
Participation

- Prepare well and ask questions!
- The problem sets on Coursera and in the course are essential parts of the course
- You will not learn much without careful work on the problem sets

http://simpsons.wikia.com/wiki/Homer_Simpson
Questions?