Introduction to Modern Cryptography

E-Learning Seminar

Stefan Lucks, Eik List

Bauhaus-Universität Weimar

13 Oct 2017

Motivation

Welcome to the E-Learning Course
Introduction to Modern Cryptography!

Motivation

- We give several interesting master courses on advanced topics of cryptography:
  - Cryptographic Hash Functions*
  - Secure Channels*
  - Safe and Secure Software
- They (*) require introduction to cryptography
  - Should be no problem for students from the bachelor at BUW
    $\Longrightarrow$ bachelor courses here
- Maybe problem for beginning master students from other universities
  - Bachelor courses are in German

Motivation

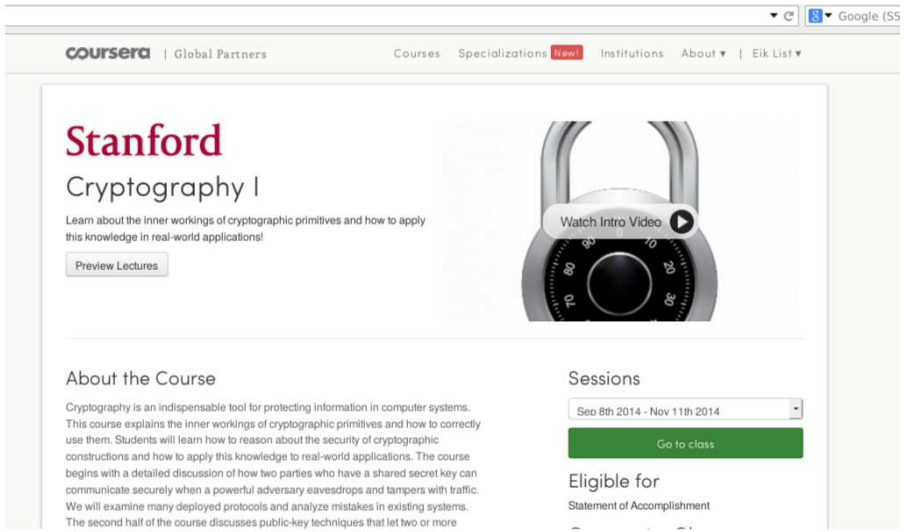
- We give several interesting master courses on advanced topics of cryptography:
  - Cryptographic Hash Functions*
  - Secure Channels*
  - Safe and Secure Software
- They (*) require introduction to cryptography
  - Should be no problem for students from the bachelor at BUW
    $\Longrightarrow$ bachelor courses here
- Maybe problem for beginning master students from other universities
  - Bachelor courses are in German

Motivation

- We give several interesting master courses on advanced topics of cryptography:
  - Cryptographic Hash Functions*
  - Secure Channels*
  - Safe and Secure Software
- They (*) require introduction to cryptography
  - Should be no problem for students from the bachelor at BUW
    $\Longrightarrow$ bachelor courses here
- Maybe problem for beginning master students from other universities
  - Bachelor courses are in German

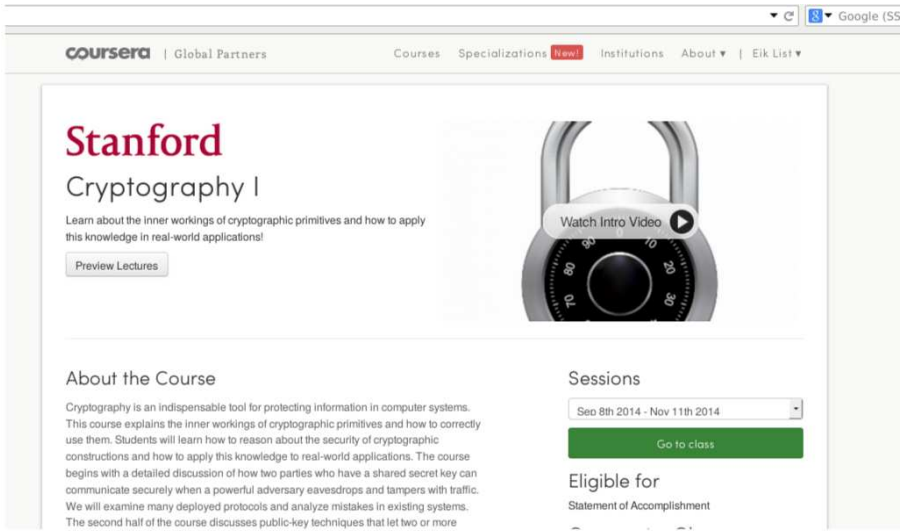
This Course

- Provides an introduction to cryptography for master students from external universities
- Wraps the Stanford course **Crypto I** by Prof Boneh
- We accompany your learning
- 3 ECTS for the electives module



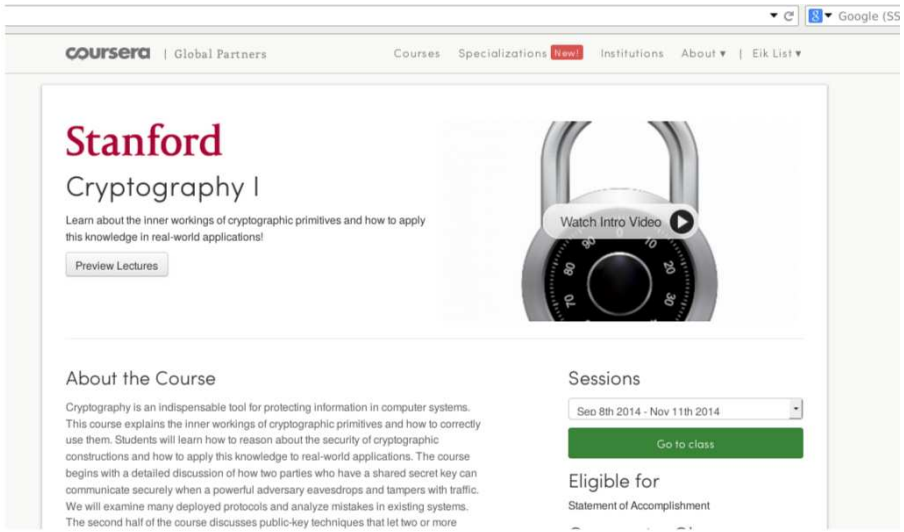
This Course

- Provides an introduction to cryptography for master students from external universities
- Wraps the Stanford course **Crypto I** by Prof Boneh
- We accompany your learning
- 3 ECTS for the electives module



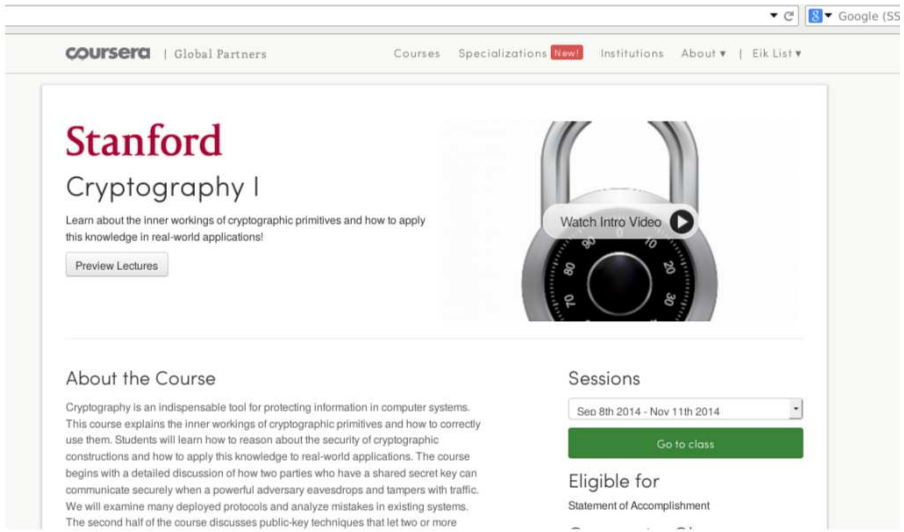
This Course

- Provides an introduction to cryptography for master students from external universities
- Wraps the Stanford course **Crypto I** by Prof Boneh
- We accompany your learning
- 3 ECTS for the electives module



This Course

- Provides an introduction to cryptography for master students from external universities
- Wraps the Stanford course **Crypto I** by Prof Boneh
- We accompany your learning
- 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.

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.

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.

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.

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.

Form

- Video lectures in small chunks
- Slides
- Assignments
- Programming assignments
- Final exam
- Approx. 5-7 hours of work/two weeks

Contents

Contents

Contents

Contents

Contents

Rough Schedule

- 2 problem sets and 2 problem sessions:
  - PS1: Due end of Nov
  - PS2: Due min of Jan
- We do not care about your points at coursera
- We change tasks compared to those on coursera
- First problem set will be published next week.

Rough Schedule

- 2 problem sets and 2 problem sessions:
  - PS1: Due end of Nov
  - PS2: Due min of Jan
- We do not care about your points at coursera
- We change tasks compared to those on coursera
- First problem set will be published next week.

Exam Conditions

- Admission to the exam:
  - 40 % of the points averaged over both problem sets
- Oral exam at the end

Organizational – You Can Find

- The slides on the course web site
- The problem sets on the problem-session web site

  `http://www.uni-weimar.de/en/media/chairs/media-security/teaching`

- Slides, videos, and Prof Boneh's problem sessions also on the coursera site (starts Oct 30)

  `https://www.coursera.org/learn/crypto`

Organizational – You Can Find

- The slides on the course web site
- The problem sets on the problem-session web site

  `http://www.uni-weimar.de/en/media/chairs/media-security/teaching`
- Slides, videos, and Prof Boneh's problem sessions also on the coursera site (starts Oct 30)

  `https://www.coursera.org/learn/crypto`

Participation

- Prepare well and ask questions!
- Problem sessions are an essential part of a course
- You will not learn much without careful work on the problem sets

Questions?