

Introduction to Modern Cryptography

E-Learning Seminar

Stefan Lucks, Eik List

Bauhaus-Universität Weimar

13 Oct 2017

**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
⇒ bachelor courses here
- Maybe problem for beginning master students from other universities
 - Bachelor courses are in German

Motivation

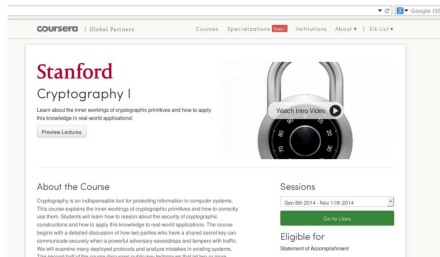
- We give several interesting master courses on advanced topics of cryptography:
 - Cryptographic Hash Functions*
 - Secure Channels*
 - Safe and Secure Software
- They (*) require introduction to cryptography
 - Should be no problem for students from the bachelor at BUW
⇒ bachelor courses here
- Maybe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

This Course

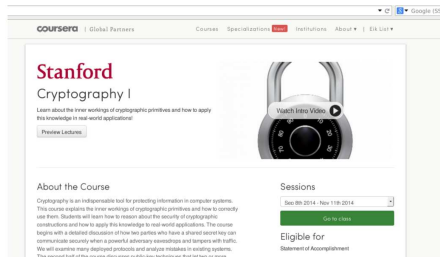
- Provides an introduction to cryptography for master students from external universities
- Wraps the Stanford course **Crypto I** by Prof Boneh
- We accompany your learning
- 3 ECTS for the electives module



The screenshot shows the Coursera course page for 'Stanford Cryptography I'. The page features the Stanford logo and the course title. A video player is visible with a 'Watch Intro Video' button. The 'About the Course' section describes the course as an indispensable tool for protecting information in computer systems. The 'Sessions' section shows the course is available from Sep 8th 2014 to Nov 11th 2014, with a 'Go to class' button. The 'Eligible for' section indicates that students are eligible for a 'Statement of Accomplishment'.

This Course

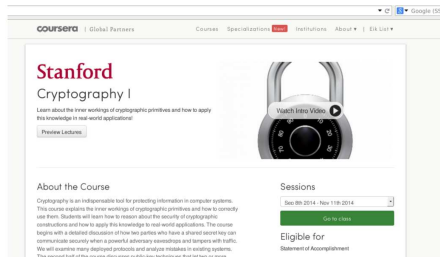
- Provides an introduction to cryptography for master students from external universities
- Wraps the Stanford course **Crypto I** by Prof Boneh
- We accompany your learning
- 3 ECTS for the electives module



The screenshot shows the Coursera course page for 'Stanford Cryptography I'. The page features the Stanford logo and the course title. A video player with a 'Watch Intro Video' button is visible. Below the video, there is a 'Previous Lectures' button. The 'About the Course' section describes the course as an indispensable tool for protecting information in computer systems, covering cryptographic primitives and their real-world applications. The 'Sessions' section shows the course dates as 'Sep 8th 2014 - Nov 11th 2014' and a 'Go to class' button. The 'Eligible for' section includes a 'Statement of Accomplishment' button.

This Course

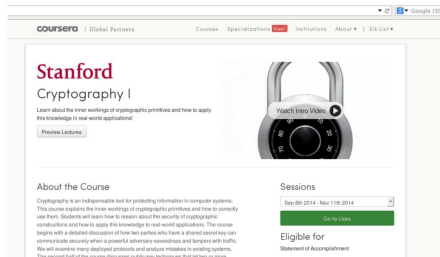
- Provides an introduction to cryptography for master students from external universities
- Wraps the Stanford course **Crypto I** by Prof Boneh
- We accompany your learning
- 3 ECTS for the electives module



The screenshot shows the Coursera course page for 'Stanford Cryptography I'. The page features the Stanford logo, the course title 'Cryptography I', and a 'Watch Intro Video' button. Below the title, there is a 'Previous Lectures' button. The 'About the Course' section describes the course as an indispensable tool for protecting information in computer systems, explaining the inner workings of cryptographic primitives and how to apply this knowledge to real-world applications. The 'Sessions' section shows a dropdown menu for the course dates (Sep 8th 2014 - Nov 11th 2014) and a 'Go to class' button. The 'Eligible for' section includes a 'Statement of Accomplishment' button.

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



The screenshot shows the Coursera course page for 'Stanford Cryptography I'. The page features the Stanford logo and the course title. A video player with a 'Watch Intro Video' button is visible. Below the video, there is a 'Previous Lectures' button. The 'About the Course' section describes the course as an indispensable tool for protecting information in computer systems, covering symmetric and public-key cryptography. The 'Sessions' section shows the course is available from Sep 8th 2014 to Nov 11th 2014, with a 'Go to class' button. The 'Eligible for' section indicates that students can earn a 'Statement of Accomplishment'.

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.

- 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 Integrity
- 6 Hash functions and collision resistance
- 7 Authentication and authenticated encryption
- 8 Applications
- 9 Key exchange
- 10 Number theory
- 11 Public-key trapdoor functions
- 12 Public-key encryption

Contents

- 1 Introduction
- 2 Stream ciphers
- 3 Block ciphers
- 4 Using block ciphers
- 5 Integrity
- 6 Hash functions and collision resistance
- 7 Authentication and authenticated encryption
- 8 Applications
- 9 Key exchange
- 10 Number theory
- 11 Public-key trapdoor functions
- 12 Public-key encryption

Contents

- 1 Introduction
- 2 Stream ciphers
- 3 Block ciphers
- 4 Using block ciphers
- 5 Integrity
- 6 Hash functions and collision resistance
- 7 Authentication and authenticated encryption
- 8 Applications
- 9 Key exchange
- 10 Number theory
- 11 Public-key trapdoor functions
- 12 Public-key encryption

Contents

- 1 Introduction
- 2 Stream ciphers
- 3 Block ciphers
- 4 Using block ciphers
- 5 Integrity
- 6 Hash functions and collision resistance
- 7 Authentication and authenticated encryption
- 8 Applications
- 9 Key exchange
- 10 Number theory
- 11 Public-key trapdoor functions
- 12 Public-key encryption

Contents

- 1 Introduction
- 2 Stream ciphers
- 3 Block ciphers
- 4 Using block ciphers
- 5 Integrity
- 6 Hash functions and collision resistance
- 7 Authentication and authenticated encryption
- 8 Applications
- 9 Key exchange
- 10 Number theory
- 11 Public-key trapdoor functions
- 12 Public-key encryption

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?