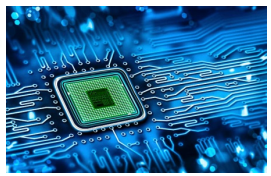
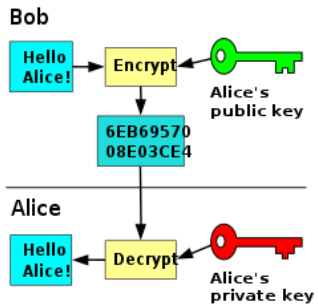
Introduction to "Introduction to Security 2025"

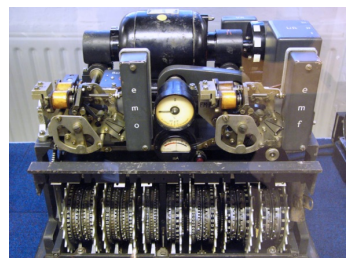
Kostas Papagiannopoulos
University of Amsterdam
k.papagiannopoulos@uva.nl

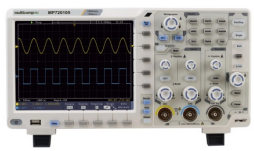
Introduction

- A course that covers the basics of Computer Security – a very fragmented field
- Introduction to . . . *meh*. . .
- We will combine theory with practice, coding assignments and detailed real-world attacks









People

Lecturers:

- Kostas Papagiannopoulos
  k.papagiannopoulos@uva.nl
- Francesco Regazzoni
  f.regazzoni@uva.nl

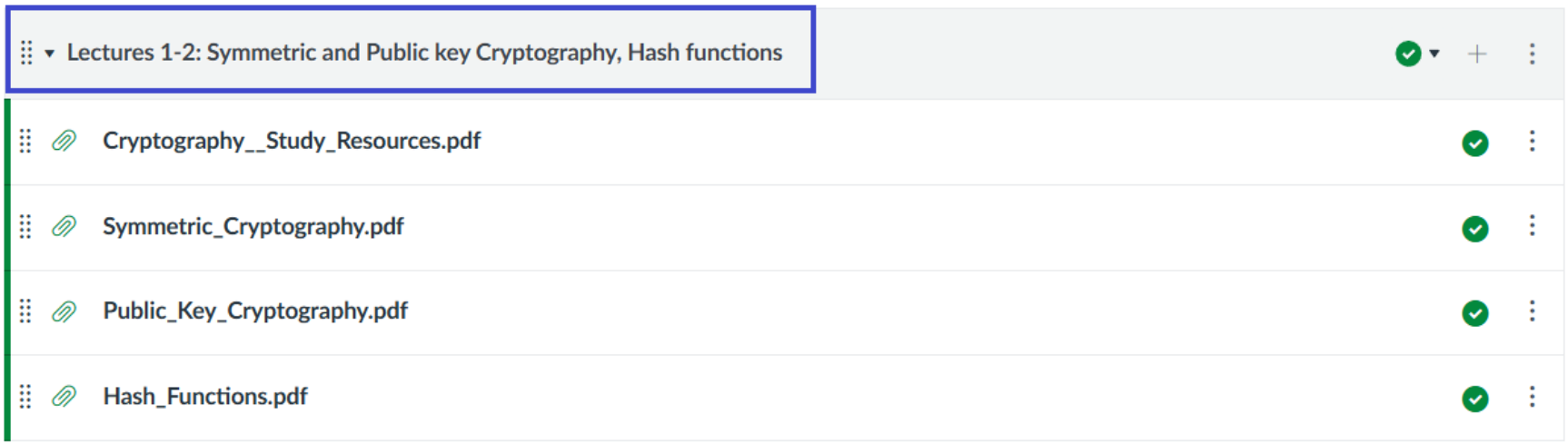
Teaching Assistants:

- Remco Hogerwerf
  remco.hogerwerf@student.uva.nl

Canvas Material

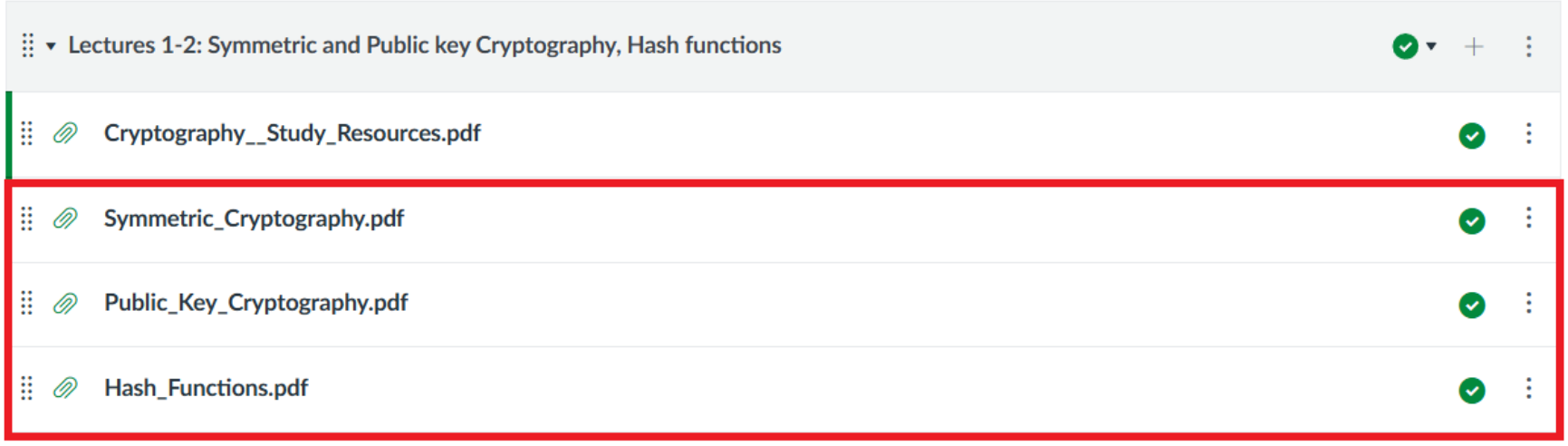
- Canvas module: title

topics of the week



Canvas Material

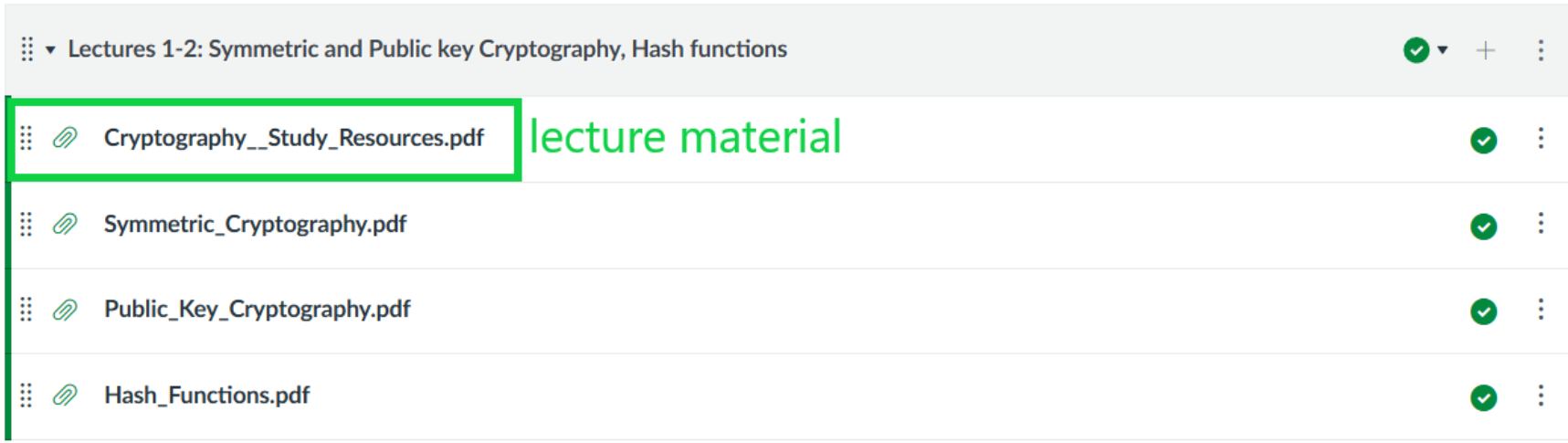
- Canvas module: lecture slides



lecture slides

Canvas Material

- Canvas module: study resources



Canvas Material

- Study resources

Resources on Cryptography

Preparation Lecture 1

- Core principles and algorithms of cryptosystems:
  Information Security: Principles and Practice by M. Stamp
  Chapter 2 on Crypto Basics, chapter 3 on Symmetric Key Crypto
  http://tinyurl.com/y9dkjx76

Literature Lecture 1

- Attacks on the WEP protocol:
  Intercepting Mobile Communications: The Insecurity of 802.11 by N. Borisov et al.
  http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf
  Emphasize on sections 2, 3 and 4.1
- Announcing the Crypto1 hack on the OV-chipkaart:
  Security Flaw in MIFARE Classic by R. Schreur et al.
  https://www.cs.bham.ac.uk//~garciaf/publications/Security_Flaw_in_MIFARE_Classic.pdf

Extras Lecture 1

- Core principles of cryptosystems:
  Handbook of Applied Cryptography, by A. Menezes
  https://cacr.uwaterloo.ca/hac/
- Core principles and algorithms of symmetric cryptosystems:
  Network Security Essentials: Application And Standards by W. Stallings
- Refreshing probability theory

Canvas Material

- Study resources: before the lecture

Resources on Cryptography

Preparation Lecture 1

- Core principles and algorithms of cryptosystems:
  Information Security: Principles and Practice by M. Stamp
  Chapter 2 on Crypto Basics, chapter 3 on Symmetric Key Crypto
  http://tinyurl.com/y9dkjx76

study before the lecture

Literature Lecture 1

- Attacks on the WEP protocol:
  Intercepting Mobile Communications: The Insecurity of 802.11 by N. Borisov et al.
  http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf
  Emphasize on sections 2, 3 and 4.1
- Announcing the Crypto1 hack on the OV-chipkaart:
  Security Flaw in MIFARE Classic by R. Schreur et al.
  https://www.cs.bham.ac.uk//~garciaf/publications/Security_Flaw_in_MIFARE_Classic.pdf

Extras Lecture 1

- Core principles of cryptosystems:
  Handbook of Applied Cryptography, by A. Menezes
  https://cacr.uwaterloo.ca/hac/
- Core principles and algorithms of symmetric cryptosystems:
  Network Security Essentials: Application And Standards by W. Stallings
- Refreshing probability theory

Canvas Material

- Study resources: after the lecture

Resources on Cryptography

Preparation Lecture 1

- Core principles and algorithms of cryptosystems:
  Information Security: Principles and Practice by M. Stamp
  Chapter 2 on Crypto Basics, chapter 3 on Symmetric Key Crypto
  http://tinyurl.com/y9dkjx76

Literature Lecture 1

- Attacks on the WEP protocol:
  Intercepting Mobile Communications: The Insecurity of 802.11 by N. Borisov et al.
  http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf
  Emphasize on sections 2, 3 and 4.1
- Announcing the Crypto1 hack on the OV-chipkaart:
  Security Flaw in MIFARE Classic by R. Schreur et al.
  https://www.cs.bham.ac.uk//~garciaf/publications/Security_Flaw_in_MIFARE_Classic.pdf

study after the lecture

Extras Lecture 1

- Core principles of cryptosystems:
  Handbook of Applied Cryptography, by A. Menezes
  https://cacr.uwaterloo.ca/hac/
- Core principles and algorithms of symmetric cryptosystems:
  Network Security Essentials: Application And Standards by W. Stallings
- Refreshing probability theory

Schedule

Course Schedule: `https://datanose.nl/#course[137658]`

- **Lecture 1** (3 September – Kostas)
  What is cryptography? Symmetric cryptosystems, modes of operation
- **Lecture 2** (5 September – Kostas)
  Asymmetric cryptography and hash functions
- **Assignment 1:** The Padding Oracle Attack on DES CBC
- **Lecture 3** (9 September – Francesco)
  How to implement cryptography? Efficient and protected components in software and hardware – part 1
- **Lecture 4** (10 September – Francesco)
  How to implement cryptography? Efficient and protected components in software and hardware – part 2
- **Assignment 2:** Implementing the AES cipher

Schedule

Course Schedule:

- **Lecture 5** (17 September – Kostas)
  How to break cryptography? Classical and Timing-based cryptanalysis
- **Lecture 6** (19 September – Kostas)
  How to break cryptography? Side-channel and Fault-based cryptanalysis
- **Assignment 3:** Cryptanalysis attacks on symmetric ciphers
- **Lecture 7** (24 September – Kostas)
  Intrusion Detection Systems: Core elements
- **Lecture 8** (26 September – Kostas)
  Intrusion Detection Systems: Algorithms
- **Assignment 4:** Constructing and evaluating Intrusion Detection Systems

Schedule

Course Schedule:

- **Lecture 9** (1 October – Francesco)
  Is my system safe? Virus and OS security

- **Lecture 10** (3 October – Francesco)
  Is my system safe? IoT and CPSs Security

  Assignment 5: Make a short video on system security concepts

- **Lecture 11** (8 October – Kostas)
  User authentication and passwords

- **Lecture 12** (10 October – Kostas)
  User privacy and privacy-enhancing technologies

  Assignment 6: Privacy-enhancing techniques and data analysis

Schedule

Course Schedule:

- **Lecture 13** (15 October – Kostas)
  Protocol & Network Security, introducing the TLS/SSL protocol
- **Lecture 14** (17 October – Kostas)
  Open hour with questions and clarifications

- **Digital Exam** (24 October, 12:30-14:30, World Fashion Center Westhal)
- **Digital Resit Exam** (16 December, 9:30-12:30, NTH A5.01)
- **Exam information:** closed book exam, you can bring an A4 paper with your notes (on both sides)

Assignments and Grading

- To pass the course you have to pass **all** the course assignments
- No individual deadlines for the assignments
- **Hard deadline for all assignments: 17 October 2024**
- You can do the assignments in pairs or alone – if you cannot find a co-worker mail me and we will try to make random pairs for you

- We grade every assignment with **pass** or **fail**
  - If all is correct or if there are minor issues, then **pass**
  - If we detect serious issues then **fail** and you can try again
- We hope this way to deal with unexpected circumstances but also to motivate you towards actual work instead of work-under-pressure

- The course grade is the grade of the final examination

Contact

- Join the Discord server for Q&A
  `https://discord.gg/fzFXjCR7QD`
- Mail questions directly to the lecturers or use Canvas

- Feedback, correction and comments are always highly appreciated – stay communicative!
- Let's try to move towards cooperative learning!