Cryptography

Corso di Laurea Magistrale in Informatica

Master Degree in Artificial Intelligence

Introduction to the Course

Ugo Dal Lago

Academic Year 2024-2025

What?

- The objective of this course is to study **cryptography**, which forms the foundation to **cybersecurity**.

What?

- The objective of this course is to study **cryptography**, which forms the foundation to **cybersecurity**.
- The course is divided into three parts:
  - First of all, we will talk about **modern cryptography**, and this will be the bulk of the curse.
  - Then, we will give some lectures about techniques for the (automatic and semi-automatic) verification of the security of primitives and protocols, that is to say about the so-called **symbolic model**.
  - There will be a couple of lectures, towards the end of the course, in which we will talk about some **advanced topics**.

Modern Cryptography

- This will keep us busy for at least half of the course.
- We will study some definitions and results which allow cryptography to be considered a *science*, as opposed to a form of *art*.
- We will proceed in two phases:
  - First of all, we will formally **define** the desired security properties.
  - We will then **prove** that secure cryptographic constructions are, under certain conditions, possible.
- We will treat this way *private-key encryption*, *public-key encryption*, *authentication*, and (perhaps) *non-repudiation*.
- We will use the following as tools: *pseudorandomness*, *number theory*, and *group theory*.
  - Requirements: **probability theory**, and a little bit of **algorithmics**.

Formal Verification of Security Protocols

- This will keep us busy for at least one fourth of the course.
- The model here is simpler and more abstract than in modern cryptography.
- There are **so many** techniques for formally verifying the security of communication protocols.
  - **Model-checking**.
  - **Interactive Theorem-Proving**.
  - **Abstract Interpretation**.
  - **Logic Programming**.
  - ...
- We will take a look at two concrete tools:
  - **ProVerif**, `http://www.proverif.ens.fr/`
  - **EasyCrypt**, `http://www.easycrypt.info/`

Who?

- This is a course meant to be attended by Master students in Computer Science or Artificial Intelligence.
  - Students attending other courses should check with the teacher.
- The teacher is **Ugo Dal Lago**.
  - Email: `ugo.dallago@unibo.it`
  - Office: **via Mura Anteo Zamboni 7, Bologna**
  - Office hours:
    - By appointment (just send an email to the teacher).
- The very last lectures will be given by Giulio Malavolta, from Bocconi University (to be confirmed).

How?

- The course comprises 40 hours of lectures.
- Weekly Schedule:
  - **Monday**: 11:00-14:00 (E2).
  - **Friday**: 11:00-13:00 (E1).

How?

- The course comprises 40 hours of lectures.
- Weekly Schedule:
  - **Monday**: 11:00-14:00 (E2).
  - **Friday**: 11:00-13:00 (E1).
- Two Ways of Passing the Course:
  - **Homework.**
    - During the course, there will be *three* homework assignments.
    - Each of the assignments consists in three or four exercises, to be solved in 10 to 15 days.
    - The exercises are meant to be solved *individually*.
    - Homeworks will be made available as an assignment in `http://virtuale.unibo.it`.
    - If a student passes the three homeworks, then the only thing remaining is a very short oral exam.
  - **Oral Exam.**
    - It will be relatively long, and it will be about the whole course.

Course Material

- The following textbook covers *all* what we will do in the first part of the course:
  - *J. Katz and Y. Lindell.* **Introduction to Modern Cryptography**. Chapman & Hall, 2007.
- These are other useful references:
  - *D. O Goldreich.* **Foundations of Cryptography I: Basic Tools**. Cambridge University Press, 2001.
  - *D. O Goldreich.* **Foundations of Cryptography II: Basic Applications**. Cambridge University Press, 2004.
  - *D. R. Stinson.* **Cryptography: theory and practice**. Chapman & Hall, Third Edition, 2006.

Course Material

- The following textbook covers *all* what we will do in the first part of the course:
  - *J. Katz and Y. Lindell.* **Introduction to Modern Cryptography**. Chapman & Hall, 2007.
- These are other useful references:
  - *D. O Goldreich.* **Foundations of Cryptography I: Basic Tools**. Cambridge University Press, 2001.
  - *D. O Goldreich.* **Foundations of Cryptography II: Basic Applications**. Cambridge University Press, 2004.
  - *D. R. Stinson.* **Cryptography: theory and practice**. Chapman & Hall, Third Edition, 2006.
- Unfortunately, the second part of the course is not covered by any existing textbook. However, there exist some surveys and lectures notes.

Course Material

- The following textbook covers *all* what we will do in the first part of the course:
  - *J. Katz and Y. Lindell.* **Introduction to Modern Cryptography**. Chapman & Hall, 2007.
- These are other useful references:
  - *D. O Goldreich.* **Foundations of Cryptography I: Basic Tools**. Cambridge University Press, 2001.
  - *D. O Goldreich.* **Foundations of Cryptography II: Basic Applications**. Cambridge University Press, 2004.
  - *D. R. Stinson.* **Cryptography: theory and practice**. Chapman & Hall, Third Edition, 2006.
- Unfortunately, the second part of the course is not covered by any existing textbook. However, there exist some surveys and lectures notes.
- About the third part of this course, some references will be made available later during the course.

Course Material

- The following textbook covers *all* what we will do in the first part of the course:
  - *J. Katz and Y. Lindell.* **Introduction to Modern Cryptography**. Chapman & Hall, 2007.
- These are other useful references:
  - *D. O Goldreich.* **Foundations of Cryptography I: Basic Tools**. Cambridge University Press, 2001.
  - *D. O Goldreich.* **Foundations of Cryptography II: Basic Applications**. Cambridge University Press, 2004.
  - *D. R. Stinson.* **Cryptography: theory and practice**. Chapman & Hall, Third Edition, 2006.
- Unfortunately, the second part of the course is not covered by any existing textbook. However, there exist some surveys and lectures notes.
- About the third part of this course, some references will be made available later during the course.
- All the material for the course, including slides, will be made available on `http://virtuale.unibo.it`.