

Foundations of Cybersecurity

Gianluca Dini

Dept. of Ingegneria dell'Informazione

University of Pisa

gianluca.dini@unipi.it

Version: 2024-02-26

1

Lecturer

- Prof. **Gianluca Dini**
- Dept. of Ingegneria dell'Informazione
 - Largo Lucio Lazzarino, (building A)
 - Office hours: by appointment
- Email:
 - gianluca.dini@unipi.it



feb. '24

Course introduction

2

2

Contents



UNIVERSITÀ DI PISA

- Applied cryptography
 - Learn what “secure” means
 - Learn how crypto-primitives work
 - Learn how to use them correctly and reason on security
 - Authentication and identification protocols
 - Case studies: How to build insecure systems with secure components
 - Programming secure applications (crypto lib for C/C++)
- Handson and challenges

feb. '24

Course introduction

3

3

Prerequisites



UNIVERSITÀ DI PISA

- Computer architectures
- Operating systems
- Computer networks
- Algorithms and data structures
- Complexity and probability theory

feb. '24

Course introduction

4

4

Organization



UNIVERSITÀ DI PISA

- Foundations of Cybersecurity (FoC) is a course of the Master in Computer Engineering (WCN-LM)
 - 9 CFU, 90 hours
- FoC is shared with the Master in Artificial Intelligence and Data Engineering (WAI-LM) and with the Master in Cybersecurity (WCY-LM)

feb. '24

Course introduction

5

5

Time table



UNIVERSITÀ DI PISA

- Mon 14:30 – 17:30, A12
- Wed 10:30 – 13:30, A12
- Thu 10:30 – 12:30, A12

26 February, 2024

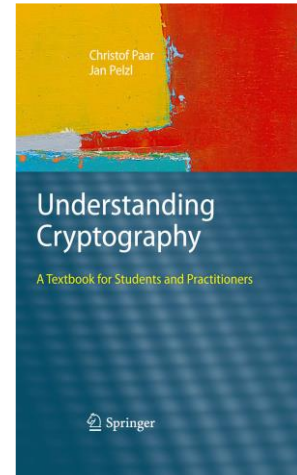
Course introduction

6

6

Textbooks

- C.Paar, J.Pelzl. *Understanding Cryptography – Testbook for Students and Pratictioners.* Springer



feb. '24

Course introduction

7

7

Other teaching material



UNIVERSITÀ DI PISA

- Handouts
 - Last year slides can be found [HERE](#)
- Recordings
 - 2021-22 recordings can be found [HERE](#)
- Reader
 - Papers, Standards, White papers, ...

feb. '24

Course introduction

8

8

Communications



UNIVERSITÀ DI PISA

- Microsoft Team:
 - [880II 23/24 - FOUNDATIONS OF CYBERSECURITY \[WCN-LM\]](#)
 - Communications (Generale/Post)
 - Material (Generale/File)
- Email (filter safe)
 - Subject: [FoC] <the subject>

feb. '24

Course introduction

10

10

Final Exam



UNIVERSITÀ DI PISA

- Project
 - 1-2 people per group
 - Assigned at ~May
 - *Conditio sine qua non* for the rest
- Written-part
 - Closed-book, closed-notes
- Oral-part

feb. '24

Course introduction

11

11

26 February, 2024

Course introduction

12