Cryptography and Security

Cunsheng DING

HKUST, Hong Kong

Version 3

Information about the instructor

- Dr. Cunsheng DING
- Office: Room 2533
- Email: cding@ust.hk
- https://www.cse.ust.hk/faculty/cding/

- Office hours: Please send an email for appointment.

Textbook and Lecture Notes

Textbook: W. Stallings, Cryptography and Network Security, Seventh Edition, Pearson, 2017.

Reference books: We recommend the following.

1. D. Stinson, Cryptography: Theory and Practice, CRC Press, 1995.
2. A. Salomaa, Public-Key Cryptography, second Edition, Springer-Verlag, 1992.

Level of Presentation and Contents

Background: Ph.D, M.Phil, top UGs, and some exchange students.

Presentation: With the assumption that all students have the basic knowledge of functions, elementary number theory, and computer networks.

Contents: Cryptography, distributed systems security, network security, and Web security.

The Required Basic Knowledge of Mathematics

- Functions:
  https://www.cse.ust.hk/faculty/cding/COMP2711H/SLIDES/functions.pdf
- Modular arithmetic:
  https://www.cse.ust.hk/faculty/cding/COMP2711H/SLIDES/modulon.pdf
- Number theory: Part I:
  https://www.cse.ust.hk/faculty/cding/COMP2711H/SLIDES/elemnumb1.pdf
- Number theory: Part II:
  https://www.cse.ust.hk/faculty/cding/COMP2711H/SLIDES/elemnumb2.pdf
- Groups, rings and fields:
  https://www.cse.ust.hk/faculty/cding/COMP2711H/SLIDES/groupring.pdf

Related materials can be found in the 2nd-year undergraduate course web page:
https://www.cse.ust.hk/faculty/cding/COMP2711H/slides.html

Course Grading

- Lecture attendance 6%
- Four assignments 44%
- Final exam (50%)

Learning Outcomes

On completion of this course, you will be able to:

- evaluate potential vulnerabilities and attacks on computer and communication systems;
- learn certain basic security tools;
- select and apply basic security tools to build security systems; and
- get familiar with real-world security systems.

Other Issues

- There are other reading materials on the course website. I will remind you of them at due time.
- Online demos of some cryptosystems are available on the course website and my lecture slides.
- If you are weak in mathematics, you may have difficulty to handle this course.
- My lecture slides are for presentation only and **must** be brief. They are not designed for self-learning.

  If you miss or skip some lectures, you may have to read the corresponding parts in the textbook.