Cryptography

Cunsheng DING

HKUST, Hong Kong

COMP3631

Information about the Instructor

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

Textbook and Reference Books

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, 1996.

Information on This Course

Prerequisite: COMP2711 or COMP2711H (Discrete Mathematics) or a similar course.

Course topics: mathematical foundations of cryptography, private-key and public-key ciphers, public key infrastructure, key management, digital signature schemes, authentication protocols, hash functions, keyed hash functions, security services, security tools, cryptographic protocols, cryptographic primitives, secret sharing.

Remark: This course is the foundation of cybersecurity and computer 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

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

Who Can/Cannot Take This Course?

Any year-2 or year-3 or year-4 student from any program or joint program offered by all schools of a university can take this course as long as the student meets the following conditions:

- The student has taken COMP2711 or COMP2711H (Discrete Mathematics) or a similar mathematics course.
- The student has good capability in mathematics (specifically, her/his grade for COMP2711 is at least C+).

Warnings: Those without reasonable capability in mathematics **cannot** take this course.

If you plan to skip live lectures, you may have difficulty to handle this course.

Course Grading

- Lecture attendance 4%
- Four assignments 56%
- Final exam 40%
  - It will be an open-book exam.
  - It does not have multiple choice questions.
  - It covers the contents of all the lectures.
  - The date and venue of the exam will be informed by the university.

Remark: This course does not have a midterm quiz and midterm exam.

Remark: The course grading is not curve-based, but outcome-based (standards-based).

Learning Outcomes

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

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

Saturday Zoom Q&A Sessions

This course does not have formal tutorials. Instead, Zoom Q&A sessions will be provided.

From 10:30am to 11:20am on Saturday a Zoom Q&A session will be conducted.

- These Q&A sessions are not compulsory for students.
- If a student has questions about any past lecture, she/he may come to a Zoom Q&A session for clarification.
- Zoom Q&A sessions can be accessed via Canvas.

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. You are encouraged to play them.
- My lecture slides are for lecture presentation only and **must** be brief. They are not designed for self-learning.

  If you miss or skip a lecture, you may have to read the corresponding part in the textbook. This may take you much more time. Hence, it is better that you attend live lectures.