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: Just drop by or send email for appointment.

Textbook and Lecture Notes

Textbook: W. Stallings, Cryptography and Network Security, Fourth Edition, Pearson, 2006.

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 and M.Sc students, 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

- Course project 15%
- Three assignments 45%
- Final exam (40%)

Learning Outcomes

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

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

Quiz I

Let A and B be two sets with $|A| = m$ and $|B| = n$.

- What is the total number of functions from A to B?
- If $m \geq n$, what is the total number of onto functions (i.e., surjections) from A to B?
- If $m \leq n$, what is the total number of one-to-one functions (i.e., injections) from A to B?

Quiz II

Let $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, where p_i's are pairwise distinct and $e_i \geq 1$.

- What is the total number of invertible elements in Z_n?
- Is there any polynomial algorithm for computing the inverse of x in Z_n?