Cryptography Principles and Applications

Yu Zhang

HIT/CST/NIS

Cryptography, Spring, 2014

Purposes

- Learn what the rigorous information security is.
- Learn how to secure information rigorously.
- Learn how mathematics interplays with engineering.
- *Learn some English at least.*

Things to remember

Cryptography is:

- A tremendous tool
- The basis for many security mechanisms

Cryptography is **NOT**:

- The solution to all security problems
- Reliable unless implemented and used properly
- Something you should try to invent yourself

Outline

- Classic cryptography, Perfect Secrets
- Private Key Encryption, MAC, Block Cipher, OWF
- Number Theory, Factoring and Discrete Log
- Key Management, Public Key, Digital Signature
- Random Oracle Model, Cryptographic Protocols

Textbooks

- **Introduction to Modern Cryptography**, *Jonathan Katz and Yehuda Lindell*, Chapman & Hall/CRC.
- **Applied Cryptography: Protocols, Algorithms, and Source Code in C**, *Bruce Schneier*, John Wiley & Sons. (Chinese)
- Dan Boneh's Cryptography @Stanford's Coursera.

Grades

- Composition:
  - Homework (30%)
  - Final Exam (70%)
- How to score high:
  - Read as much as you can.
  - Be skeptical about what you learn.
  - No Plagiarism!

Contact

Office: 710 Zong-He-Lou.

Email: yuni.zhang@gmail.com