Cryptography Principles

Yu Zhang

HIT/CST/NIS

Cryptography, Autumn, 2014

Purposes

- Learn what the rigorous information security is
- Learn how to secure information rigorously
- Learn how mathematics interplays with engineering

Cryptography is:

- A tremendous tool
- The basis for many security mechanisms
- Secure communication:
  - web traffic: HTTPS
  - wireless traffic: 802.11i WPA2 (and WEP), GSM, Bluetooth
  - encrypting files on disk: EFS, TrueCrypt
  - content protection (e.g. DVD, Blu-ray): CSS, AACS
  - user authentication

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
- TPD, Random Oracle Model
- Cryptographic Protocols

Textbooks & Slides

- **Introduction to Modern Cryptography**, *Jonathan Katz and Yehuda Lindell*, Chapman & Hall/CRC. (Eng & Chi.)
- **Applied Cryptography: Protocols, Algorithms, and Source Code in C**, *Bruce Schneier*, John Wiley & Sons. (Eng. & Chi.)
- Coursera: Dan Boneh's Cryptography @Stanford
- Slides: https://github.com/YuZhang/crypto2014

Grades

- Composition:
  - Homework (30%)
  - Final Exam (70%)
- How to score high:
  - Read the textbook IMC
  - Do homework by yourself
  - No Plagiarism! Otherwise, 0 point if copy two times.

Contact

Office: 710 Zong-He-Lou.

Email: yuni.zhang@gmail.com