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

What cryptography is and is not

Cryptography is:

- A tremendous tool
- The basis for many security mechanisms
- Secure communication:
  - web traffic: HTTPS (SSL/TLS)
  - wireless traffic: 802.11i WPA2 (and WEP), GSM, Bluetooth
  - encrypting files on disk: EFS, TrueCrypt
  - content protection: DVD (CSS), Blu-ray (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 (Many magics here)

We will learn from Turing Award recipients

- 1995 Manuel Blum
- 2000 Andrew Yao
- 2002 R. Rivest, A. Shamir, L. Adleman
- 2012 S. Micali, S. Goldwasser
- 2013 L. Lamport

Textbooks & Slides

- **Introduction to Modern Cryptography**, *Jonathan Katz and Yehuda Lindell*, Chapman & Hall/CRC. (Eng & Chi.)
- Stanford Dan Boneh's Cryptography @Coursera
- Slides: https://github.com/YuZhang/crypto2014

Grades

- Composition:
  - Homework ($6 \times 5 = 30\%$)
  - Final Exam (70%)
- How to score high:
  - Read the textbook IMC
  - Do homework by yourself
  - No Plagiarism! Otherwise, -5 point each time.

Contact

Office: 710 Zong-He-Lou.

Email: yuni.zhang@gmail.com