

Cryptography Principles

Yu Zhang

Harbin Institute of Technology

Cryptography, Autumn, 2022

What cryptography is and is not

Cryptography is:

- A tremendous tool
- The basis for many security mechanisms
- Secure communication/computation:
 - web traffic: HTTPS (SSL/TLS)
 - wireless traffic: Wifi (WPA2/3), 5G (AES-128 CTR), Bluetooth (SAFER+)
 - encrypting files on disk: EFS, TrueCrypt
 - digital rights management: Apple's FairPlay, console games
 - cryptocurrency: bitcoin

Cryptography is **NOT**:

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

Purposes

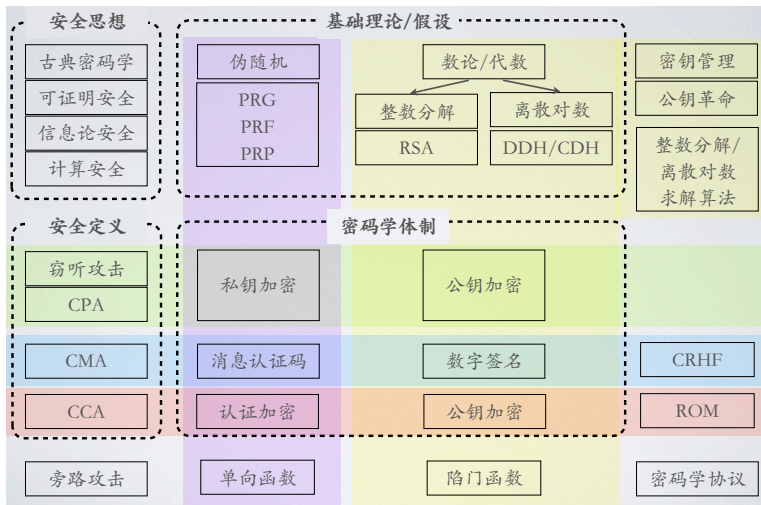
- Learn what the rigorous information security is
- Learn how to secure information rigorously
- Learn how mathematics interplays with engineering

We will learn from Turing Award recipients

- 1995 M. Blum
- 2000 A. Yao
- 2002 R. Rivest, A. Shamir, L. Adleman
- 2012 S. Micali, S. Goldwasser
- 2013 L. Lamport
- 2015 M. E. Hellman, W. Diffie

- 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)

Syllabus [in Chinese]



Textbook: **Introduction to Modern Cryptography (2nd Ed.)**,
Jonathan Katz and Yehuda Lindell

MOOC: Stanford Dan Boneh's Cryptography @Coursera

Slides: <https://github.com/YuZhang/cryptography>

QQ group: 672069016 for 2022

- Composition:

Homework: $4 \times 5 = 20\%$ (Homework 1~5)

Final Exam: 80%

Extra: 5% for outstanding homework (Homework 1~6)

- How to score high:

- Read the textbook IMC
- Do homework by yourself
- **No Plagiarism!**