课程简介

哈尔滨工业大学

张宇

2024春

密码学

- 信息化重塑了人类社会，形成了信息社会，而密码学是保护信息社会中人类信息活动的理论基础
  - 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
- 密码学不是：
  - 对所有安全问题的解
  - 可靠的，除非正确地实现和使用
  - 尝试自己发明的东西

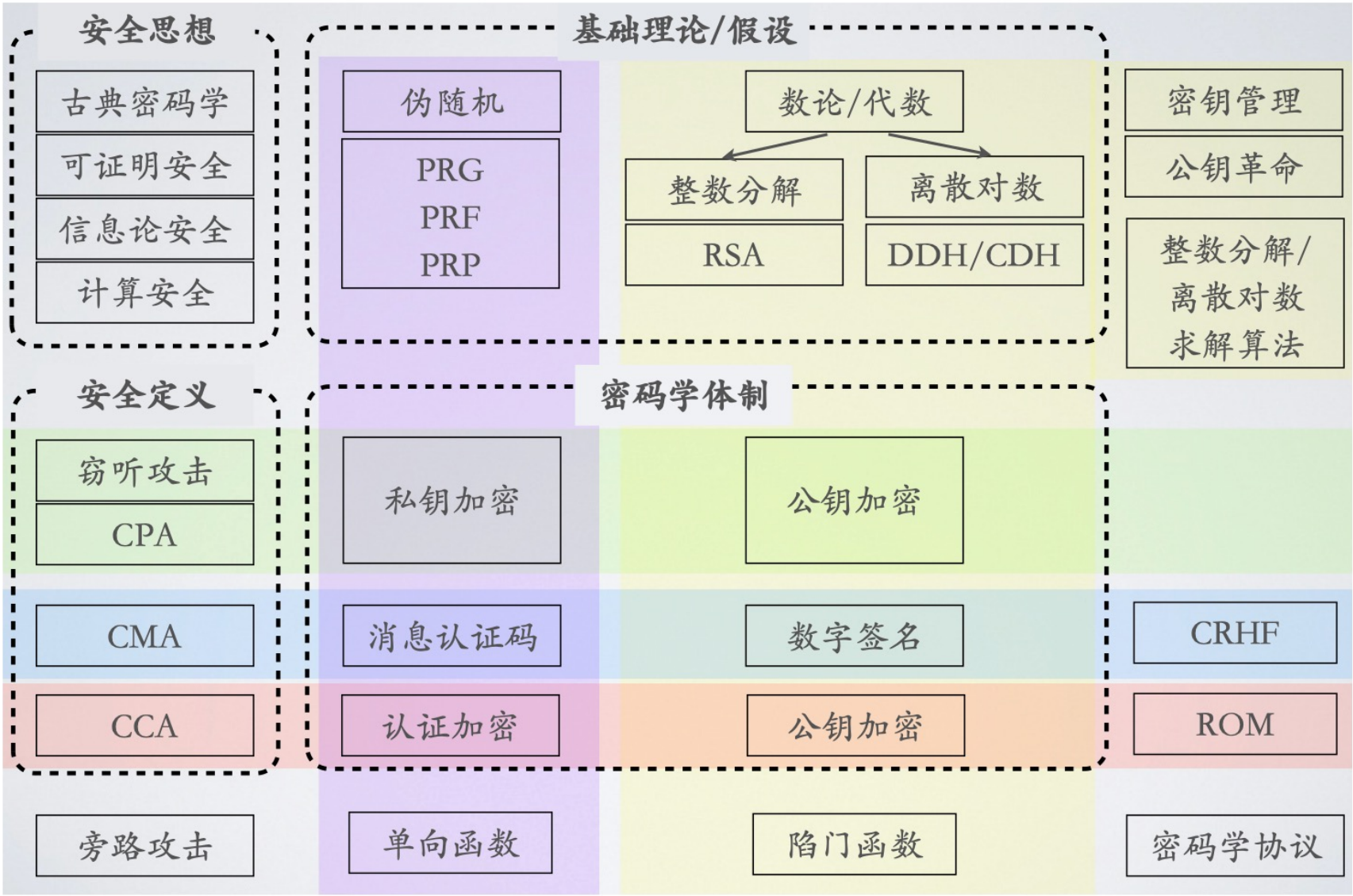
课程目标

- 学习什么是严格的信息安全
- 如何严格地保护信息
- 以及数学与工程是如何互动的

跟随图灵奖得主学习

- 1983 S. A. Cook
- 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

课程大纲


安全思想
古典密码学
可证明安全
信息论安全
计算安全
基础理论/假设
伪随机
PRG
PRF
PRP
数论/代数
整数分解
离散对数
RSA
DDH/CDH
密钥管理
公钥革命
整数分解/
离散对数
求解算法
安全定义
窃听攻击
CPA
CMA
CCA
密码学体制
私钥加密
公钥加密
消息认证码
数字签名
认证加密
公钥加密
CRHF
ROM
旁路攻击
单向函数
陷门函数
密码学协议

教材、课件、慕课

Textbook: **Introduction to Modern Cryptography (3rd Ed.)**, *Jonathan Katz and Yehuda Lindell*

MOOC: Stanford Dan Boneh's Cryptography @Coursera

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

- 为什么要学习英文教材和课件?

因为未来我们将与英文的密码学资料打交道。密码学知识成果最初是英文书写的，最好的密码学资料也是英文的，而且密码学工具也是英文。

为了更易于学习，我们用中文PPT。（配套了中文讲义）

课程考核

- 20% 作业：5次x4分
- 20% 实验：4次x5分
- 60% 期末考试：30分填空，30分简答

- 如何取得好成绩？
  - 阅读IMC教材
  - *思考*课堂练习和作业

- QQ群：295604020