密码理论与技术
– 计算机密码学理论与应用

田园

Father of Modern Cryptology, Diffie & Hellman，Laureate of Turing Prize at 2016

$$ed = 1 \bmod \varphi(N)$$
$$Y = M^e \bmod N$$
$$M = Yd \bmod N$$

课程概要

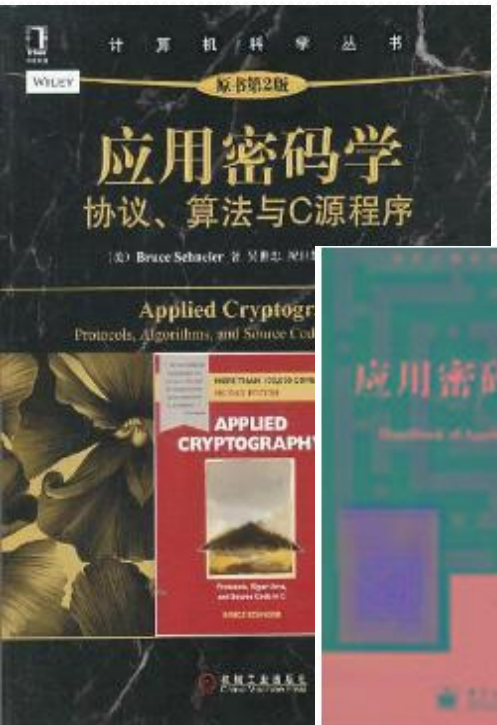
- 一、数学基础
- 整数的算术理论、有限域
- 二、密码学基本理论和典型密码方案
- 单向函数(OWF：*One-way Function*)、
- 难解性问题：因子分解、离散对数等；
- 公钥加密、数字签名、混合加密方案
- 密码方案/协议的安全模型
- 安全证明简介
- 三、典型密码协议
- 身份认证协议、密钥协商协议、零知识证明协议
- 四、先进密码学简介
- 椭圆曲线密码学(ECC)、
- 格密码学(Lattice Cryptography)

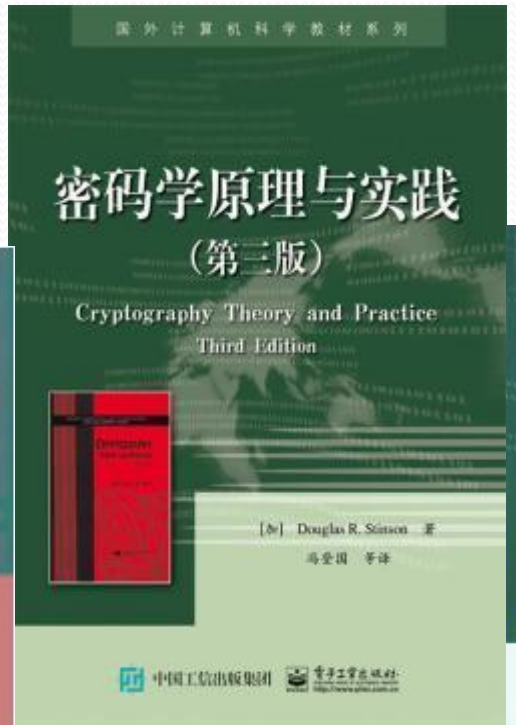
信息安全学科的主要分支简介

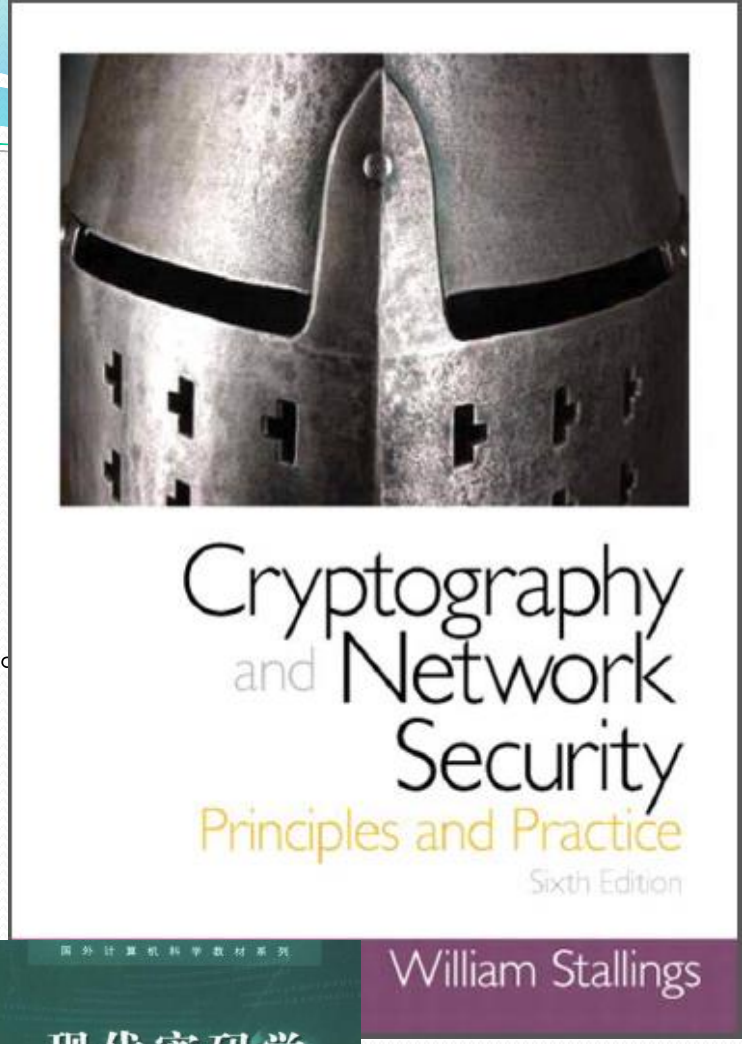
- 理论基础/计算机密码学
- （1）计算密码学：Computational Cryptography
- 密码学的计算复杂性理论基础
- 密码方案的数学基础
- 理论安全方案的构造
- 安全模型、安全方案/协议的证明
- （2）形式演算的密码学：Symbolic Cryptography
- 基于符号演算的安全证明方法和工具
- 应　用
- 密码方案及协议的应用、电子商务的应用、入侵检测技术、病毒识别、数据库安全、操作系统安全、网络体系安全，云计算安全，等。

参考书

- 主要参考书：
- 密码学原理与实践，E.R.Stinson，第三版。
- 供进一步深入学习的材料：
- 现代密码学理论与实践，W.Mao，2005。
- 应用密码学，B.Schnerier，2001。
- 应用密码学手册，Menezes & Vanstone，1997。







教程学习内容

- W.Stallings，第6版
- **第一单元 整数算术基础** ~2周
- 第4章、第8章、
- 二次剩余理论初步（补充材料/参见Stinson）

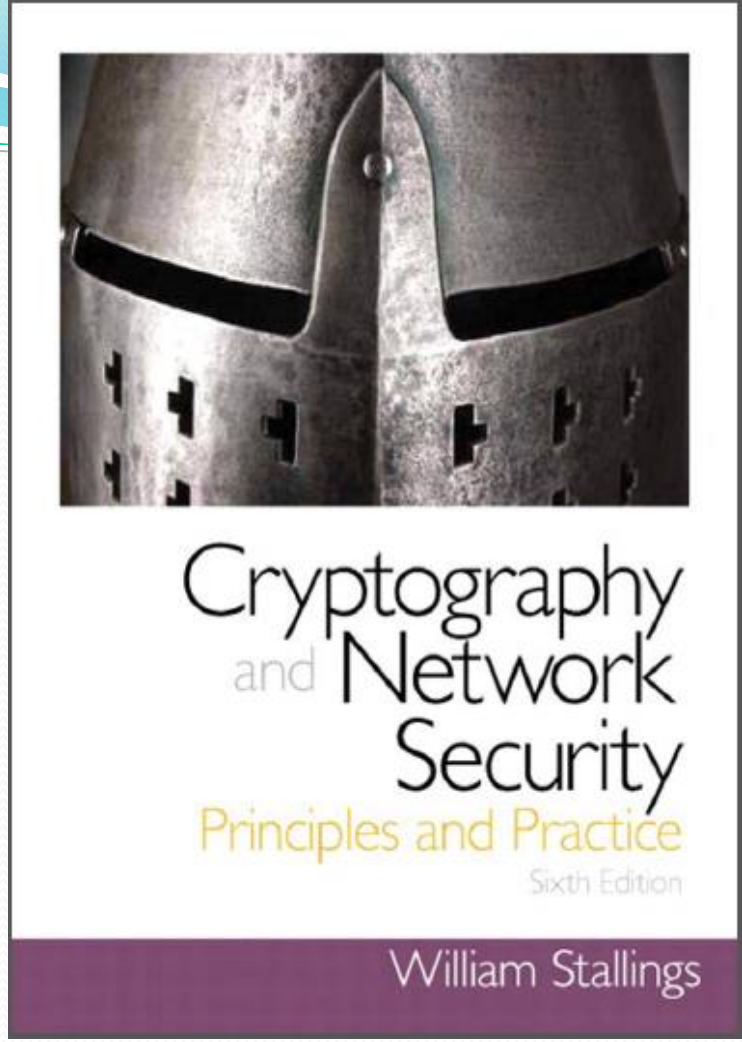
- **第二单元 基本安全方案** ~3.5周
- 公钥加密类方案 第9、10章+一些补充材料
- 公钥认证/签字类方案 第13章+一些补充材料
- 混合类加密方案 补充材料
- 对称加密类安全方案 第3、5、6章
  对称认证类方案 第11、12章
- 公钥及对称类安全方案的安全模型 补充材料

第三单元 安全协议 ~2.5周

身份认证类协议 第15章+补充材料

密钥协商类协议 第10章（略去椭圆曲线的部分）+补充材料

总体成绩：30%作业成绩+ 70%笔试成绩



计算机安全的基本理念

- （1）计算机安全方案/协议的安全性，是基于计算复杂性的现实安全性。
- 一个计算机安全方案/协议是安全的，并非指其不可被破译，而是指为达到可行的概率，破译该方案所必须的计算复杂度不可接受（指数复杂度范畴），或等价地，以可接受的复杂度（多项式复杂度范畴）破译该方案所达到的成功概率低到不可接受。
- （2）任何计算机安全方案/协议的构造都是公开的，计算机安全方案的安全性都不是建立在对方案本身如何工作进行保密的基础上。
- （3）信息安全理论相关的复杂度是指渐进复杂度，即复杂度随某个或某组安全参数变化而变化的趋势，例如某概率$p=O(e^{-k})$。
- （4）当代计算机安全方案/协议的基本分类：
- 对称类：基于共享的秘密参数；少部分。
- 非对称类/公钥类：不基于任何共享秘密；绝大部分。

计算机安全理论的数学基础

- 整数的算术理论
- （1） 同余等价关系及其基本性质 【第4章】
- （2）基本定理和公式：
- Euclid定理及等价形式、一次同余方程； 【第4章】
- 中国余数定理； 【第8章】
- Fermat公式和Euler公式； 【第8章】
- 二次剩余理论及应用
- 有限域的基本理论及应用
- 素域F_p和扩域F_{p^d}的重要性质 【第4章】