现代密码学理论与实践

授课人：王平辉
电子邮箱： phwang@mail.xjtu.edu.cn

课件来源：中国科技大学 杨寿保 教授

课程的简单介绍

1. 课程内容
   - 基本概念 (数论基础等)
   - 数据加密技术 (对称的和非对称的密码系统)
   - 密钥的产生、分享和管理
   - 数据的完整性保护
   - 身份认证、数字签名、数据鉴别和应用
   - 访问控制、网络安全等
   - 密码学的应用实践

课程的简单介绍

2. 教材和参考书
   - 密码编码学与网络安全：原理与实践 (第四版)， William Stallings，电子工业出版社， 2006.7. 已有第五版 (2011.12)
   - 通信网的安全－理论与技术，王育民等，西安电子科技大学出版社， 1999.4
   - Applied Cryptography—Protocols, Algorithms, and Source Code in C, Sec. ED. Bruce Schneier，机械工业出版社， 2001.1
   - 密码学与计算机网络安全，卿斯汉，清华大学出版社， 2001. 7.
3. 学时和学分

   32 学时，授课 8 周

课程的简单介绍

4. 成绩
   - 两次大作业 （ 50% ）
   - 闭卷考试 （ 50% ）

姚期智

（１）创建理论计算机科学的重要次领域：通讯复杂性和伪随机数生成计算理论

（２）奠定现代密码学基础，在基于复杂性的密码学和安全形式化方法方面有根本性贡献。例如：针对两方安全计算难题，提出乱码电路(Garbled circuits)

（３）解决线路复杂性、计算几何、数据结构及量子计算等领域的开放性问题并建立全新典范

王小云

1) How to Break MD5 and other Hash Functions
   (如何破解 MD5 及其他 Hash 函数）
   Eurocrypt 2005 “*Best Paper*Award” (2005 欧洲密码会议最佳论文奖)
2) Finding Collisions in the Full SHA-1
   Crypto 2005 “*Best Paper Award”* (2005 美国密码会议最佳论文奖)