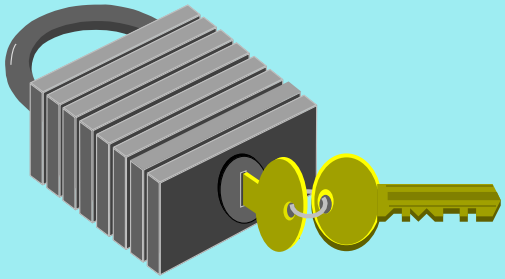

现代密码学

陈晓峰

网络与信息安全学院

Email: xfchen@xidian.edu.cn
Homepage: http://web.xidian.edu.cn/xfchen

内容提纲

第一讲：保密学基础

第二讲：单钥密码

第三讲：双钥密码

第四讲：认证与杂凑函数

第五讲：数字签字与身份认证

第六讲：安全协议及应用

第七讲：电子商务协议

参考书籍

- 王育民，刘建伟著，通信网的安全与保密，西安电子科技大学出版社，2000；
- Bruce Schneier, Applied Cryptography，John Wiley & Sons, 1994.
- Wenbo Mao，现代密码学-理论与实践，电子工业出版社，2003；
- Wenbo Mao, Modern Cryptography: Theory and Practice, Prentice-Hall, PTR，2003;
- Stallings, W., Cryptography and Network Security. Principles and Practice, 3rd edition, Prentice Hall, 2002

课程要求

- 了解和掌握密码学与网络安全的一些基本原理、技术、及最新研究成果
- 具有一定的网络与信息安全的理论基础和基本实践能力
- 考试成绩：平时作业+论文+期末试卷成绩（待定）

引论：Impossible Mission

- 公平掷币（Coin-Flipping by Phone）
- 零知识证明（Zero-knowledge Proof）
- 盲签名（Blind Signature）

……

Objective of Cryptography

- 机密性 (Confidentiality)：确保只有授权用户得到信息。(ensuring that information is accessible only to those authorized to have access.)
- 数据完整性 (Integrity)：确保数据是完整的，即所收到的数据完全和由授权的发件人发送的数据相同。没有人可以修改或替换消息。(ensuring data is "whole" or complete, i.e., that the data received are exactly as sent by an authorized sender. No one can modify or substitute a message.)
- 认证性 (Authentication)：建立或确认某事(或某人)是真实可信的，包括实体或数据来源的认证。(establishing or confirming something (or someone) as authentic, including entity or data origin authentication.)
- 不可抵赖性 (Non-repudiation)：在争议时确保一方不能否认或反驳声明的有效性。(ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement.)

密码学的历史
古典密码 (Classic Cryptography)

- BC 487：置换密码 Transposition Cipher, “Scytale”
- BC 300：隐匿术 (Steganography)：希腊人用奴隶传递信息
- BC 100–BC 44：代换密码 Substitution Cipher, “Caesar Cipher”
- 1883：Kerckhoffs’ Assumption
- WW II：Turing Machine for Cryptanalysis (Breaking the Enigma)
- 1949：Perfect Secrecy (C.E. Shannon) “Confusion”混淆 and “Diffusion”扩散

密码学的历史
现代密码学 (Modern Cryptography)

- 1976：公钥密码学(Public-Key Cryptography) (Diffie, Hellman)
- 1977：数据加密标准(Data Encryption Standard, DES (NIST))
- 1978：RSA (Rivest, Shamir, Adleman)
- 1982/85：Goldwasser presented 2 paradigms for firm foundations of cryptography. “Indistinguishability” and “Simulatability”
- 1998：DES 被破译
- 2000：AES (2000年10月2日确定了以 Rijdeal 作为 AES 的标准算法)

PKC Schemes

- RSA scheme (78) : R.L.Rivest, A.Shamir, L.Adleman
- McEliecescheme (78)
- Rabin scheme (79)
- Knapsack scheme (79): Merkle-Hellman, Chor-Rivest
- Williams scheme (80)
- ElGamal scheme (85)
- Elliptic Curve based scheme(85): Koblitz, Miller
- Hidden Field Equations(95): C*,Patarin
- Lattice Cryptography(97): Ajtai (AD, DDH, NTRU)
- Non abelian group Cryptography(2000): Braid
- Subgroup Cryptography: GH (99)； LUC(94)； XTR(2000)


thank you