《现代密码学》第四讲

分组密码（一）

《现代密码学》第四讲

分组密码的发展历史

本节主要内容

- 分组密码定义
- **分组密码的发展历史**
- 保密系统的安全性分析及分组密码的攻击
- 数据加密标准（DES）算法介绍
- 高级加密标准（AES）算法介绍
- 中国无限局域网标准（SMS4）算法介绍
- 分组密码算法的运行模式

分组密码的发展历史

- 二十世纪之前的密码算法

  算法、密钥保密

- 二十世纪之后的密码算法

  Kerokhoffs 假设：密码分析者已有密码算法及实现的全部详细资料 .

Kerckhoff 假设密码的安全性完全依赖于密钥 .

分组密码的发展历史

- **密码算法为什么需要公开?**
  - 民用

使用范围从军事到民用拓展。

  - 无陷门

使用者须确认算法不存在陷门。

  - 安全强度高

可以由全世界的密码学家对其安全性评估确保其足够的安全强度。

  - 标准化通信

分组密码的发展历史

- 1973 年 5 月美国联邦政府提出征求在传输和存储数据中保护计算机数据的密码算法的建议；
- 1975 年 3 月，美国国家标准局（NBS）首次公布 IBM 公司提出的算法 Lucifer 中选；
- 1977 年 1 月 NBS 正式向社会公布，采纳 IBM 公司设计的方案作为非机密数据的数据加密标准（Data Encryption Standard）. DES 正式成为美国联邦政府信息处理标准，即 FIPS-46 标准，同年 7 月开始生效。
- 此后，每隔 5 年美国国家保密局（NSA）对 DES 作新的评估，并重新审定它是否继续作为联邦加密标准。

分组密码的发展历史

- 理论强度，97 年 $100000 的机器可以在 6 小时内用穷举法攻破 DES 。

- 实际攻破的例子，97 年 1 月提出挑战，有人利用 Internet 的分布式计算能力，组织志愿军连接了 70000 多个系统在 96 天后攻破。

分组密码的发展历史

- 1997 年， 美国标准技术研究所（NIST）对 DES 进行再次评测并宣布： DES 算法的安全强度已经不足以保障联邦政府信息数据的安全性， 所以 NIST 建议撤销相关标准。

- 同时， NIST 开始征集新的数据加密标准 ---- 高级数据加密标准（Advanced Encryption Standard）。

- 新算法的分组长度为 128， 支持可变密钥长度 128 、 192 、 256 比特。

分组密码的发展历史

- 1999 年， NIST 从提交的 15 个候选草案中选取了 5 个优良的算法作为 AES 的候选算法： MARS 、 RC6 、 Rijndael 、 Serpent 和 Twofish

- 综合评价最终确定 Rijndael 算法为新的数据加密标准， 2001 年 12 月正式公布 FIPS-197 标准。

- www.nist.gov/aes

分组密码的发展历史

- www.nist.gov/aes

分组密码的发展历史

- 欧洲于2000年1月启动了NESSIE工程，该工程的目的是评价出包含分组密码，流密码等在内的一系列安全， 高效和灵活的密码算法。
- 至2000年9月， 共征集到了17个分组密码算法， 同时将TDES和AES纳入了评估范围，并作为分组密码算法的评测基准。
- 经过3年2个阶段的筛选，最终确定下列算法为推荐的分组密码算法： MISTY-64、 Camllia-128、 AES-128和SHACAL-2。

分组密码的发展历史

- 日本政府在2000年成立了密码研究与评估委员会（CRYPTREC）并参考欧洲NESSIE工程的作法对密码算法的安全性和效率等问题进行评估，以备政府使用.
- 2002年初步拟定了推荐算法的草案，2003年3月确定了推荐算法名单， 其中分组密码算法包括:

(1) 分组长度为64比特的算法: CIPHERUNICORN-E、 MISTY1和3-key-TDES.

(2) 分组长度为128比特的算法: Camellia、 CIPHERUNICORN-A、 Hierocrypt-3、 SC2000和

THE END □