《现代密码学》第四讲

分组密码（一）

上讲内容回顾

- 问题的定义及分类
- 算法复杂度定义及分类
- P 问题和 NP 问题
- 密码算法的计算安全性

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

注意事项

从本讲开始，假定加密认证的文本、图像、音频等任何格式的原始信息，都存在相应的编码方式，转化为二进制的数据流。在具体算法中，表示为message={0,1}*

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

分组密码的定义

- 分组密码（block cipher）是现代密码学中的重要体制之一，其主要任务是提供**数据保密性**
- 分组密码加解密速度较快
- 现代分组密码发展非常快，技术较成熟，使用广泛
- 其他密码算法设计领域有广泛应用，例如：可以用于构造伪随机数生成器、流密码、认证码和哈希函数等

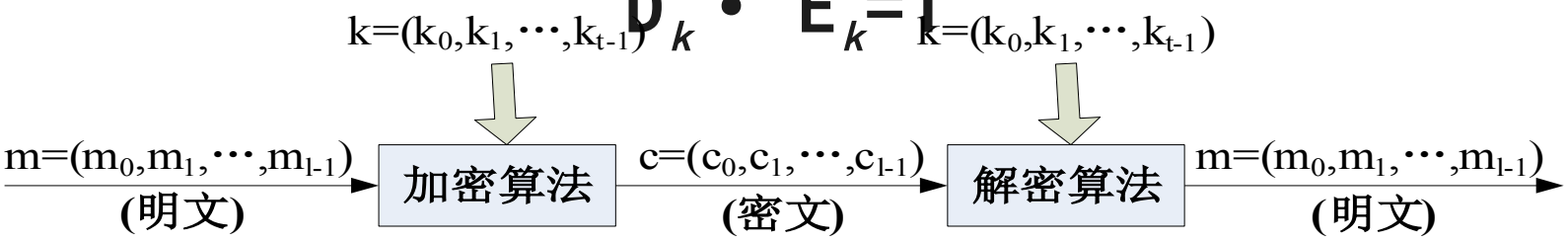
分组密码的定义

定义 一个分组密码体制（P，K，C，E，D），其中 $P=C=\{0,1\}^{l}$；$K=\{0,1\}^{t}$.

加密变换： $E: P\times K\rightarrow C$，当 $k\in K$ 确定时，E_k 为 $P\rightarrow C$ 的一一映射.

解密变换： $D: C\times K\rightarrow P$，当 $k\in K$ 确定时，D_k 为 $C\rightarrow P$ 的一一映射.

$$D_k \cdot E_k = I$$



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

回顾分组密码设计准则

- 迭代结构：选择某个较为简单的密码变换，在密钥控制下以迭代方式多次利用它进行加密变换，就可以实现预期的扩散和混乱效果。
- 混淆：是指在加密变换过程中是明文、密钥以及密文之间的关系尽可能地复杂化，以防密码破译者采用统计分析法进行破译攻击。
- 扩散：明文和密钥中任何一比特值得改变，都会在某种程度上影响到密文值的变化，以防止将密钥分解成若干个孤立的小部分，然后各个击破。

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

保密系统的安全性分析及分组密码攻击手段

- 攻击目的

1. 完全破译：破译使用者的密钥

2. 部分破译：恢复某些密文对应的明文

保密系统的安全性分析及分组密码攻击手段

- 攻击种类

1. 唯密文攻击：密码分析者有一个或更多的用同一个密钥加密的密文，通过对这些截获的密文进行分析得出明文或密钥。

2. 已知明文攻击：除待解的密文外，密码分析者有一些明文和用同一个密钥加密这些明文所对应的密文。

被动攻击

保密系统的安全性分析及分组密码攻击手段

3. 选择明文攻击：密码分析者可得到所需要的任何明文所对应的密文，这些密文与待解的密文是用同一个密钥加密得来的。

4. 选择密文攻击：密码分析者可得到所需要的任何密文所对应的明文，解密这些密文所使用的密钥与解密待解的密文的密钥一样。

5. 自适应选择明文攻击：密码分析者可得到所需要的任何明文所对应的密文，这些密文与待解的密文是用同一个密钥加密得来的，明文可以在看到加密机的返回结果后随时选取。

6. 自适应选择密文攻击：密码分析者可得到所需要的任何密文所对应的明文，解密这些密文所使用的密钥与解密待解的密文的密钥是一样的．密文可以在看到解密机的返回结果后随时选取。

主动攻击

保密系统的安全性分析及分组密码攻击手段

- 攻击手段

  1. 穷举法：当分组长度 n 较小时，攻击者可以有效地穷举明文空间，得到密钥。
  2. 差分分析
  3. 线性分析
  4. 相关密钥
  5. 侧信道攻击

  …

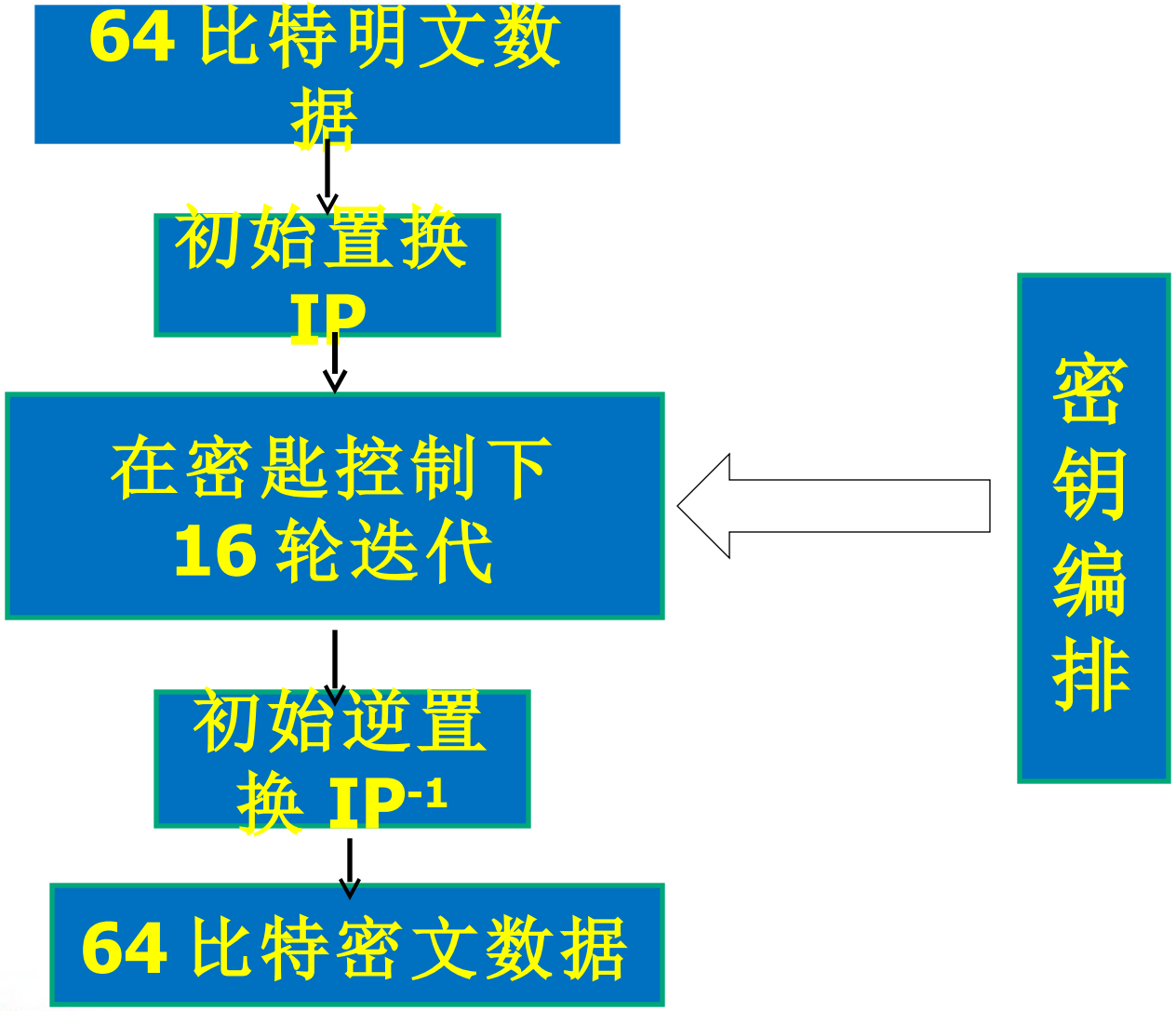
本节主要内容

- 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

DES 算法概述

- 明文和密文分组长度为 64 比特
- 算法包含两部分：迭代加解密和密钥编排
- Feistel 结构（加解密相似）：加密和解密除密钥编排不同外， 完全相同
- 密钥长度： 56 比特（ DES 的密钥空间： 2^{56} ），每 7 比特后为一个奇偶校验位（第 8 位），共 64 比特
- 轮函数采用混乱和扩散的组合，共 16 轮

DES 算法概述



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

AES 算法算法概述

- 分组加密算法：明文（128/256 比特）和密文分组（128/192/256 比特）可变长度。
- SPN 结构：轮函数包含代换层－置换层－密钥混合层。
- 密钥长度： 128 比特（AES 的密钥空间：2^{128}）
- 128 比特： 10 轮 .

AES算法的一个加密过程演示

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

无限局域网密码算法 --SMS4

- 中国政府颁布的 CO 标准算法
- 分组加密算法：明文和密文分组长度 128 比特
- 结构：广义 Feistel 结构，基本操作单位 32 比特

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

分组密码运行模式

1. 电码本模式（ECB 模式）
2. 密码反馈模式（CFB 模式）
3. 密码分组链接模式（CBC 模式）
4. 输出反馈模式（OFB 模式）
5. 计数模式（CRT 模式）

主要知识点小结

- 分组密码定义
- 保密系统的安全性分析及分组密码的攻击

THE END !