



《现代密码学》第四讲

分组密码（一）





《现代密码学》第四讲

保密系统的安全性分析 及分组密码的攻击





● 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
- 中国无线局域网标准（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
- 中国无线局域网标准（SMS4）算法介绍
- 分组密码算法的运行模式





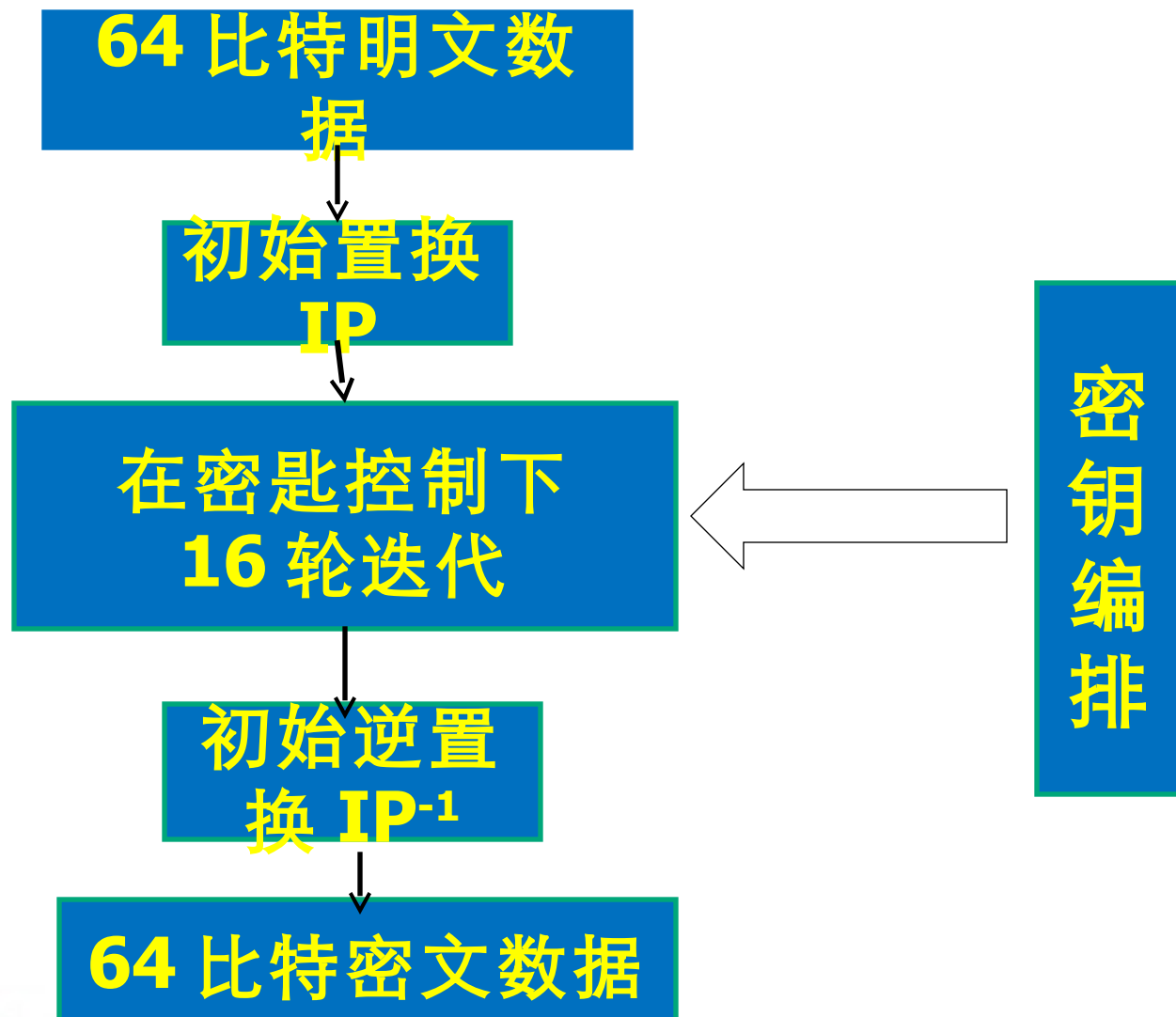
DES 算法概述

- 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
- 中国无线局域网标准（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。





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
- 中国无线局域网标准（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 G0 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
- 中国无线局域网标准（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（CTR 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 ☐

