《现代密码学》第四讲

分组密码（一）

上讲内容回顾

- Shannon的通信保密系统
- 熵和无条件保密
- 复杂度理论基础概念
- 计算安全性

注意事项

从本讲开始，假定原始的文本、图像、音频等任何格式的数据信息，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}*

本讲主要内容

- 分组密码定义
- 分组密码的发展历史
- 分组密码算法设计思想
- 数据加密标准（DES）算法介绍
- 高级加密标准（AES）算法介绍
- 分组密码算法的应用

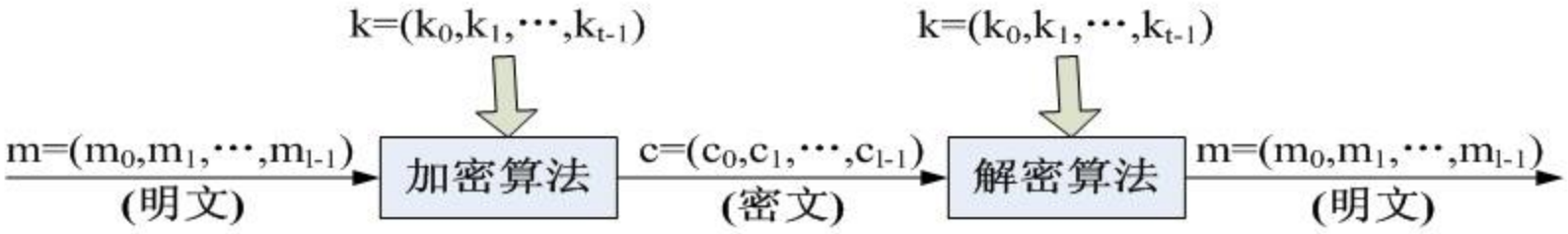
分组密码的定义

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.

$$D_k \bullet E_k = I$$



本讲主要内容

- 分组密码定义
- 分组密码的发展历史
- 分组密码算法设计思想
- 数据加密标准（DES）算法介绍
- 高级加密标准（AES）算法介绍
- 分组密码算法的应用

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

- 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

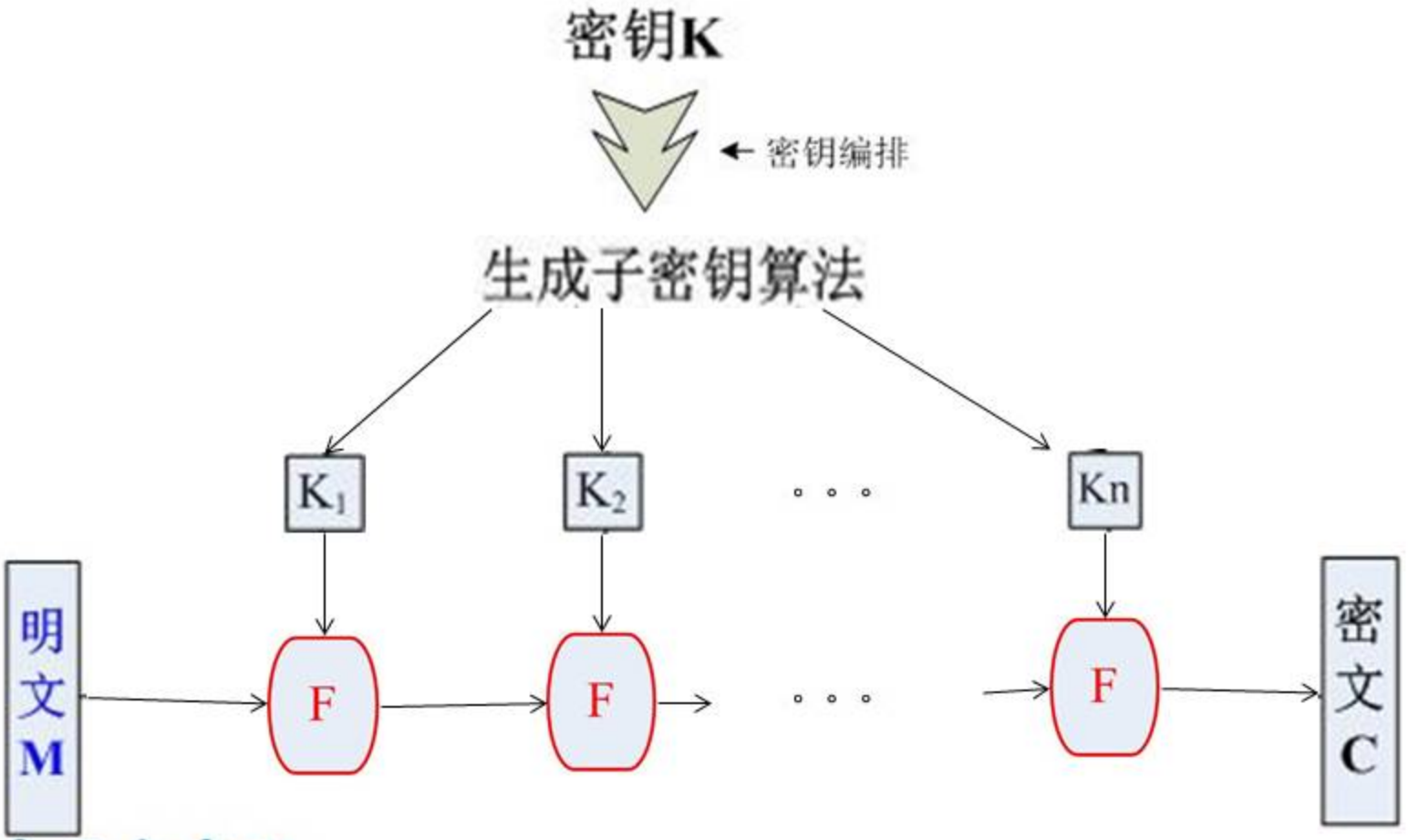
- 1997年，美国标准技术研究所（NIST）对DES进行再次评测并宣布：DES算法的安全强度已经不足以保障联邦政府信息数据的安全性，所以NIST建议撤销相关标准。

- 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。

分组密码算法设计思想

- 迭代结构（乘积密码）：



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

分组密码算法设计思想

- 如果密码体制不是幂等的($F^2 \neq F$), 那么多次迭代有可能提高密码体制的安全性.
- 采用迭代结构的优点：软、硬件实现节省了代码（硬件）资源.

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Rijndael128.

分组密码算法设计思想

- 混淆：明文/密钥和密文之间的关系复杂

- 扩散：明文/密钥的每一个比特都影响密文的每一个比特

分组密码的发展历史

- WAPI标准是中国颁布的无线局域网安全国家标准，
- 2006年1月，国家密码管理局公开SMS4密码算法--国家密码管理局公告（第 7 号）这是我国第一次公布自己的商用密码算法。
- 2012年SMS4被国家商用密码管理局确定为国家密码行业标准，标准编号GM/T 0002-2012，并且改名为SM4算法。

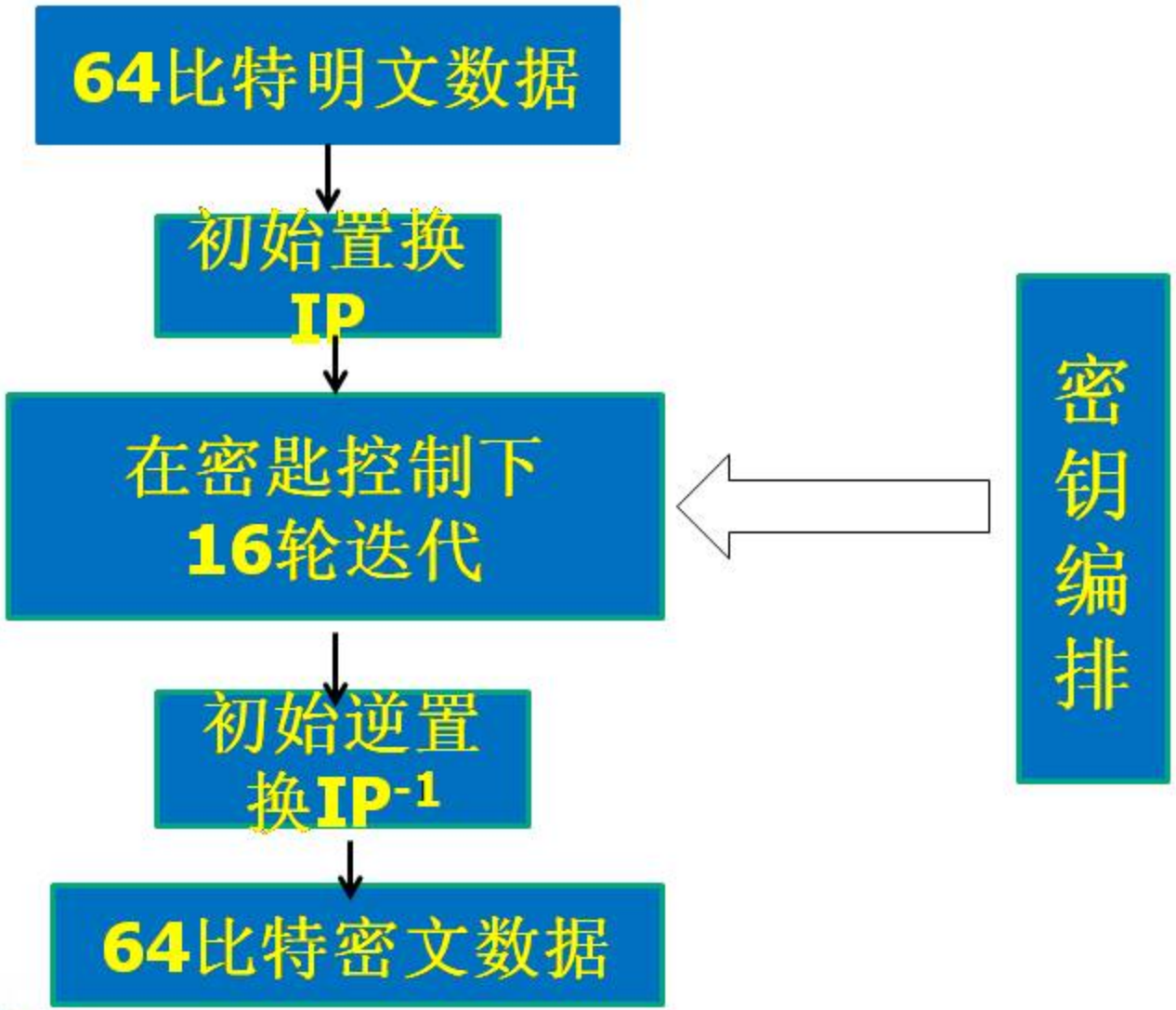
本讲主要内容

- 分组密码定义
- 分组密码的发展历史
- 分组密码算法设计思想
- 数据加密标准（DES）算法介绍
- 高级加密标准（AES）算法介绍
- 分组密码算法的应用

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

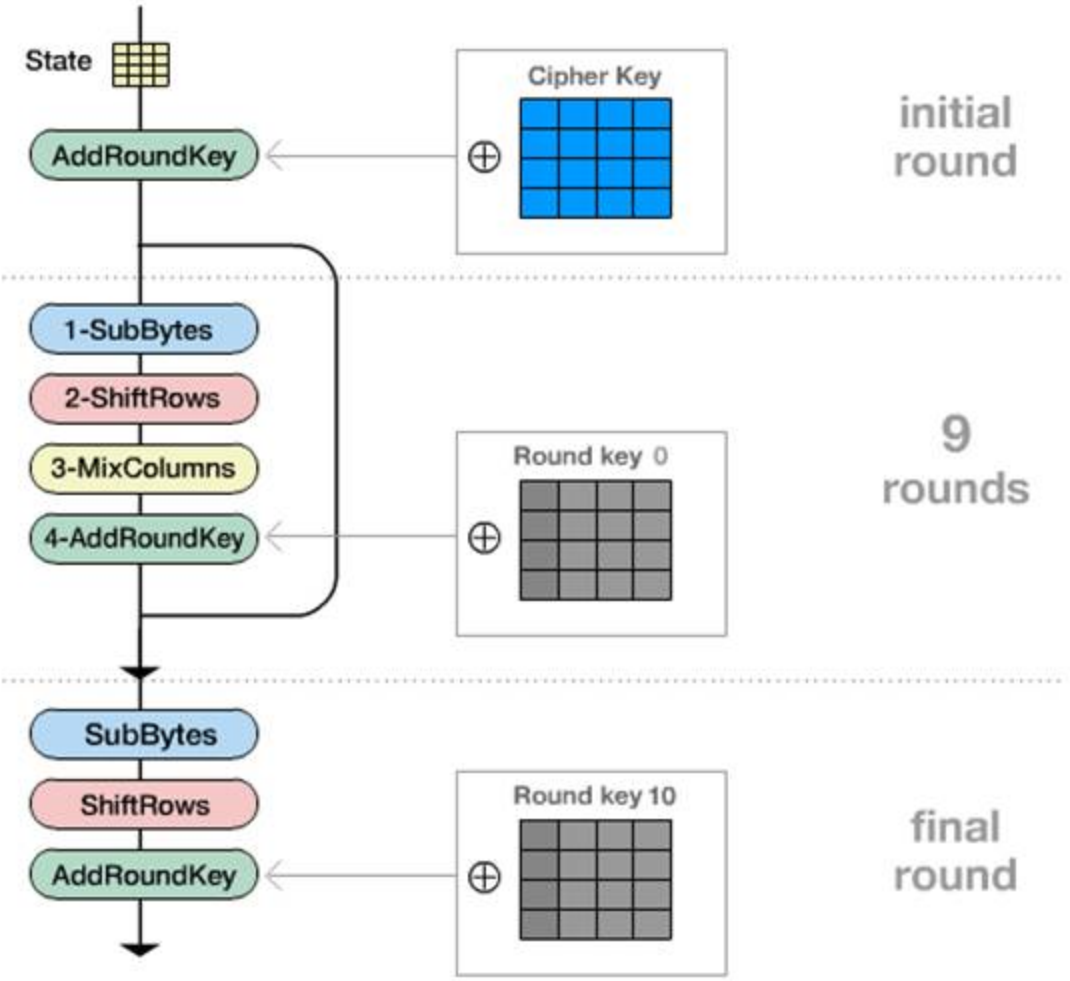
DES算法概述



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算法算法概述


State
AddRoundKey
Cipher Key
initial round
1-SubBytes
2-ShiftRows
3-MixColumns
4-AddRoundKey
Round key 0
9 rounds
SubBytes
ShiftRows
AddRoundKey
Round key 10
final round

主要知识点小结

- 分组密码定义
- 分组密码算法的设计思想

THE END!