第 2 章：分组密码体制

2.1 分组密码的基本原理

赵俊舟

junzhou.zhao@xjtu.edu.cn

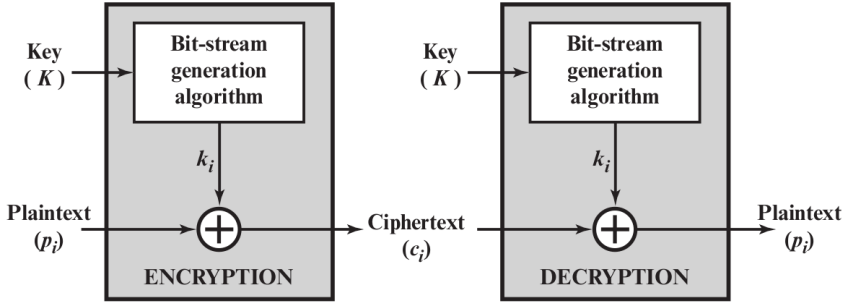
2025 年 2 月 28 日

目录

目录

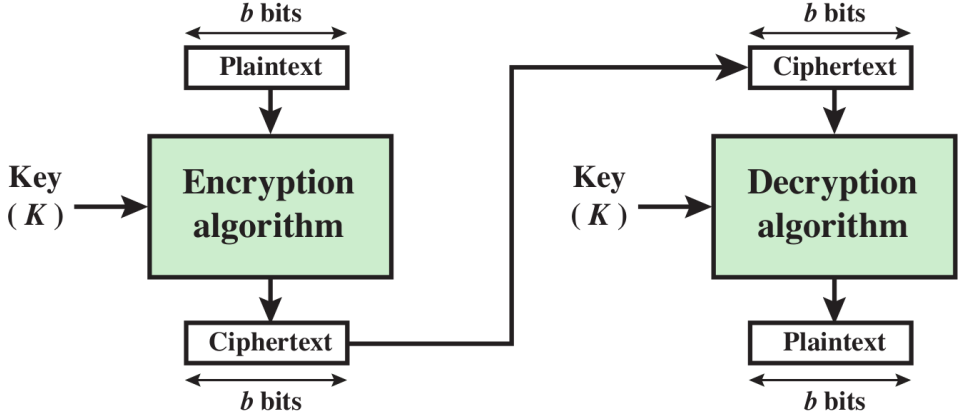
流密码（Stream Cipher）

- 流密码每次加密数据流的一个比特位或一个字节，得到与明文序列同样长度的密文序列。
- 加密：以比特/字节为单位，让明文序列与密钥流按比特/字节异或运算后，作为密文序列。
- 解密：以比特/字节为单位，让密文序列与相同的密钥流按比特/字节异或运算后，得到明文文序列。



分组密码（Block Cipher）

- 分组密码将一个明文分组作为整体进行加密，得到与明文等长的密文分组。
- 通常以大于等于 64 位的数据块为分组单位，加密得到相同长度的密文分组。



目录

理想分组密码：可逆映射

- 分组密码作用于 n 位明文分组上，产生 n 位密文分组。
- n 位明文分组有 2^n 种输入，每一种都必须产生一个唯一密文分组，这种变换称为可逆的或非奇异的。

明文	密文
00	11
01	10
10	00
11	01

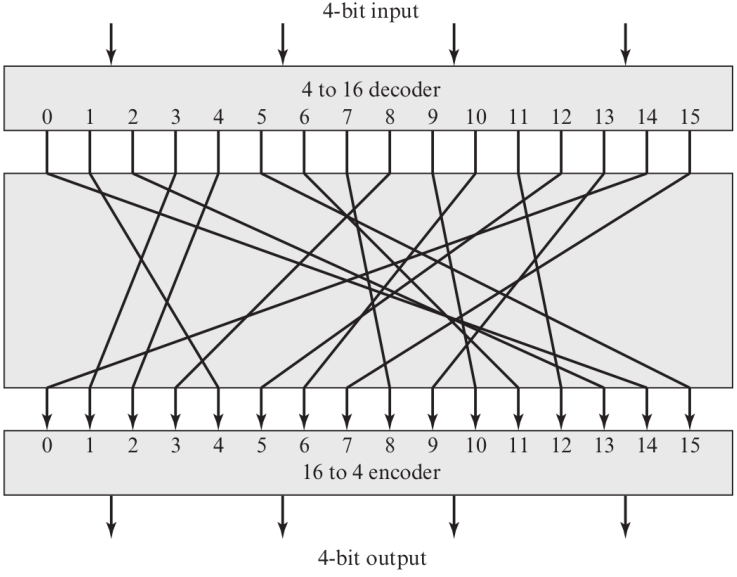
可逆映射

明文	密文
00	11
01	10
10	01
11	01

不可逆映射

理想分组密码：一个 4 位到 4 位的分组密码

分组密码本质上可以看作是一个巨大的代换密码。



理想分组密码的密钥

- 一共有 $2^n!$ 种可逆映射。
- 表的第二列定义了 $2^n!$ 个映射中的某个特定映射，即为理想分组密码的密钥。
- Feistel 称这种密码为理想分组密码，因为它允许生成最大数量的映射。
- 理想分组密码拥有最大的密钥空间 $2^n!$
- 密钥大小为 $n2^n$ 比特，因为只需保存表的第二列。

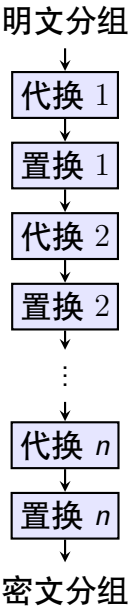
Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

理想分组密码存在的问题

- 分组长度 n 比较小时，例如 $n = 8$，密码系统等价于传统代换密码，容易利用明文的统计信息攻击它。
- 如果 n 充分大并且允许明密文之间采用任意可逆变换，那么明文的统计特征将被掩盖，从而不能利用明文的统计信息攻击这种密码系统。
- 对于 n 位分组，密钥大小为 $n2^n$ 比特。
  - 例如一个 64 位理想分组密码，密钥大小为 $64 \times 2^{64} = 2^{70}\text{bit} = 1\text{Zb}$
  - 1ZB: global yearly Internet traffic in 2016.
- 1973 年，Horst Feistel 指出：我们所需要的分组密码是对理想分组密码的一种近似，更容易实现，提出了基于可逆乘积密码概念的 Feistel 分组密码结构。

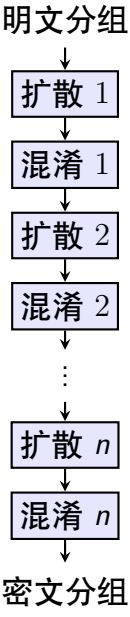
乘积密码的设计思想

- 乘积密码指依次使用两个或两个以上的基本密码，增强密码的强度。
- Feistel 建议交替使用代换和置换设计分组密码：
  - 代换：每个明文字母被唯一地替换为相应的密文字母
  - 置换：明文字母序列被替换为该序列的一个置换
- 实际上这个方案是 Shannon 1949 年提出的 Substitution-Permutation Networks (SPN) 的实现。
- Shannon 认为，为了应对基于统计分析的密码分析，必须对明文做扩散和混淆，以减少密文的统计特性，为密码分析制造障碍。



乘积密码的设计思想：扩散和混淆

- **扩散（Diffusion）**：使输入（包括明文和密钥）的统计特征消散在输出（例如密文或哈希值）中，让每个输入比特影响尽可能多的输出比特。其目的是隐藏输出和输入的统计关系，使输入的统计特征扩散到输出中去，从而无法根据输出的统计特征分析输入的统计特征。
- **混淆（Confusion）**：输出结果的每一个比特位都应该依赖于输入的大部分内容，即输入和输出之间没有直接的映射关系。其目的是隐藏输入与输出之间的映射关系，使之变得尽可能复杂而难以分析。
- 扩散-混淆原则的目的是为了增强密码算法的安全强度，评判扩散-混淆效果的标准是看能否发生雪崩效应：输入的微小改变导致输出的大幅改变。



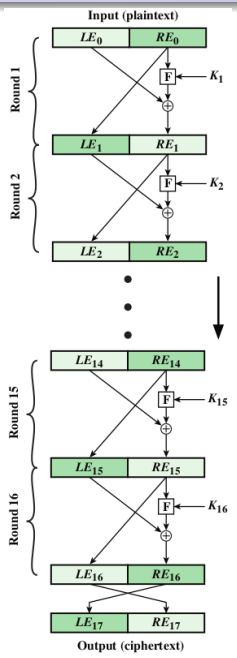
目录

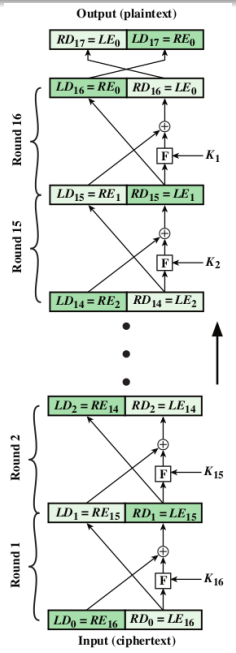
Feistel 密码结构

- Feistel 密码结构（也叫 Feistel Networks），由德裔美国人 Horst Feistel（物理学家和密码学家）在 1973 年提出。
- Feistel 在美国 IBM 工作期间完成此项开拓性研究，目前大部分分组密码都使用该方案，包括数据加密标准（DES）。
- Feistel 密码结构的优点在于加密和解密操作非常相似，在某些情况下甚至是相同的，只需逆转密钥编排，因此能够使代码或电路规模减半。
- 密码学家已经深入研究了 Feistel 密码结构的安全性。

Feistel 密码结构

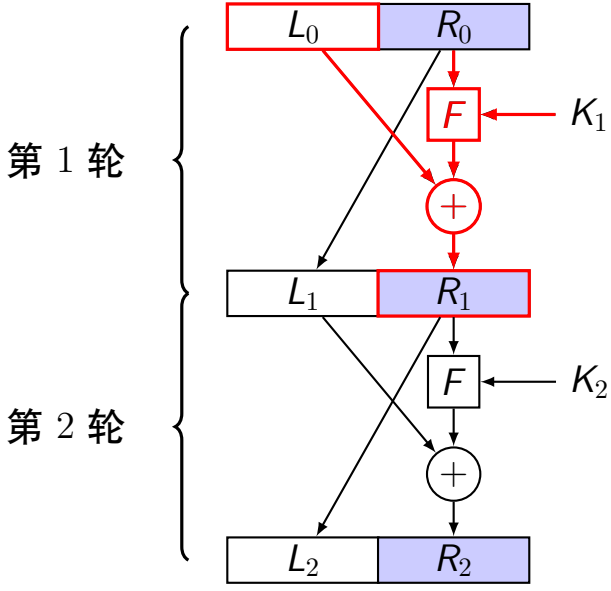
加密过程 →



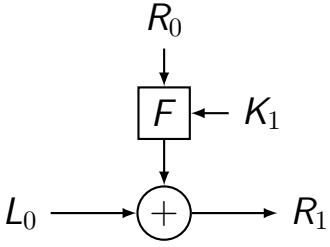


← 解密过程

Feistel 密码结构

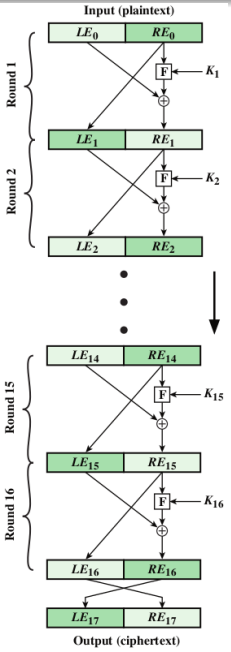


L_0, R_0	本轮输入分组
K_1	轮密钥
F	轮函数
L_1, R_1	本轮输出分组



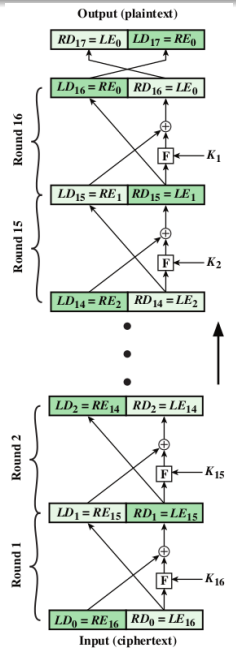
Feistel 密码：加密过程

- 将输入分组分成左右两部分，实施 Shannon's 的 SPN 概念；
- 对左半部数据实施多回合的代替操作；
- 将右半部数据和子密钥输入到轮函数 F，其输出与左半部分数据异或；
- 最后一轮操作结束后，将两部分数据进行互换，得到输出密文分组。



Feistel 密码：解密过程

- 解密过程本质上与加密过程一致；
- 将密文作为算法输入，逆序使用子密钥；
- 解密的过程不要求轮函数 F 是可逆的；
- 由于加密与解密对称，Feistel 结构的电路实现可以减少硬件元器件。



Feistel 密码设计原则

- 分组长度：分组越长则安全性越高，但加/解密速度越低，分组长度为 64 位是一个合理的折衷；
- 密钥长度：密钥越长越安全，但加/解密速度越低，64 位长的密钥已被证明是不安全的，128 位是常用的长度；
- 迭代次数：迭代越多越安全，通常为 16 次迭代；
- 子密钥产生算法：越复杂则密码分析越困难；
- 轮函数 F：越复杂则抗密码分析的能力越强；
- 快速的软件加密/解密：算法的执行速度很重要；
- 简化分析难度：算法简洁清楚，易于分析弱点，发现问题。

小结

1. 流密码与分组密码
2. 理想分组密码
3. Feistel 分组密码