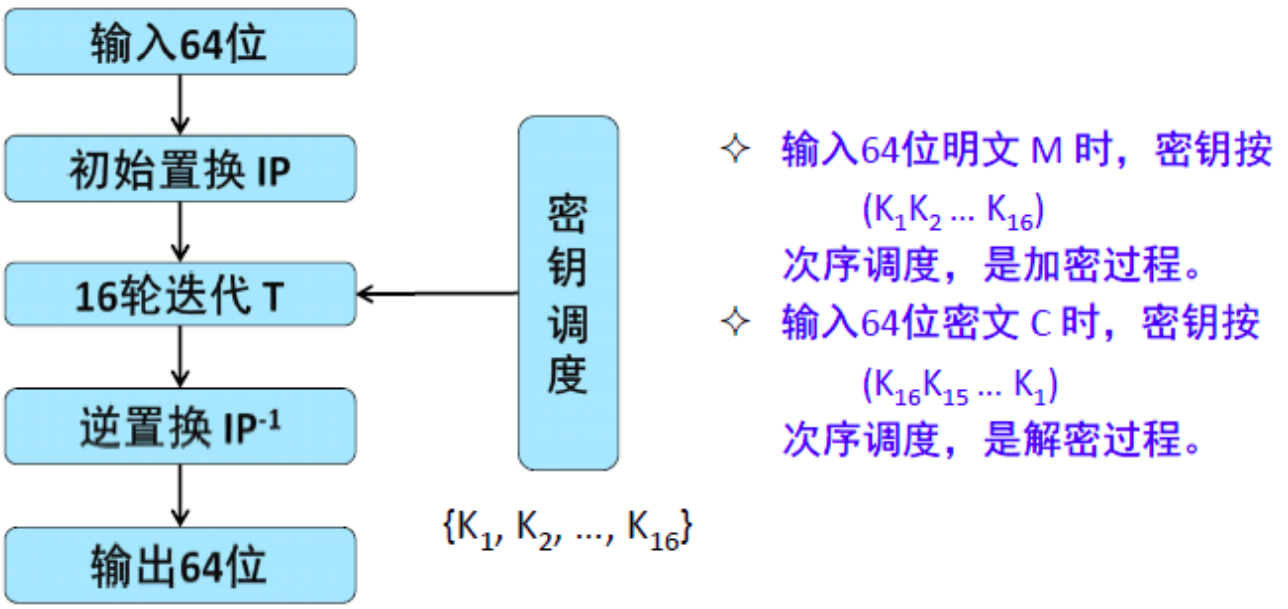
DES算法的详细设计

算法原理概述

- DES算法是一种典型的块加密算法，以64位为一组的明文块作为输入，经过加密后输出同样64位的密文。
- DES算法使用加密密钥定义变换过程，算法认为只有使用加密所使用的密钥才可以解密
- DES算法使用64位密钥，但是实际上64位密钥被分成8个分组，每个分组的最后一位为奇偶校验位，实际的密钥长度为56位。
- DES算法的基本过程是换位和置换

总体结构

DES算法的总体结构—— *Feistel* 结构



模块分解

- 密钥调度模块
  - 子密钥生成模块
    - PC-1置换模块
    - 循环左移模块
    - PC-2压缩置换模块
- IP 与IP^{-1} 置换模块
- 16 轮迭代 T 模块

- 迭代逻辑模块
- *Feistel* 轮函数 $f(R_{i-1}, K_i)$
  - E-扩展模块
  - S-盒模块
  - P-置换模块

数据结构

类-C语言算法过程