DES算法详细设计

1. 算法原理概述

数据加密标准 (DES，Data Encryption Standard) 是一种使 用密钥加密的块密码，1976年被美国国家标准局 (NBS, National Bureau of Standards，1988年改名为 NIST) 确定为联邦信息处理标准 (FIPS)，随后在国际上获得广泛采用。

DES 是一种典型的块加密方法：它以64位为分组长度，64 位一组的明文作为算法的输入，通过一系列复杂的操作，输出同样64位长度的密文。

DES使用加密密钥定义变换过程，因此算法认为只有持有 加密所用的密钥的用户才能解密密文。

DES的采用64位密钥，但由于每8位中的最后1位用于奇偶校验，实际有效密钥长度为56位。密钥可以是任意的56位的数，且可随时改变。其中极少量的数被认为是弱密钥，但能容易地避开它们。所有的保密性依赖于密钥。

DES 算法的基本过程是换位和置换。

1. 总体结构

1）基本信息

设信息空间由{0, 1}组成的字符串构成，明文信息和经过DES加密的密文信息是64位的分组，密钥也是64位。

明文：

密文：

密钥：

◌ 除去k8, k16, …, k64 共8位奇偶校验位，起作用的仅为56位。

加密过程

 ,其中为初始置换，是的逆，是一系列的迭代变换。

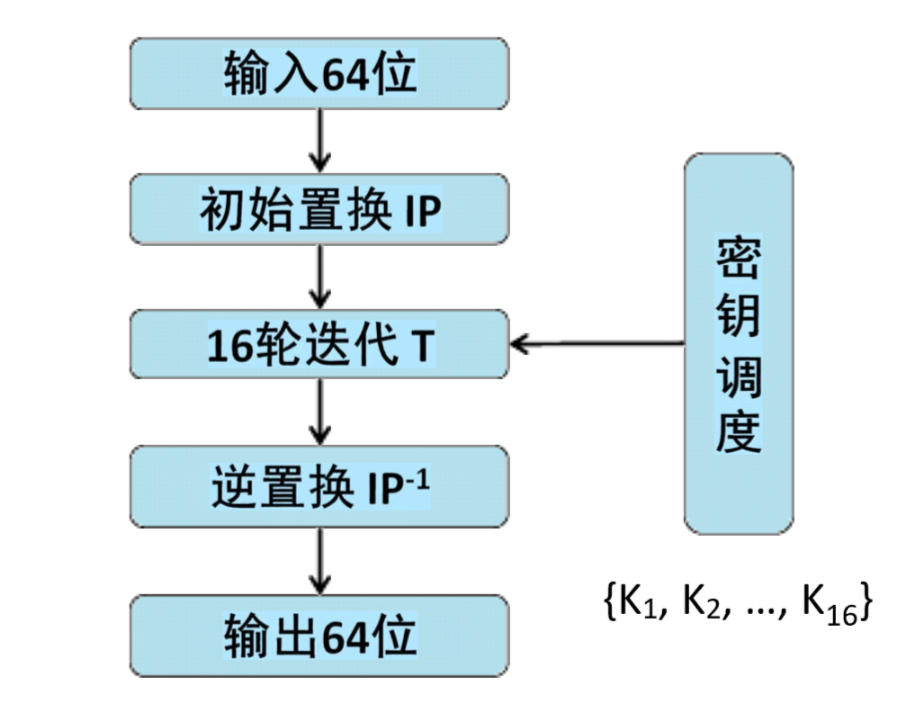
解密过程

 

2）Feistel结构

输入64位明文M 时，密钥按次序调度，是加密过程。

输入64位密文C 时，密钥按次序调度，是解密过程。



1. 输入64bit明文
2. 初始置换IP

给定64位明文块M，通过一个固定的初始置换IP 来重排M中的二进制位，得到二进制串M0 = IP(M) = L0R0，这里L0 和分别是R0 的前32位和后32位。下表给出IP 置换后的下标编号序列。



64bit看作线性表，用下标位置表示排列结果

1. 迭代T

根据 L0R0 按下述规则进行16次迭代，即

Li = Ri-1, Ri = Li-1 *f*(Ri-1, Ki), i = 1 .. 16

这里是32位二进制串按位异或运算，f 是 Feistel 轮函数

16个长度为48bit的子密钥Ki (i = 1 .. 16)由密钥K 生成 

16次迭代后得到L16R16

 左右交换输出R16L16

1. 模块分解
2. 数据结构
3. 类C语言算法过程