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

2.1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。

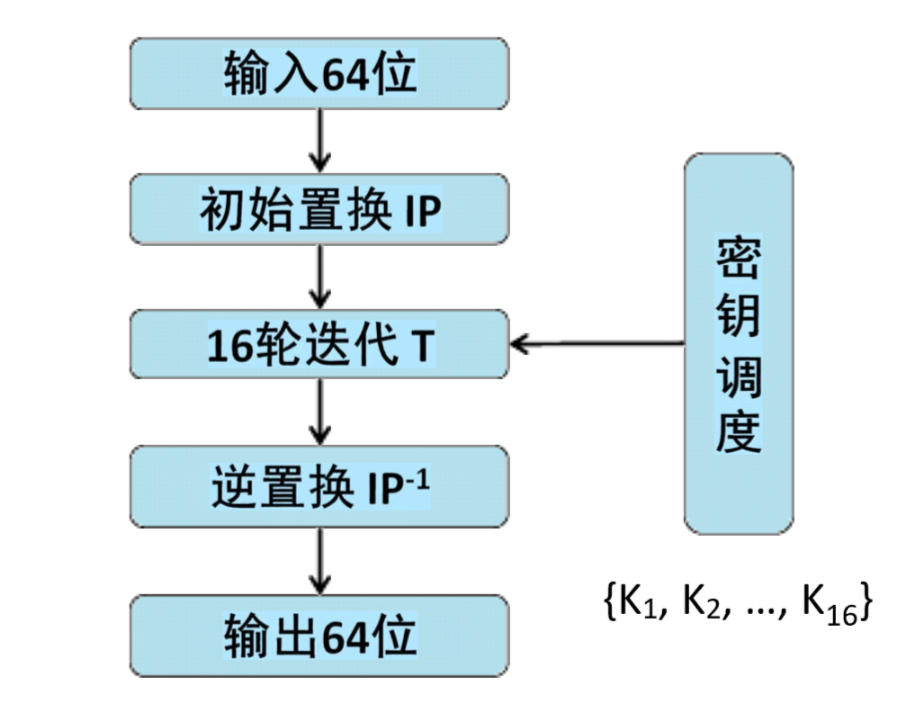
解密过程

 

2.2 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。



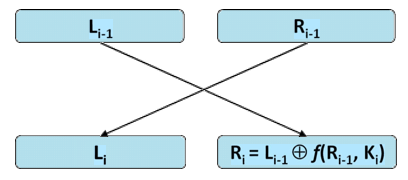
1. 输入64bit明文
2. 初始置换IP

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

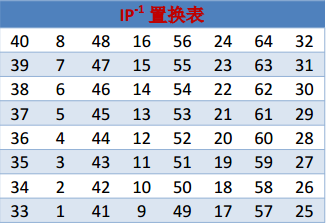
16次迭代后得到L16R16

左右交换输出R16L16

1. 逆置换IP-1

对迭代T输出的二进制串R16L16使用初始置换的逆置换IP-1得到密文C，

即：C = IP-1 (R16L16).





注1： 迭代T中使用Feistel轮函数 f(Ri-1, Ki)详解

1. 将长度为32位的串 Ri-1作 E-扩展，成为48位的串 E(Ri-1)

E-扩展规则：



1. 将 E(Ri-1) 和长度为*48*位的子密钥 Ki 作48位二进制串按位异或运算，Ki 由密钥 K 生成
2. 将 (2)得到的结果平均分成8个分组 *(*每个分组长度6位*)*，分别经过8个不同的 *S-*盒进行 6-4 转换，得到8个长度分别为4位的分组

二进制6-4 转换机制：S-盒

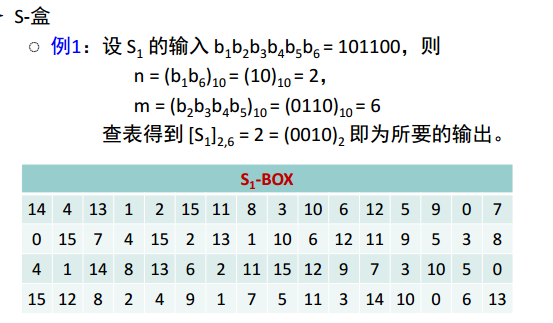
S-盒是一类选择函数，用于二进制6-4转换。Feistel 轮函数使用8个S-盒S1, …, S8，每个S-盒是一个4行(编号0-3)、16 列(编号0-15)的表，表中元素是一个4位二进制数的十进制表示，取值在0-15之间。

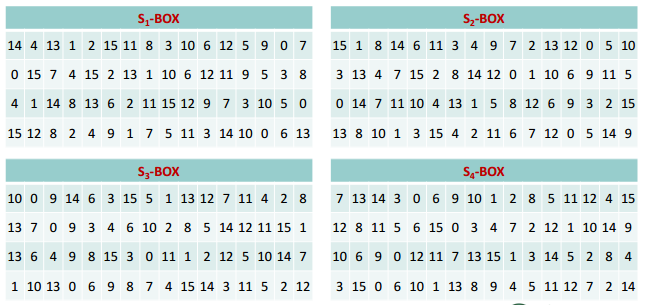
设Si 的6位输入为b1b2b3b4b5b6，则:

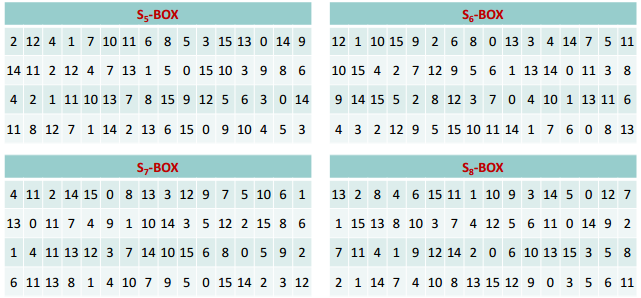
n = (b1b6)10 确定行号

m = (b2b3b4b5)10 确定列号

[Si]n,m 元素的值的二进制形式即为所要的Si的输出





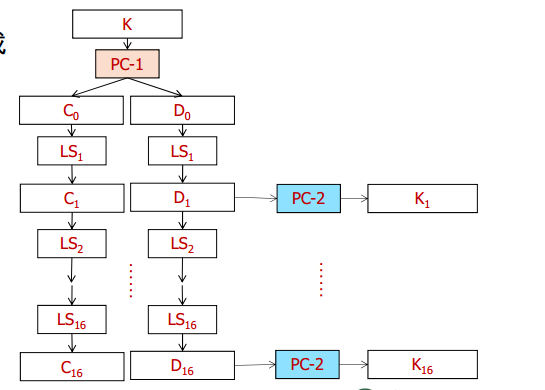


1. 将 (3) 得到的分组结果合并得到长度为32位的串
2. 将 (4) 的结果经过 P*-*置换，得到轮函数 f(Ri-1, Ki)的最终结果

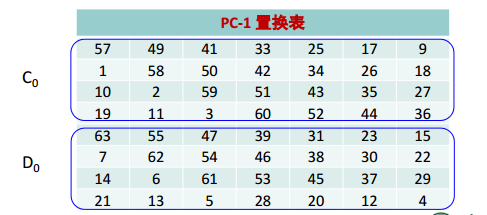


注2：迭代T中Feistel轮函数 f(Ri-1, Ki)子密钥Ki生成

子密钥生成过程根据给定的64位密钥K生成Feistel 轮函数的每轮中使用的子密钥Ki



1. 对K的56个非校验位实行置换PC-1，得到C0D0，其中C0 和D0 分别由PC-1置换后的前28位和后28位组成。i = 1

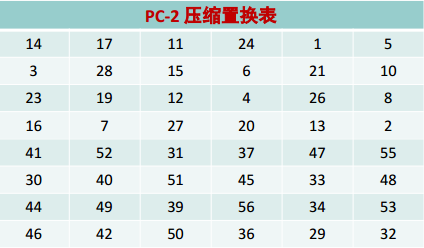


1. 计算Ci = LSi(Ci-1) 和Di = LSi(Di-1)

当i =1, 2, 9, 16时，LSi (A)表示将二进制串A循环左移一个位置；否则循环左移两个位置。

1. 对56位的CiDi 实行PC-2压缩置换，得到48位的Ki。i = i+1。

PC-2压缩置换：从56位的CiDi 中去掉第9, 18, 22, 25, 35, 38,43, 54位，将剩下的48位按照PC-2置换表作置换，得到Ki。



1. 如果已经得到K16，密钥调度过程结束；否则转(2)。
2. 模块分解
3. 数据结构
4. 类C语言算法过程