> 姓名：佘崧林
>
> 学号：1613574

# DES

## 实验目的

通过用 DES 算法对实际的数据进行加密和解密，来深刻了解 DES 的运行原理。

## 实验原理

### 整体流程

明文分组长度为 64 位，秘钥长度为 56 位，最终形成的密文长度为 64 位。如果明文长度不足 64 位，即将其扩展为 64 位(如补零等方法)。

具体加密过程: (1) 将输入的数据进行初始置换 IP ，即将明文 M 中数据的排列顺序按一定的规则重新排列，生成新 的数据序列，以打乱原来的次序; (2) 将变换后的数据平分成左右两部分，左边记为 L0 ，右边记为 R0 ，然后对 R0 实行在子密钥(由加密密钥产生)控制下的变换 f ，结果记为 f(R0，K1) ，再与 L0 做逐位异或运算，其结果记 为 R1，R0 则作为下一轮的 L1;(3)如此循环16轮，最后得到 L16、R16;(4)再对 L16、R16 实行逆初始置 换 IP-1 ，即可得到加密数据。解密过程与此类似，不同之处仅在于子密钥的使用顺序正好相反;

### 基本函数

DES 的加密算法包括 3 个基本函数:

1. 初始置换：它的作用是把输入的 64 位数据块的排列顺序打乱，每位数据按照下面的置换规则重新排列，即将第 58 位换到第一 位，第 50 位换到第 2 位，...，依次类推。置换后的 64 位输出分为 L0 、 R0 (左、右)两部分，每部分分别为 32 位。

   ```
   58 50 42 34 26 18 10 02    60 52 44 36 28 20 12 04
   62 54 46 38 30 22 14 06    64 56 48 40 32 24 16 08
   57 49 41 33 25 17 09 01    59 51 43 35 27 19 11 03
   61 53 45 37 29 21 13 05    63 55 47 39 31 23 15 07
   ```

   R0 和 K1 经过 f(R0，K1) 变换后的输出结果，再和 L0 进行异或运算，输出结果位 R1 ， R0 则赋给 L1 。 L1 和 R1 同样再做类似运算生成 L2 和 R2 ，...，经过 16 次运算后生成 L16 和 R16 。

2. f 函数：f 函数是多个置换函数和替代函数的组合函数，它将 32 位比特的输入变换为 32 位的输出。Ri 经过扩展运算 E 变换后 扩展为 48 位的 E(Ri), 与 Ki+1 进行异或运算后输出的结果分成 8 组，每组 6 比特。每一组再经过一个 S 盒(共 8 个 S 盒)运算转换为 4 位，8 个 4 位合并为 32 位后再经过 P 变换输出为 32 位 `f (Ri, Ki+1)`。其中，扩展运算 E 与置换 P 主要作用是增加算法的扩散效果。

3. 逆初始置换 `IP-1`：它将 L16 和 R16 作为输入，进行逆初始置换得到密文输出。逆初始置换是初始置换的逆运算，置换规则如下所列：

```
40, 8, 48, 16, 56, 24, 64, 32, 39, 7, 47, 15, 55, 23, 63, 31
38, 6, 46, 14, 54, 22, 62, 30, 37, 5, 45, 13, 53, 21, 61, 29
36, 4, 44, 12, 52, 20, 60, 28, 35, 3, 43, 11, 51, 19, 59, 27
34, 2, 42, 10, 50, 18, 58, 26, 33, 1, 41, 9,  49, 17, 57, 25
```

4. 子密钥生成：DES 的加密算法中除了上面介绍的 3 个基本函数，还有一个非常重要的功能模块，即子密钥的生成模块。输入的初 始密钥值为 64 位，但 DES 算法规定，其中第 8、16、…、64 位为奇偶校验位，不参与 DES 的运算。所以，实际可 用位数只有 56 位，经过缩小选择位表 1(表 1-2)即密钥置换 PC-1 的变换后，初始密钥的位数由 64 位变成了 56 位，将其平分为两部分 C0 ， D0 。然后分别进行第一次循环左移，得到 C1 和 D1 ，将 C1 (28 位)、 D1 (28 位) 合并后得到 56 位的输出结果，再经过压缩置换 PC-2(表 1-3)，从而得到了密钥 K1 (48 位)。依次类推，便可得 到 K2 、…、 K16 。需要注意的是，16 次循环左移对应的左移位数要依据表 1-1 的规则进行。

# 实验要求

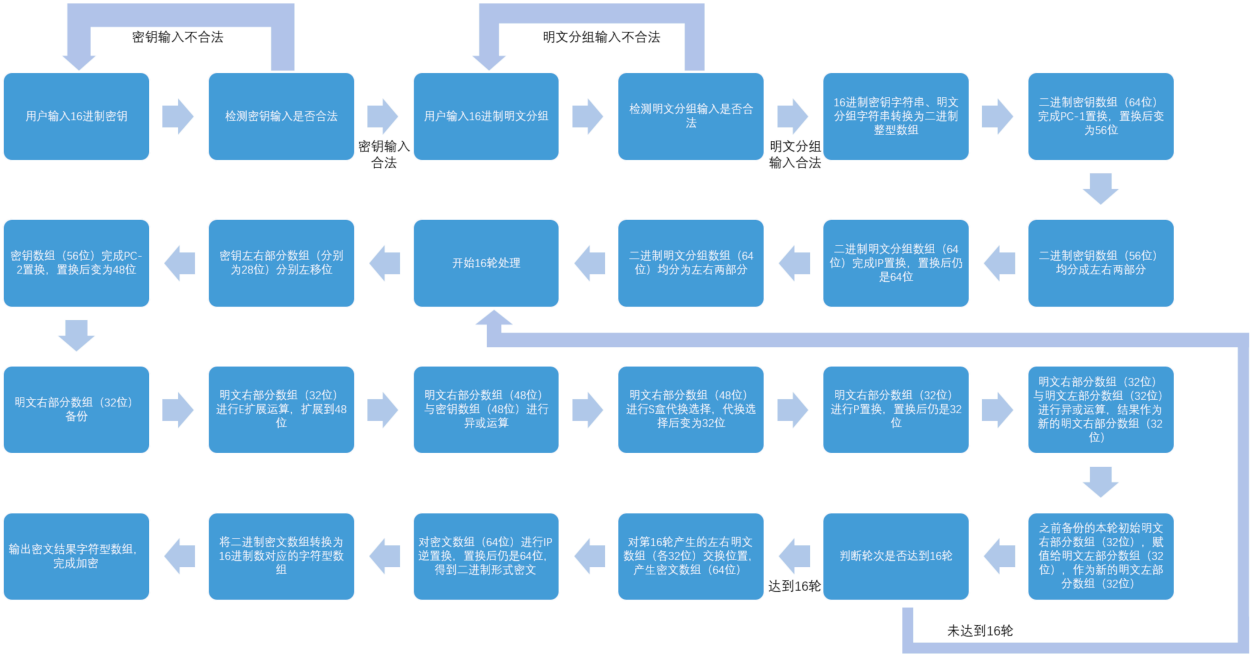
DES 实现程序的总体设计:在第一步的基础上，对整个 DES 加密函数的实现进行总体设计，考虑数据的存储格式， 参数的传递格式，程序实现的总体层次等，画出程序实现的流程图。

在总体设计完成后，开始具体的编码，在编码过程中，注意要尽量使用高效的编码方式。

对 DES 的密文进行雪崩效应检验。即固定密钥，仅改变明文中的一位，统计密文改变的位数;固定明文，仅改变密钥 中的一位，统计密文改变的位数。

# 实验内容

## 流程图



## 实验结果

```
$ ./bin/lab2
InitKey:  0001000000110001011011100000001010001100100011110011101101001010
PlainText:  0000000000000000000000000000000000000000000000000000000000000000
CipherText: 1000001011011100101110101111101111011110101010110110011000000010
CalcCipher: 1000001011011100101110101111101111011110101010110110011000000010
Avalance test: (Average 28.1719)
0 31 33 30 27 30 33 23 0 32 35 33 24 38 36 25 0 36 31 35 42 39 34 35 0 35 26 34
34 25 29 31 0 33 36 35 32 32 30 34 0 36 31 32 40 26 39 34 0 37 26 34 36 29 34
32 0 27 26 34 29 36 29 28
----------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  1001010111111000101001011110010111011101001100011101100100000000
CipherText: 1000000000000000000000000000000000000000000000000000000000000000
CalcCipher: 1000000000000000000000000000000000000000000000000000000000000000
Avalance test: (Average 28.9844)
0 31 37 36 31 30 32 28 0 35 29 34 32 35 33 36 0 33 31 30 36 31 26 31 0 35 30 34
33 25 28 35 0 36 30 33 31 33 30 35 0 34 32 36 33 28 38 36 0 36 29 32 32 38 34
39 0 35 34 37 40 40 34 33
----------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  1101110101111111000100100001110010100101000000101010110000011001
CipherText: 0100000000000000000000000000000000000000000000000000000000000000
CalcCipher: 0100000000000000000000000000000000000000000000000000000000000000
Avalance test: (Average 27.7188)
0 40 33 30 30 28 31 30 0 29 39 35 30 34 33 29 0 36 29 32 30 32 41 37 0 29 24 28
32 28 35 31 0 26 27 33 30 31 30 34 0 30 40 29 33 29 34 33 0 29 33 24 34 31 30
32 0 34 38 31 32 29 33 30
----------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  0010111010000110010100110001000001001111001110000011010011101010
CipherText: 0010000000000000000000000000000000000000000000000000000000000000
CalcCipher: 0010000000000000000000000000000000000000000000000000000000000000
Avalance test: (Average 28.0156)
0 34 28 29 39 29 35 33 0 27 32 24 31 36 35 36 0 33 32 38 29 29 28 29 0 33 27 23
38 36 37 28 0 34 30 25 30 35 32 37 0 30 29 35 32 26 29 38 0 34 37 35 30 33 35
31 0 35 29 32 32 34 33 33
----------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  0100101111010011100010001111111101101100110110000001110101001111
CipherText: 0001000000000000000000000000000000000000000000000000000000000000
CalcCipher: 0001000000000000000000000000000000000000000000000000000000000000
Avalance test: (Average 27.3438)
0 31 32 32 25 29 33 34 0 34 26 27 34 23 28 38 0 38 27 32 26 29 28 27 0 29 31 28
26 32 37 32 0 26 35 27 39 30 34 37 0 28 38 36 33 35 37 40 0 30 33 34 29 34 27
31 0 26 27 27 35 34 26 34
----------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
```

```
PlainText:  0010000010111001111001110110011111011001011111011000101000101011
0
CipherText: 0000100000000000000000000000000000000000000000000000000000000000
0
CalcCipher: 0000100000000000000000000000000000000000000000000000000000000000
0
Avalance test: (Average 28.75)
0 30 34 35 27 30 32 31 0 43 35 35 34 31 40 36 0 35 29 34 33 31 37 31 0 33 37 36
36 28 31 31 0 38 29 30 39 36 33 31 0 40 31 29 30 33 25 33 0 29 32 30 29 37 29
36 0 31 34 34 30 38 26 33
----------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  0101010101010111100100111000000011010111011100010011100011101111
CipherText: 0000010000000000000000000000000000000000000000000000000000000000
0
CalcCipher: 0000010000000000000000000000000000000000000000000000000000000000
0
Avalance test: (Average 27.7656)
0 31 27 31 37 33 31 36 0 31 31 35 34 25 25 35 0 30 29 31 29 35 33 27 0 27 30 33
33 27 29 34 0 29 29 32 29 41 30 32 0 33 35 31 26 29 32 35 0 30 30 35 33 36 30
29 0 32 35 31 41 32 32 39
----------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  0110110011000101110111101111101010101111000010001010001001011111
CipherText: 0000001000000000000000000000000000000000000000000000000000000000
0
CalcCipher: 0000001000000000000000000000000000000000000000000000000000000000
0
Avalance test: (Average 27.6406)
0 29 32 40 32 29 34 32 0 34 24 33 30 30 29 34 0 37 27 35 32 27 31 33 0 29 25 33
37 36 34 34 0 32 29 29 28 38 28 29 0 27 33 29 35 32 35 35 0 34 31 27 38 27 32
35 0 35 22 34 26 31 34 32
----------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  0000110110011111001001111001101110100101110110000111001001100000
CipherText: 0000000100000000000000000000000000000000000000000000000000000000
0
CalcCipher: 0000000100000000000000000000000000000000000000000000000000000000
0
Avalance test: (Average 27.9219)
0 36 26 27 39 32 30 28 0 37 26 27 38 31 33 22 0 36 28 25 41 24 31 28 0 34 39 32
30 28 27 33 0 34 22 34 29 32 38 37 0 28 32 38 38 35 34 37 0 34 39 35 28 30 32
34 0 38 30 28 26 31 31 35
----------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  1101100100000011000110110000001001110001101111010101101000001010
CipherText: 0000000010000000000000000000000000000000000000000000000000000000
0
CalcCipher: 0000000010000000000000000000000000000000000000000000000000000000
0
Avalance test: (Average 27.2656)
0 36 24 37 34 28 34 33 0 28 33 32 32 35 30 35 0 27 32 33 32 35 30 31 0 35 30 28
28 25 33 33 0 28 27 27 39 23 32 29 0 38 29 29 32 30 30 30 0 33 25 35 33 37 30
30 0 32 25 37 31 28 30 33
----------------------------------------------------------------
InitKey:  0001000000110001011011100000001010001100100011110011101101001010
PlainText:  1000001011011100101110101111101111011110101010110110011000000010
CipherText: 0000000000000000000000000000000000000000000000000000000000000000
0
CalcPlain:  0110000111110010010110011110010111100001010110011111011000010001
Avalance test: (Average 27.5469)
```

```
0 41 27 22 29 29 29 33 0 25 34 29 34 32 38 30 0 32 36 27 36 29 32 35 0 38 26 39
27 28 27 34 0 34 31 34 32 32 28 29 0 26 34 35 28 34 31 26 0 22 30 30 42 25 34
35 0 38 38 31 24 41 29 32
----------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  1000000000000000000000000000000000000000000000000000000000000000
CipherText: 1001010111111000101001011110010111011101001100011101100100000000
CalcPlain:  1000000000000000000000000000000000000000000000000000000000000000
Avalance test: (Average 28.6875)
0 31 35 23 43 38 36 30 0 35 28 29 31 27 29 33 0 31 37 37 30 33 32 32 0 33 33 39
32 32 35 31 0 26 36 31 33 33 34 35 0 38 36 32 27 37 27 29 0 33 30 34 42 33 37
33 0 35 33 37 29 35 29 27
----------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  0100000000000000000000000000000000000000000000000000000000000000
CipherText: 1101110101111111000100100001110010100101000000010101011000011001
CalcPlain:  0100000000000000000000000000000000000000000000000000000000000000
Avalance test: (Average 27.7031)
0 33 26 24 36 27 24 35 0 29 32 30 38 32 33 29 0 36 36 37 34 34 28 30 0 38 27 28
36 35 38 34 0 30 29 29 37 35 31 36 0 36 32 27 29 34 34 29 0 25 32 36 28 26 33
30 0 38 36 33 32 27 20 30
----------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  0010000000000000000000000000000000000000000000000000000000000000
CipherText: 0010111010000110010100110001000001001111001110000011010011101010
CalcPlain:  0010000000000000000000000000000000000000000000000000000000000000
Avalance test: (Average 28.3281)
0 28 31 27 34 36 32 35 0 33 32 38 26 39 34 34 0 30 25 24 30 32 27 27 0 34 29 29
34 39 36 40 0 31 29 35 26 38 29 33 0 36 37 34 26 39 27 31 0 33 32 34 34 38 32
29 0 39 32 33 37 33 31 30
----------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  0001000000000000000000000000000000000000000000000000000000000000
CipherText: 0100101111010011100010001111111101101100110110000001110101001111
CalcPlain:  0001000000000000000000000000000000000000000000000000000000000000
Avalance test: (Average 28.6875)
0 35 37 32 41 35 33 38 0 29 32 28 37 37 31 31 0 40 41 29 33 35 31 23 0 34 37 36
29 25 34 27 0 34 38 30 28 32 27 26 0 38 32 34 36 35 34 31 0 29 32 33 35 38 35
30 0 32 28 33 38 32 30 26
----------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  0000100000000000000000000000000000000000000000000000000000000000
CipherText: 0010000010111001111001110110011111011001011111011000101000101011 0
CalcPlain:  0000100000000000000000000000000000000000000000000000000000000000
Avalance test: (Average 27.8125)
0 26 32 37 35 40 35 37 0 39 35 30 32 30 27 30 0 27 23 30 32 30 31 32 0 37 33 33
38 28 29 28 0 32 37 29 35 29 29 31 0 30 30 34 31 29 27 36 0 29 31 29 29 36 40
31 0 32 29 35 35 31 30 28
----------------------------------------------------------------
```

```
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  0000010000000000000000000000000000000000000000000000000000000000
CipherText: 0101010101011111001001110000000110101110111000100111000111101111
CalcPlain:  0000010000000000000000000000000000000000000000000000000000000000
Avalance test: (Average 27.9219)
0 30 30 39 33 31 29 29 0 30 25 36 35 34 35 37 0 35 30 25 32 35 35 33 0 28 41 32
41 29 35 29 0 25 32 29 35 30 30 31 0 37 31 31 34 32 28 35 0 26 35 25 31 32 39
36 0 30 32 34 29 27 27 31
----------------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  0000010000000000000000000000000000000000000000000000000000000000
CipherText: 0110110011000101110111101111101010101111000010001010001001011111
CalcPlain:  0000010000000000000000000000000000000000000000000000000000000000
Avalance test: (Average 27.7656)
0 35 31 34 32 32 23 35 0 43 31 34 33 28 27 37 0 24 33 34 33 30 39 24 0 31 22 33
31 27 33 36 0 32 31 26 33 24 33 31 0 31 29 28 35 36 35 25 0 27 33 38 31 27 29
37 0 34 30 37 40 31 31 38
----------------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  0000000100000000000000000000000000000000000000000000000000000000
CipherText: 0000110110011111001001111001101110100101110110000111001001100000
CalcPlain:  0000000100000000000000000000000000000000000000000000000000000000
Avalance test: (Average 27.6562)
0 32 39 30 27 34 30 23 0 30 34 30 36 35 32 29 0 36 33 31 32 25 37 27 0 32 40 33
31 33 25 31 0 23 23 36 27 25 30 30 0 33 31 32 32 35 38 37 0 40 31 26 28 32 34
29 0 36 29 30 32 40 30 34
----------------------------------------------------------------------
InitKey:  0000000100000001000000010000000100000001000000010000000100000001
PlainText:  0000000010000000000000000000000000000000000000000000000000000000
CipherText: 1101100100000011000110110000001001110001101111010101101000001010
CalcPlain:  0000000010000000000000000000000000000000000000000000000000000000
Avalance test: (Average 27.4531)
0 32 27 33 38 28 32 29 0 33 34 36 24 30 26 28 0 36 31 31 32 30 28 34 0 28 25 32
33 30 35 29 0 32 39 33 30 28 30 32 0 31 33 32 36 30 30 27 0 27 39 27 38 29 31
33 0 35 35 31 36 27 33 29
----------------------------------------------------------------------
```