密码学综合设计实验

实验 2：DES 加密解密算法实现

学号：031803108

姓名：苏煜程

2019 年　9 月　29 日

一、 实验要求

1.实现 Feistel 密码结构（64bit 分组长度）

a) 输入 64bit 明文分组，轮数 Round，轮函数 F，子密钥数组 K

b) 输出 64bit 密文分组

c) 提示：如果是 C 语言实现的话，轮函数用函数指针

2.DES 算法实现

d) 初始置换实现

e) 子密钥生成实现

f) DES 轮函数实现

g) 逆初始置换实现

h) 加密分组实现

i) 解密分组实现

3.附加内容：

j) 自定义轮函数，实现一个基于 Feistel 结构的加密解密自定义算法。

k) 比如自定义轮函数：F(W,K)=(1<<W)+K，即 W 先循环左移 1 位再与 K 异或。

l) 用电码本模式对文件进行加密和解密。

二、 实验原理

1. 所需参数

key：8 个字节共 64 位的工作密钥

data：8 个字节共 64 位的需要被加密或被解密的数据

mode：DES 工作方式，加密或者解密

2. 初始置换

DES 算法使用 64 位的密钥 key 将 64 位的明文输入块变为 64 位的密文输出块，并把输出块分为 L0、R0 两部分，每部分均为 32 位。初始置换规则如下：

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

3. 轮结构

将 64 比特的轮输入分为 32 比特的左、右两半，分别记为 L 和 R。和 Feistel 网络一样，每轮变换可由以下公式表示：

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

K_i是向第 N 层输入的 48 位的秘钥， F 是以R_{i-1}和K_i为变量的输出 32 位的函数。

4. 函数 F

A. 扩展置换 E

通过扩展置换 E，数据的右半部分 R 从 32 位扩展到 48 位。
扩展置换 E 规则如下：

```
32,01,02,03,04,05,
04,05,06,07,08,09,
08,09,10,11,12,13,
12,13,14,15,16,17,
16,17,18,19,20,21,
20,21,22,23,24,25,
24,25,26,27,28,29,
28,29,30,31,32,01
```

B. S-盒代替

R 扩展置换之后与子秘钥K_i异或以后的结果作为输入块进行 S 盒代替运算，功能是把 48 比特数据变为 32 比特。然后再通过一个 S 盒，产生 32 比特的输出。

代替运算由 8 个不同的代替盒(S 盒)完成。每个 S 盒有 6 位输入，4 位输出。

C. P-盒置换

S-盒代替运算，每一盒得到 4 位，8 盒共得到 32 位输出。这 32 位输出作为 P 盒置换的输入块。

P 盒定义如下：

```
16,07,20,21,
29,12,28,17,
01,15,23,26,
05,18,31,10,
02,08,24,14,
32,27,03,09,
19,13,30,06,
22,11,04,25
```

5. 子密钥的产生

DES 算法由 64 位秘钥产生 16 轮的 48 位子秘钥。在每一轮的迭代过程中，使用不同的子秘钥。

A. 置换选择 1

将 64 位密钥通过缩小选择置换表（PC-1）的变换变成 56 位，然后将置换后的 56 位密钥分为 C0,D0 两半。PC-1 的定义如下：

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

B. 置换选择 2

在第 i 轮分别对C_{i-1}和D_{i-1}进行左循环移位，循环左移每轮移动的位数如下：

每轮移动的位数表

轮	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
位数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

移位后的结果作为下一轮求子密钥的输入，同时也作为置换选择 2 的输入。通过置换选择 2 产生的 48 比特的K_i，即为本轮的子密钥，作为函数 F 的输入。其中置换选择 2 的定义如下：

```
14, 17, 11, 24,  1,  5,
 3, 28, 15,  6, 21, 10,
23, 19, 12,  4, 26,  8,
16,  7, 27, 20, 13,  2,
41, 52, 31, 37, 47, 55,
30, 40, 51, 45, 33, 48,
44, 49, 39, 56, 34, 53,
46, 42, 50, 36, 29, 32
```

6. 解密

和 Feistel 密码一样，DES 的解密和加密使用同一算法，但子密钥使用的顺序相反。