密码学综合设计实验

实验2：DES加密解密算法实现

学号：\_\_\_\_\_\_ 031803134\_

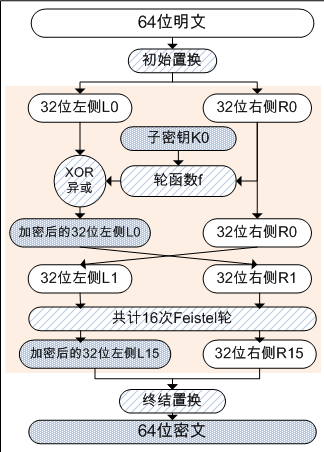
姓名：\_\_\_\_\_\_\_郑晟\_\_\_\_\_\_\_\_\_

19年 9月 28日

1. 实验要求
2. 实现Feistel密码结构（64bit分组长度）
   1. 输入64bit明文分组，轮数Round, 轮函数F, 子密钥数组K
   2. 输出64bit密文分组
   3. 提示：如果是C语言实现的话，轮函数用函数指针
3. DES算法实现
   1. 初始置换实现
   2. 子密钥生成实现
   3. DES轮函数实现
   4. 逆初始置换实现
   5. 加密分组实现
   6. 解密分组实现
4. 实验原理

DES对64位(bit)的明文分组M进行操作，M经过一个初始置换IP，置换成m0。将m0明文分成左半部分和右半部分m0 = (L0，R0)，各32位长。然后进行16轮完全相同的运算（迭代），这些运算被称为函数f，在每一轮运算过程中数据与相应的密钥结合。在每一轮中，密钥位移位，然后再从密钥的56位中选出48位。通过一个扩展置换将数据的右半部分扩展成48位，并通过一个异或操作替代成新的48位数据，再将其压缩置换成32位。这四步运算构成了函数f。然后，通过另一个异或运算，函数f的输出与左半部分结合，其结果成为新的右半部分，原来的右半部分成为新的左半部分。将该操作重复16次。经过16轮迭代后，左，右半部分合在一起经过一个末置换（数据整理），这样就完成了加密过程。

具体流程图：



1. 软件系统设计

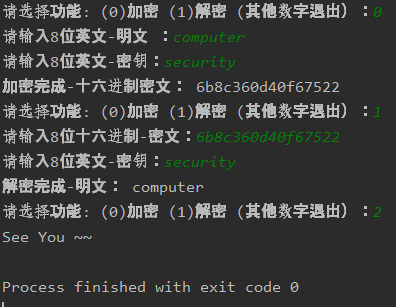
该系统有加密8位英文字符为16位16进制密文及解密16位16进制密文为8位英文字符明文的功能及其实现的函数有：子密钥生成函数，IP置换函数，E拓展置换函数，S代换函数，P变换函数，逆IP置换函数，轮函数，字符转换等函数

1. 重要的实现细节



利用python的切片将IP置换后的64位text分为左32位和右32位，在二进制数值中可能出现的第一位的0被省略的情况进行了补零，整体代码简洁。

1. 实现效果



1. 总结

该系统具有一定交互性，可进行英文字符加密，实用性较单纯16进制数据加解密更高，代码结构简洁易懂。如有需要可对轮函数进行更改，实现自定义加密。