南京信息工程大学 实验（实习）报告

实验名称 RSA加密 实验（实习）日期 2023/11/8 指导教师 高光勇

系 计算机 专业 奇安信 年级 2021 班次 1 姓名 朱宸扬 学号 202183760012

**一、实验目的**

**理解置换密码的加密方式，熟悉C语言文件操作。**

**二、实验要求**

**编程实现数据加密标准DES中的初始置换，用其加密64比特的明文。**

**三、实验内容 (要求写出算法原理、实验核心代码及运行结果)**

key = [1, 63, 40, 4, 55, 37, 44, 54, 62, 57, 56, 35, 6, 58, 46, 3, 7, 9, 50, 27, 32, 38, 43, 60, 16, 31, 51, 47, 64, 52, 2, 14, 30, 42, 17, 48, 59, 33, 45, 18, 26, 19, 24, 8, 28, 34, 36, 11, 5, 53, 41, 49, 12, 21, 61, 22, 15, 29, 20, 13, 25, 39, 10, 23]  
  
file\_path = "1.txt"   
try:  
 with open(file\_path, "r") as file:  
 # 读取整个文件内容  
 content = file.read()  
 print("文件内容:")  
 print(content)  
  
except FileNotFoundError:  
 print(f"文件 '{file\_path}' 未找到")  
  
  
new\_list = []  
for i in range(64):  
  
 new\_list.append(content[key[i]-1])  
  
print(new\_list)

**文件内容:**

**1101010101001110010000101001110111001111101010101101011010110110**

**置换后的表:**

**['1', '1', '1', '1', '1', '1', '0', '1', '1', '1', '0', '0', '1', '0', '0', '0', '0', '0', '1', '0', '1', '1', '1', '1', '0', '0', '0', '1', '0', '1', '1', '1', '1', '0', '0', '0', '1', '1', '1', '1', '0', '0', '0', '1', '1', '1', '0', '0', '0', '0', '1', '1', '0', '0', '0', '0', '1', '1', '0', '1', '1', '1', '1', '1']**

**四、实验心得**

原值按照置换表进入新表对应位置