****

**Python程序设计**

**实验报告**

**实验名称：设计凯撒密码加密和解密的程序**

**姓名：孙文秀**

**学号：22920192204059**

**专业：人工智能**

**实验日期：2021.03.25**

# 实验目的

1. 学习掌握凯撒密码的加密解密程序的相关原理与编写
2. 了解针对英文字符的凯撒密码的加密和解密程序的缺陷性，并且在此基础上进行改进

# **实验内容**

设计实现针对中文的凯撒密码的加密和解密程序

# **程序设计思路**

1、利用ord()函数将输入的中文字符转化为对应的ASCII值；利用chr()函数将相应的ASCII值转换成中文字符

2、根据**产生的随机数，字符串的长度以及字符所在位置三个要素**构成字符串中某字符的ASCII值的**改变量**，从而修改当前字符的ASCII值进行加密

1. **随机数传递给解密程序的方法**：加密后的字符串增加一元素，该元素的ASCII值只比前一个元素的ASCII值多了随机数的大小

# **程序源代码**

1. 加密程序源代码：

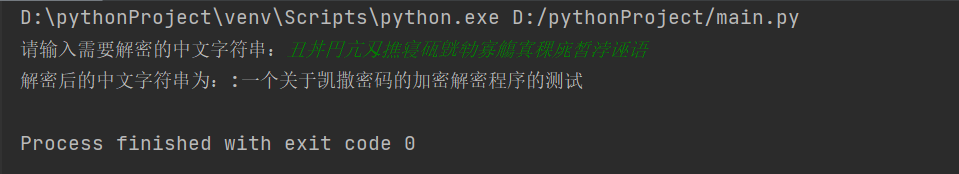
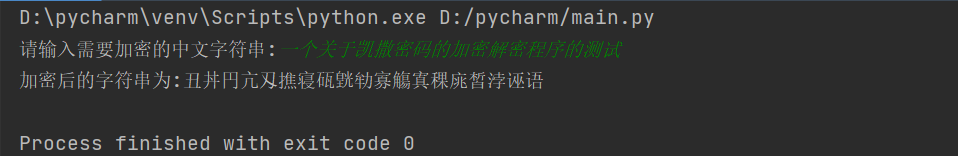
import random  
  
def main():  
 str1=input("请输入需要加密的中文字符串:")  
 rand=random.randint(1,100)  
 l=len(str1)  
 key=l-rand  
 str2=""  
 i=0  
 while i<l:  
 str2+=chr(ord(str1[i])+key+i%11)  
 i+=1  
 str2+=chr(ord(str1[l-1])+key+(l-1)%11+rand)  
 print("加密后的字符串为",str2,sep=':')  
if \_\_name\_\_=='\_\_main\_\_':  
 main()

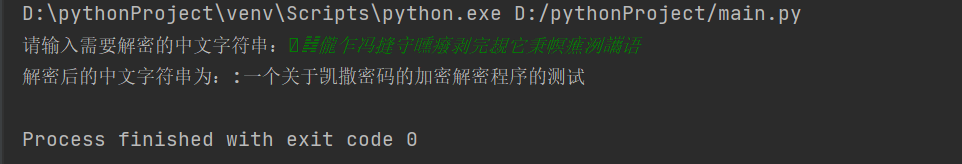
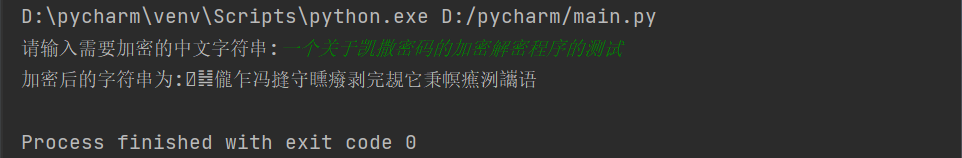
1. 解密程序源代码：

def main():  
 str1=input("请输入需要解密的中文字符串：")  
 l=len(str1)-1 #l表示原来需要加密的字符串的长度  
 rand=ord(str1[l])-ord(str1[l-1])  
 key=l-rand  
 str2=""  
 i=0  
 while i<l:  
 str2+=chr(ord(str1[i])-key-i%11)  
 i+=1  
 print("解密后的中文字符串为：",str2,sep=':')  
  
if \_\_name\_\_=='\_\_main\_\_':  
 main()

# **实验结果**

相同的字符串进行两次加密和解密操作，程序运行结果如下：





由以上结果可知，**相同的字符串两次加密后的字符串不相同**

# **实验总结**

实验过程中遇到的问题及解决方案：

1. 问题：起初的偏移量仅跟字符串的长度有关，由此相同的字符串加密后的字符串是相同的，安全性差。

解决方案：引入产生随机数的函数，随机数不固定，相同字符串加密分别两次加密产生的结果不同

1. 问题：初步改进后的偏移量虽然在多次的加密时偏移量不同，但是在一次加密时，整个字符串中每个字符的偏移量是相同的，可通过暴力破解密码，安全性较差

解决方案：由产生的随机数，字符串的长度以及字符所在位置三个要素构成每个字符的偏移量，则相邻几个字符的偏移量是不同的