**python语言程序设计**

**实验报告**

**实验题目：设计一个凯撒密码加密和解密程序**

**专 业：人工智能**

**姓 名：谷聪**

**学 号：22920192203945**

**实验日期**：2021/3/27

1. **实验目的**

设计实现针对中文的凯撒密码的加密和解密程序

1. **实验内容**

通过编写加密的python程序,对输入的中文语句，即明文，通过密钥进行加密生成密文。与此同时，根据密钥来编写对应的解密程序，使密文能够解密为对应的明文。

1. **实验步骤及实现代码**

设置三个txt文件，分别为original.txt（用于存储和输入原始的待加密的中文语句），secret.txt（用来存储加密后的语句）,以及document.txt（用来存放解密后，及翻译后的中文语句）。

接下来，分别用两个python程序来实现中文的加密与解密。加密程序为decode.py，通过读入明文（中文），将字符转化为Unicode码的列表。并设置密钥，为了使密钥更具有灵活性，利用随机数种子，产生随机数k，并与元素的位置之和作为字符的偏移量，即为密钥。同时为了使得保存密钥更具有灵活性，密钥的存储必定是非线性的，于是根据字符串中字符个数的奇偶性，若为奇数，则将最后元素的偏移量的平方存入字符串末尾，若为偶数，则直接将最后元素的偏移量存入字符串末尾。接下来是解密程序decode.py，通过字符串元素个数减一的奇偶性判断，对字符串末尾的元素开根号或者不变处理，再往前解密，即解密函数为减去存入的偏移量再加上相对元素位置。

代码如下：

encode.py(加密程序)：

import random                               #导入随机数模块

with open('C:/Users/86188/PYTHON/experiment/original.txt','r',*encoding* = 'UTF-8') as fr:

                                            #读取UTF-8编码的文本文件，需要给open()函数传入encoding参数

    lines = fr.readlines()                  #用于读取所有行(直到结束符 EOF)并返回列表,并返回一个列表，其中包含文件中的每一行作为列表项。

code =''.join(lines)

*list* = []                                   #定义一个空列表

ans = ''                                    #定义一个空字符串

k = random.randint(100,1000)                #k为随机数

for item in code:

*list*.append(ord(item))                  #它以一个字符作为参数,返回Unicode数值,并添加在列表末尾

i = 1

for item in *list*:

    item = item + k + i                     #(k+i) 即随机数k加上对应元素在列表中的位置(从1开始)作为该元素的偏移量

    ans = ans + chr(item)

    i = i + 1

i = i - 1

if i % 2 == 1:

    ans += chr(((k+i)\*\*2))                  #若列表元素个数为奇数,则将最后元素的偏移量再平方添加在字符串末尾

else:

    ans += chr(k+i)                         #若列表元素个数为奇数,则直接将最后元素的偏移量添加在字符串末尾

txt = open('C:/Users/86188/PYTHON/experiment/secret.txt', "w",*encoding* = 'UTF-8').write(ans)

#with open("test.txt","w") as f:

#f.write(ans), 自带文件关闭功能，不需要再写f.close()

decode.py(解密程序)：

import math

with open('C:/Users/86188/PYTHON/experiment/secret.txt','r',*encoding* = 'UTF-8') as fr:

    lines = fr.readlines()

code =''.join(lines)                        #转化为字符串

*list* = []

ans = ''

if (len(code)-1) % 2 == 1:                  #判断字符串的奇偶性

    k = math.sqrt(ord(code[-1])) - len(code) + 1

else:

    k = ord(code[-1]) - len(code) + 1

i = 1

for item in code:

    if(i == len(code)):

        break;

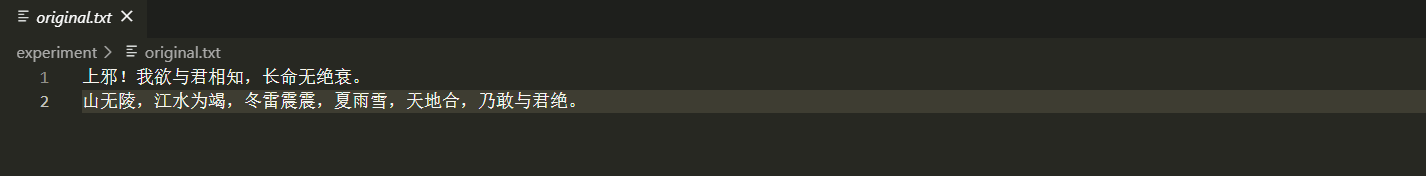
    ans += chr(*int*(ord(item)- k - i))       #解码

    i = i + 1

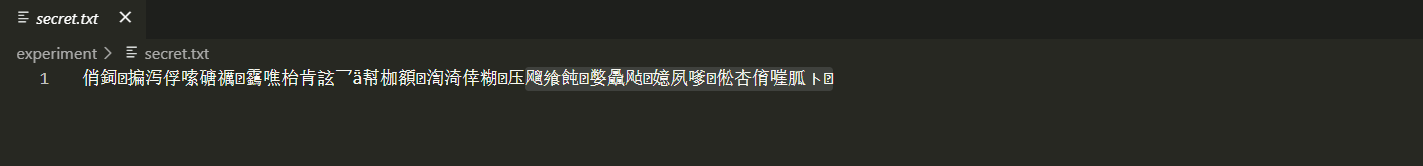
txt = open("C:/Users/86188/PYTHON/experiment/document.txt", "w",*encoding* = 'UTF-8').write(ans)

**四．实验结果**

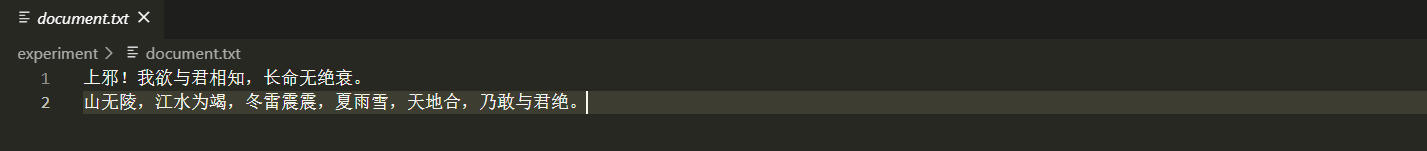
待加密的明文：



加密后的密文：



解密后的明文：



**五．实验总结**

通过本次实验，通过自己编写中文的凯撒密码加密解密程序，将所学的python知识理论应用到实践中来，加深了对python语言的掌握和学习。以及通过自己对密钥的设置，拓展了原本普通简单的凯撒密码的学习，对文件加密解密产生了浓厚的兴趣，锻炼了思维能力。