**实验报告**

1. 实验内容

利用python程序设计实现针对中文的凯撒密码的加密和解密程序，要求移位长度N不固定。

1. 算法思路

对中文片段的每个汉字取Unicode码，针对该码进行设计的数学运算得出移位长度，从而实现每个汉字的加密移位长度不一定相同，而为了加密程度足够复杂，数学运算中涉及的参数可以利用随机数来产生。我编写的程序采用将Unicode码模n再加m作为移位长度，n和m都是随机数，在文本末尾再添加m个随机字符，添加的字符中第一个的Unicode码为奇数，其余为偶数。在第m%3个字符处添加一个Unicode码为n\*n的字符。解码时，就从加密文本末尾开始扫描，直到Unicode码为奇数的字符处为止，得出m，并在第m%3个字符处取Unicode码开根号计算得到n，从而掌握解码所需的两个随机参数。

1. 代码片段

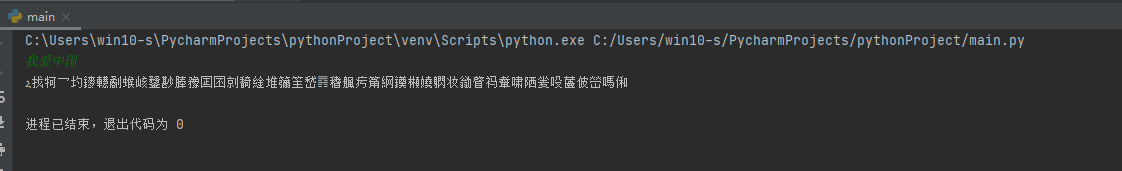
加密程序：

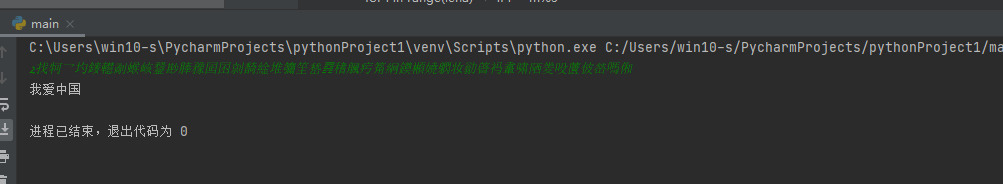
import random  
a=input()  
s=''  
n=random.randint(20,80)  
m=random.randint(10,50)  
n=n\*2-1 #随机数n需要是奇数，方便解码时逆推  
for i in a:  
 b=ord(i)  
 s=s+chr(b+b%n+m)  
s+=chr(random.randint(8000,12000)\*2+1) #在加密文本后加入一个码为奇数的字符  
for i in range(m-1): #在加密文本后再在加入m-1个随机字符  
 s+=chr(random.randint(8000,12000)\*2)  
s=list(s)  
s.insert(m%3,chr(n\*n)) #在第m%3个字符处插入一个Unicode码为n\*n的字符  
t=''.join(s)  
print(t)

解密程序：

import math  
a=input()  
a=list(a)  
i=len(a)-1  
while i>0:  
 if(ord(a[i])%2==1): #从文本末尾处开始扫描，直到其Unicode码为奇数  
 break  
 i-=1  
m=len(a)-1 #得到加密时随机数m的值  
lena=1 #文本的真实长度  
n=int(ord(a[m%3])\*\*0.5) #得到加密时随机数n的值  
t=''  
for i in range(lena):  
 if i==m%3: #第m%3个字符为干扰字符，跳过  
 continue  
 b=ord(a[i])-m #利用得到的n，m进行解码  
 if((b%n)%2==0):  
 b=int(b-(b%n)/2)  
 else:  
 b = int(b - (b % n + n) / 2)  
 t=t+chr(b)  
print(t)

1. 运行示例

加密程序：

解密程序：

1. 实验总结

本次实验是我第一次编写完整的，具有明确目的性的python程序。在了解了python各项操作的同时，也学会了如何对一段文本进行较为复杂的加密和解密，这使我受益良多。