**人工智能程序设计（python）**

**实验报告**

**实验题目：凯撒密码加密和解密程序**

**专 业：人工智能**

**姓 名：詹翁怡**

**学 号：22920192204124**

**实验日期**：**2021.3.25**

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**

凯撒加密，是一种按照正常字母序列进行移位，给定移位长度，生成新的密码的加密方式。要求设计实现一个针对中文的凯撒密码加密解密程序，其中加密和解密程序分开在两个程序中，加密的密码不能太简单地被暴力穷举法解开。

**三．实验步骤以及结果**

程序源代码如下：

**加密程序：**

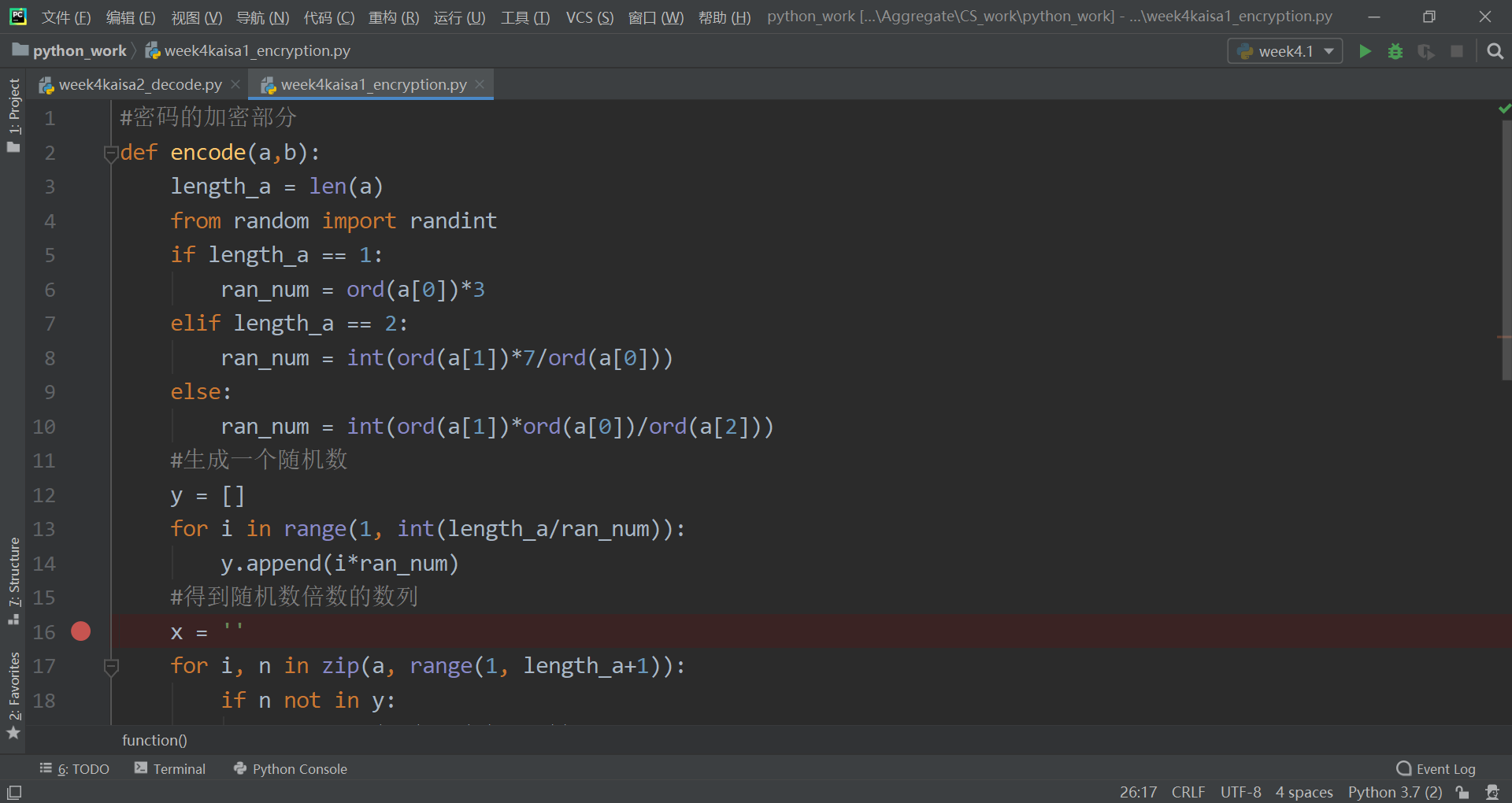
#密码的加密部分  
def encode(a,b):  
 length\_a = len(a)  
 from random import randint  
 if length\_a == 1:  
 ran\_num = ord(a[0])\*3  
 elif length\_a == 2:  
 ran\_num = int(ord(a[1])\*7/ord(a[0]))  
 else:  
 ran\_num = int(ord(a[1])\*ord(a[0])/ord(a[2]))  
 #生成一个随机数  
 y = []  
 for i in range(1, int(length\_a/ran\_num)):  
 y.append(i\*ran\_num)  
 #得到随机数倍数的数列  
 x = ''  
 for i, n in zip(a, range(1, length\_a+1)):  
 if n not in y:  
 x += chr(2\*(ord(i) + b))  
 else:  
 x += chr(ord(i)+b)  
 x += chr(ran\_num)  
 x += chr(b)  
 return x  
  
def function(a):  
 return a\*a%256  
  
  
from pyperclip import copy  
print('---加密模式---')  
a = input('请输入待加密的文本:')  
b = int(function(ord(a[0]))+function(ord(a[-1]))%ord(a[0]))  
code = encode(a,b)  
print(code)  
copy(code)  
print('文本加密成功，已复制到剪切板')

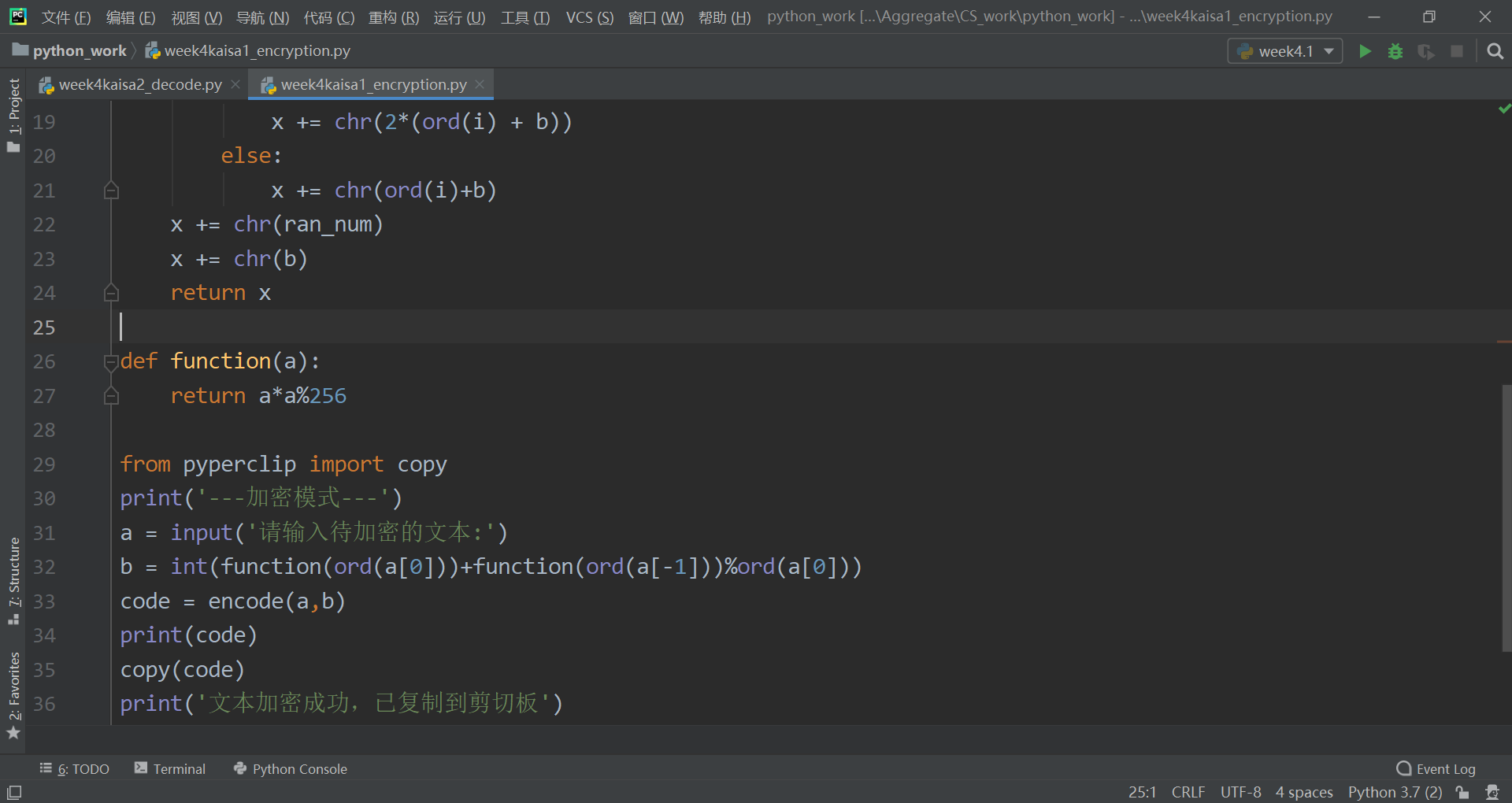
**解密程序：**

#密码的解密部分  
def decode(a):  
 b = ord(a[-1])  
 ran\_num = ord(a[-2])  
 length\_a = len(a)-2  
  
 y = []  
 for i in range(1, int(length\_a \* ran\_num)):  
 y.append(i \* ran\_num)  
 #创造随机数倍数数列  
 x = ''  
 for i,n in zip(a,range(1,length\_a+1)):  
 if n not in y:  
 x += chr(int((ord(i)/2)-b))  
 else:  
 x += chr(ord(i)-b)  
 return x  
 #解开随机数  
  
def function(a):  
 return a\*a%256  
  
print('---解密模式---')  
a = input('请输入待解密的文本:')  
#b = int(function(ord(a[0]))+function(ord(a[-1]))%ord(a[0]))  
print(decode(a), '\n')

源代码在ide中截图如下:

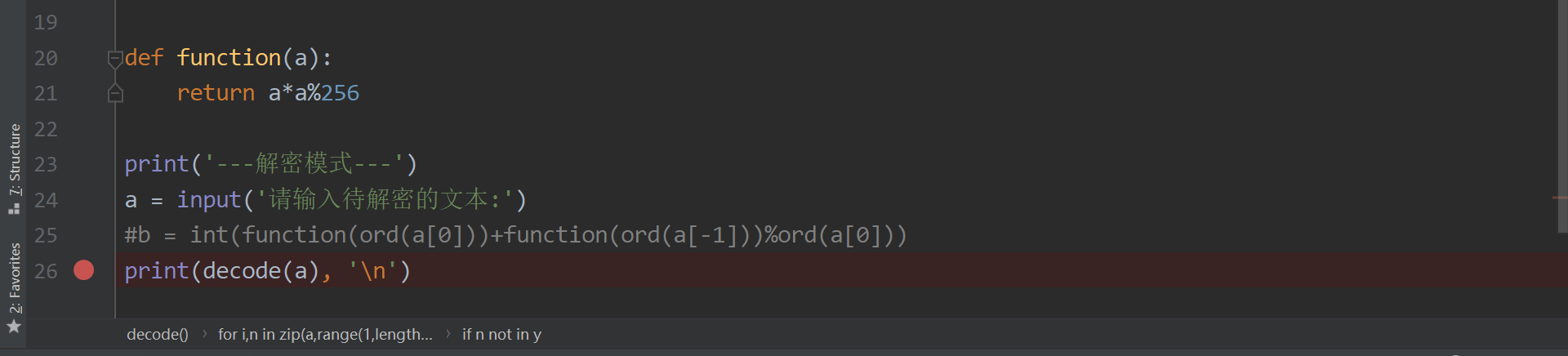
**加密程序：**





**解密程序：**





1. **数据描述：**

a：需要加密的字符串/需要解密的字符串

b：由字符串通过较复杂的函数生成的一个偏移量

length\_a：数组a的长度（不一定是字符串长度）

ran\_num：由字符串通过认为规定生成的一个伪随机数

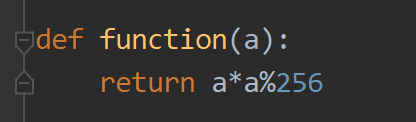
y[]：用ran\_num生成的一个随机数倍数数列

x[]：加密完毕的字符串/解密完毕的字符串（其中可能包含一些其他信息）

1. **数据预处理**

**加密函数：**

（1）function函数：一个数据处理的函数，用于简化代码



（2）对于一个输入的字符串a，取其头尾两位（如果是只有一个字的字符串，就只取这个字符本身），通过function函数及相应的取模（保证b是一个整数，以便后续找到这个数值对应的字符，传入a数组，传递给解密程序）。

（3）对于传入的字符串a，用一个较为复杂但固定的函数，算出一个伪随机值（因为字符串的长度可能不一，为防止数组越界，对长度不一的字符串做不同 处理，也可以提高伪随机数的随机性）。

（4）通过循环语句，对伪随机数做一系列规定的运算，生成一串随机数的序列，存在y中。

（5）将字符串按照改进的凯撒加密方法加密之后，把两个伪随机量b和ran\_num转换为相应字符，存入结果字符串x的末尾，传给解密程序。

**解密程序：**

1. 从传入的待解密字符串a的末尾两位反解出字符所对应的ansii码值，以获得两个伪随机量b和ran\_num。
2. 此时length\_a要及时减2，才是字符串的真正长度。
3. 通过ran\_num还原伪随机数数列y。
4. 将解密结果存入字符串x中。
5. **方法描述**

**加密程序：**

1. 接受输入，存入a中。
2. 计算出伪随机数b和ran\_num，生成伪随机数列y。
3. 对于字符串a中的各个字符，如果该字符的序号在伪随机数数列y中，就用正常的凯撒偏移，偏移量为b；如果该字符的序号不再伪随机数数列中则偏移量为2\*(ord(i) + b（可以理解成，转换一种偏移方式，这样即使被暴力破解了b，也只能解密部分文字）。
4. 解密结果依次存入x中。
5. 将两个伪随机数b和ran\_num转换成字符，存入x的结尾。
6. 通过copy函数，将转换过后的字符串复制到剪切板。

**解密程序：**

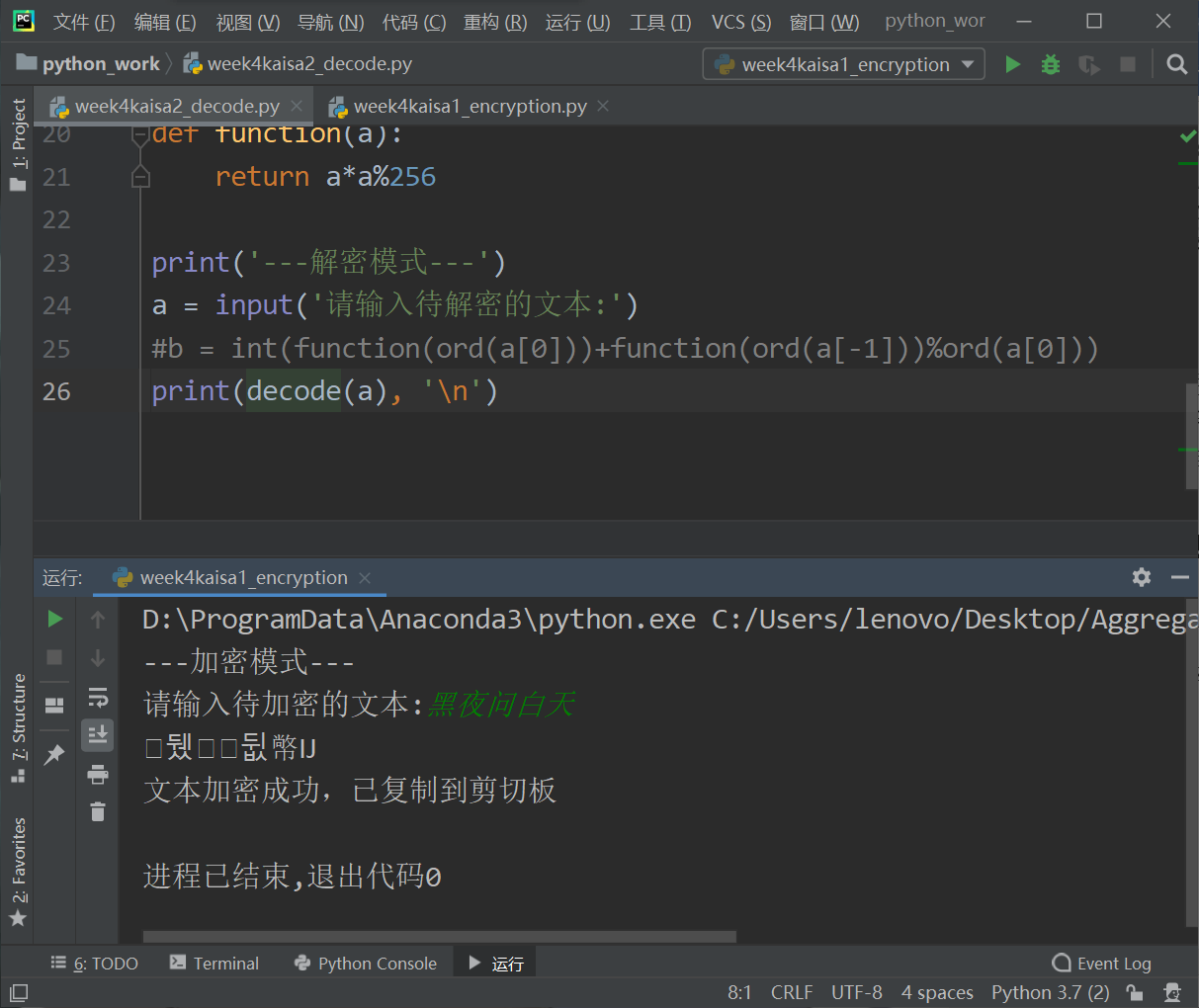
1. 从待解密的字符串a后两位反解出b和ran\_num，还原伪随机数数列。
2. 根据加密程序中的规则，反解出每一个字符对应的原字符，存入x。
3. 将x字符串打印到控制面板。

**四、实验结果与分析**

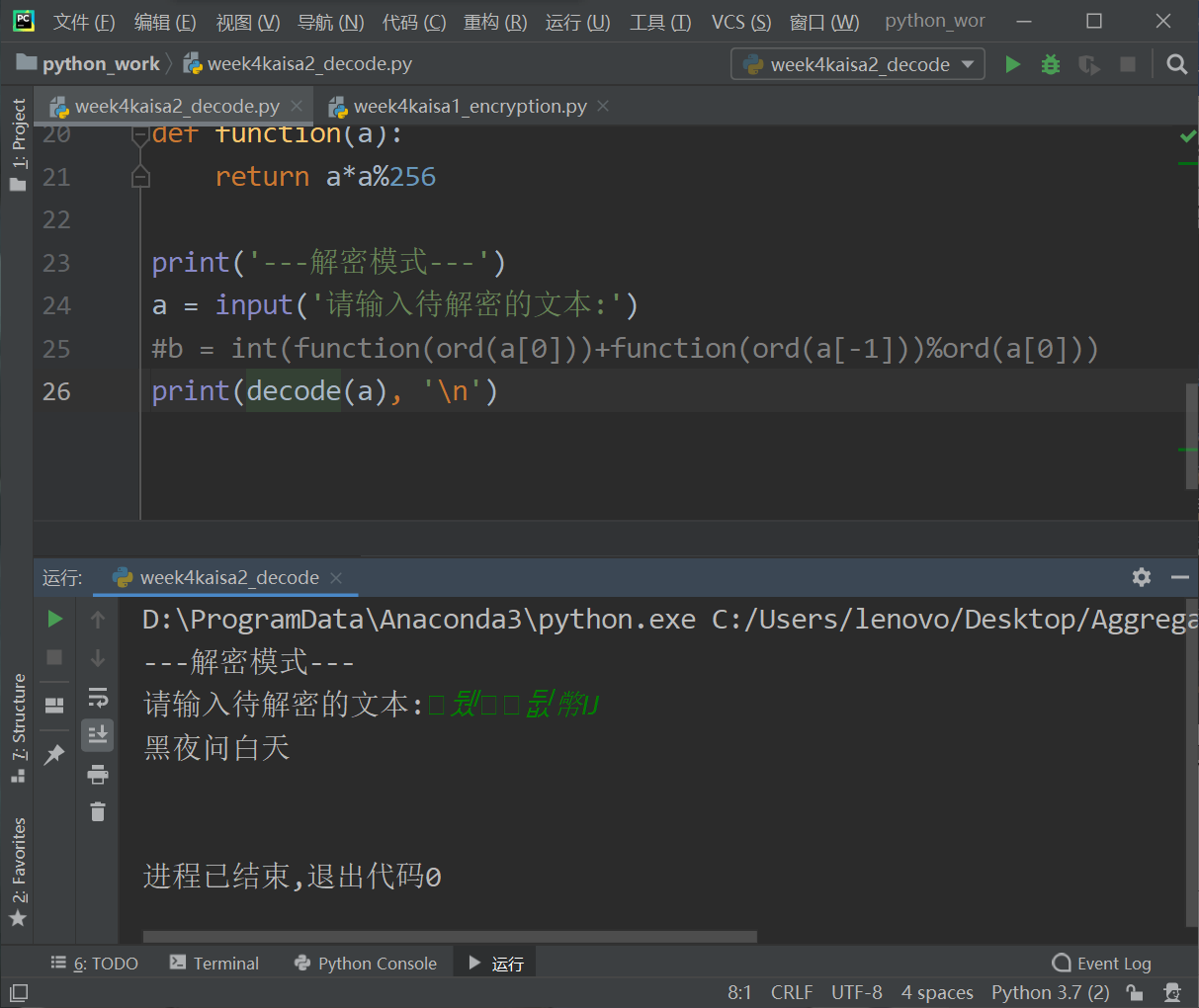
实验结果演示如下：

输入待加密的文本为：黑夜问白天

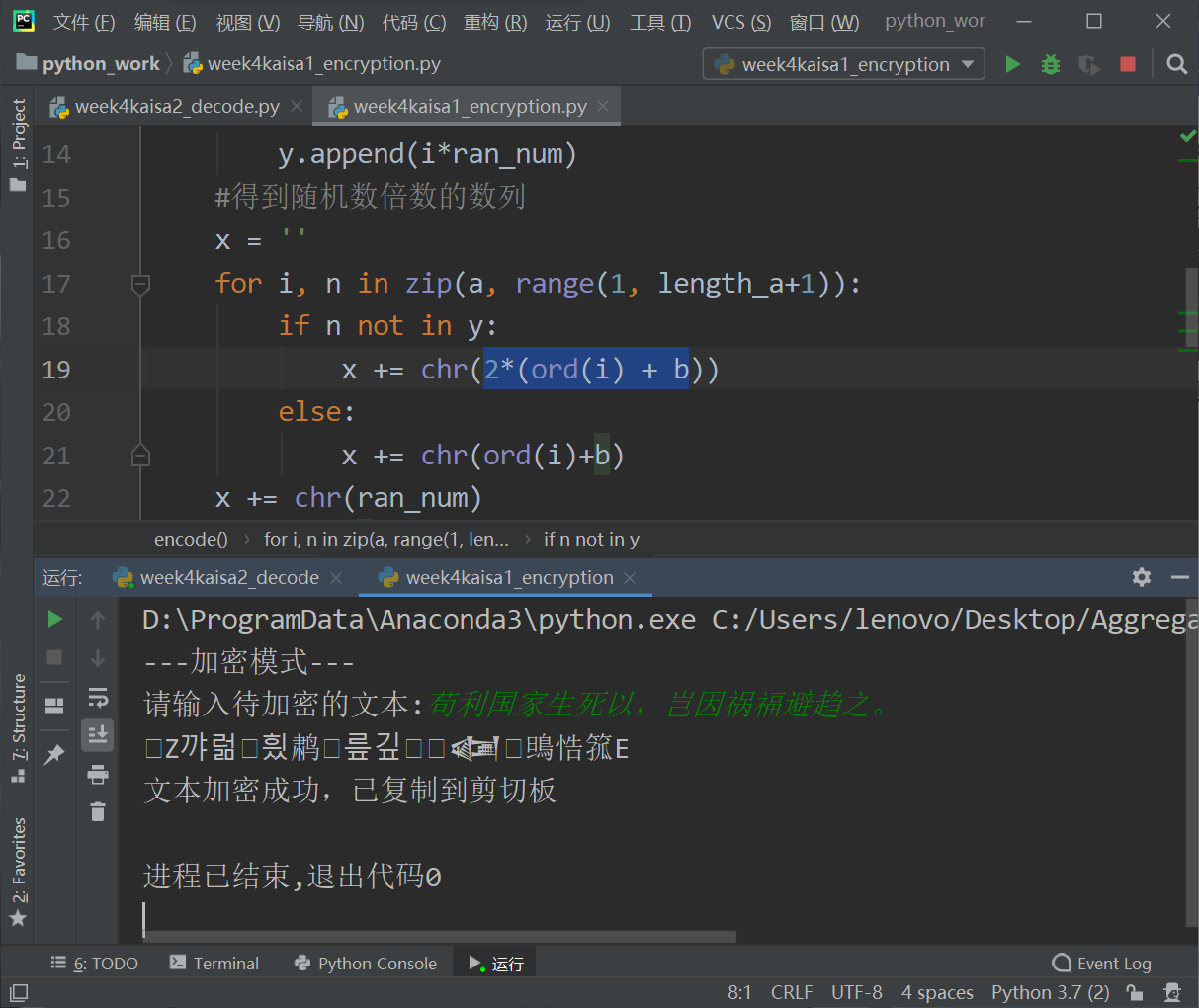
加密后的文本为：𔀆뒜𒹀뒶幤Ĳ（复制出来有些无法显示）

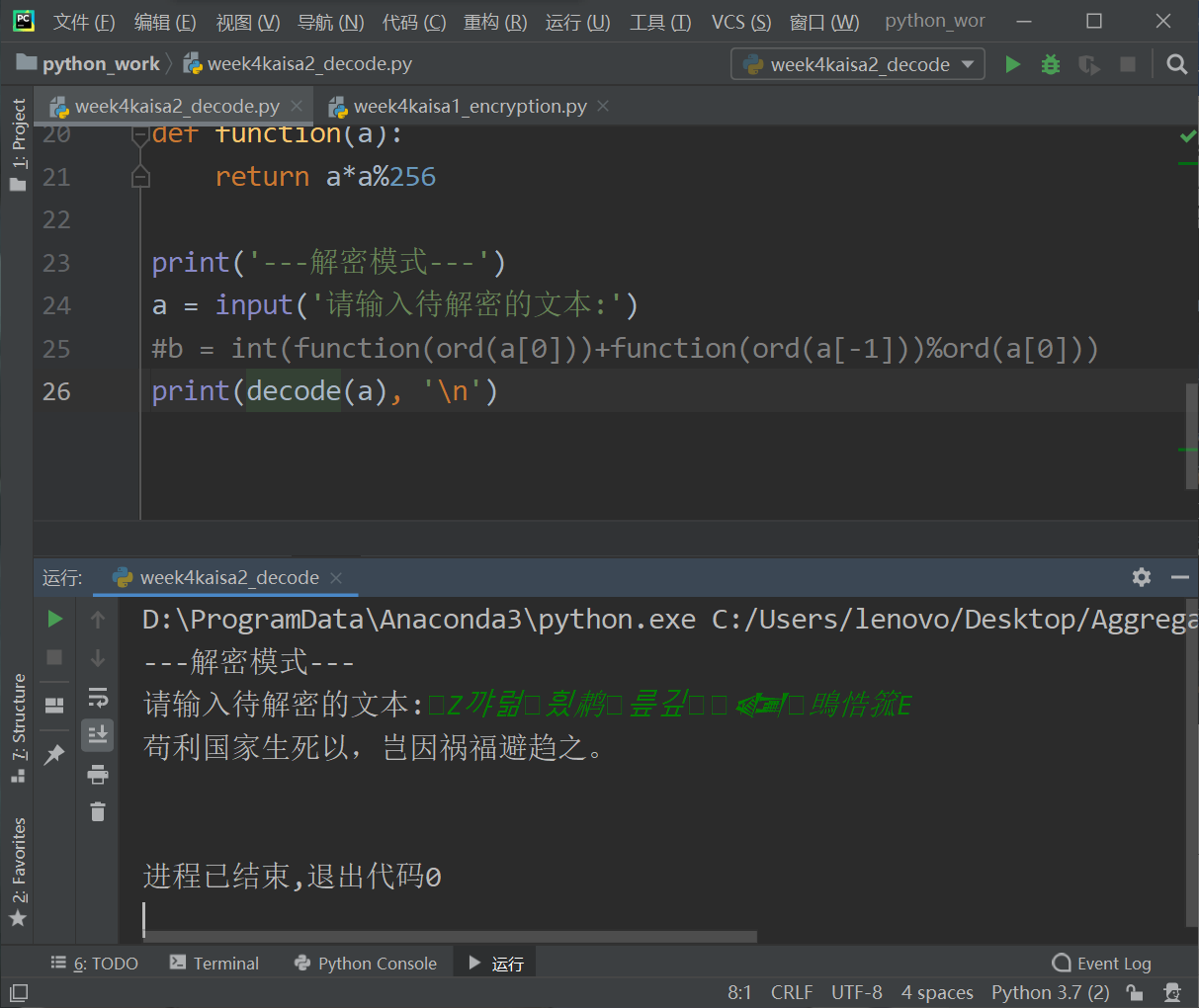


将加密后的文本赋值粘贴到解密程序，解密后的结果仍为原来的“黑夜问白天”



其他例子演示截图如下，不再赘述：





**五．实验总结**

本次实验让我在熟悉python一些基础操作代码的同时，认识了凯撒密码及其局限性，并在能力可及的范围内对凯撒密码作了相应的改进。

在实验过程中，我对python语言的debug更加熟悉，知道了一部分代码出错的大致debug方向，在查资料时也认识了很多python的库，提高了编程能力，我期待在下一次的python实验课上学习到更多的知识。