**人工智能程序设计（python）**

**实验报告**

**实验题目：用python实现中文凯撒加密**

**专 业：人工智能**

**姓 名：姚彦宇**

**学 号：22920192204115**

**实验日期**：2020.03.25

<正文内容字体为黑色宋体小四>

1. **实验目的**

对课堂上学习的理论知识进行实践，熟悉python编程语句语法，锻炼编程能力和技巧。

1. **实验内容**

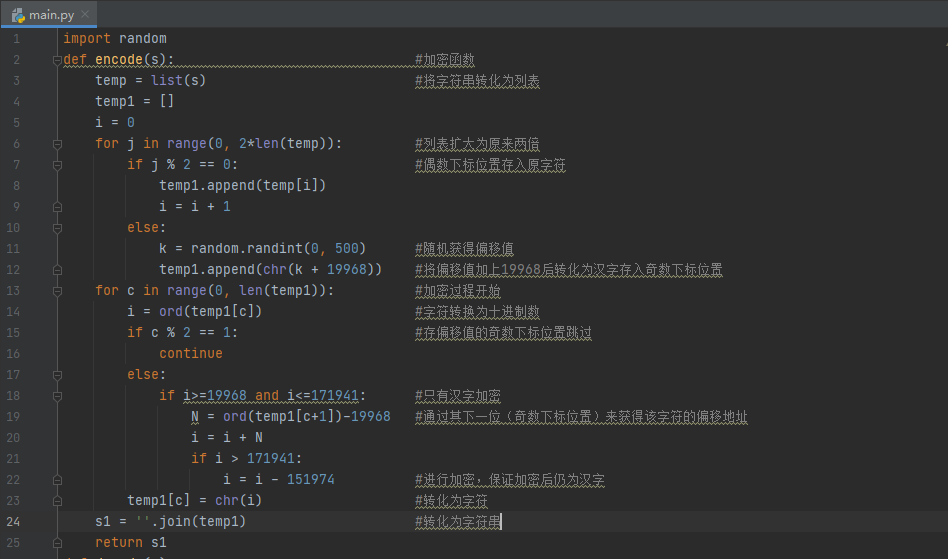
使用python语言实现汉字的凯撒加密与解密。要求偏移值应当具有隐蔽性，不能轻易被破译，偏移值的传输同样需要有隐蔽性。

**三．实验步骤以及结果**

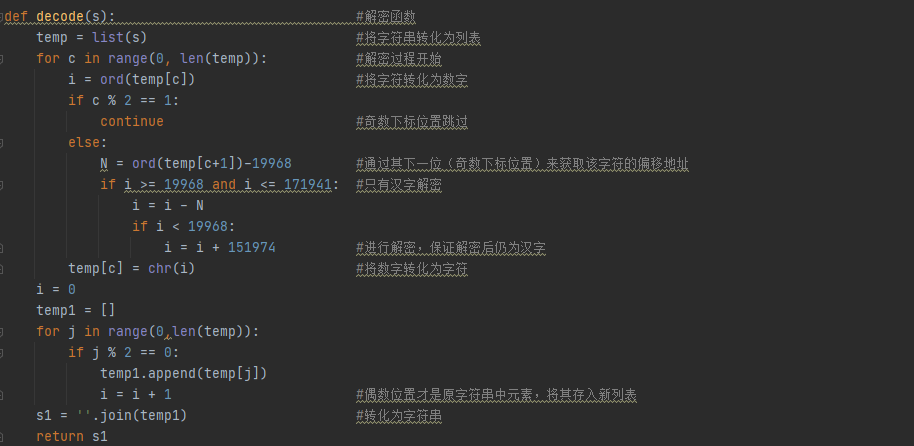
思路：根据题目要求，我设计了两个函数encode和decode分别用于加密和解密。大致思路为：将字符串转化为列表，并将列表扩大两倍，将汉字存于列表偶数下标的位置中。奇数下标位置通过random.randint（）函数随机获得一个随机数N当作偏移值，并将该偏移值加上19968后转化为汉字存入。在加密过程中，偶数下标位置的汉字通过其下一位（奇数下标）所代表的偏移值N进行加密，加密完毕后将列表转化为字符串返回，此时字符串偶数下标位置为加密后的原字符，奇数下标位置上的汉字用来传递其前一位（偶数下标）汉字的偏移值。解密时，通过奇数下标位置的汉字来获得其前一位（偶数下标）的偏移值，解密后只需将偶数下标位置字符凑成字符串返回即为原字符串。

具体代码实现：

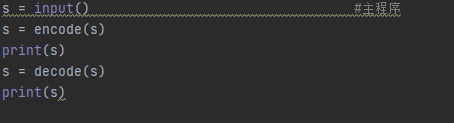
encode(s):



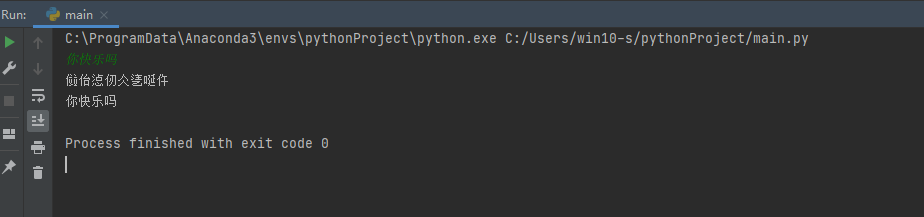
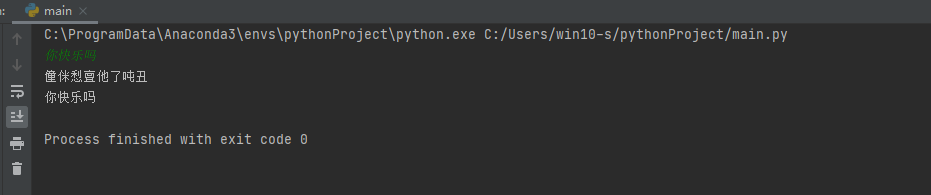
decode(s)：



主程序：



其中一次的结果：



每次同字符串的加密后密码不同

核心代码：

def encode(s): #加密函数  
 temp = list(s) #将字符串转化为列表  
 temp1 = []  
 i = 0  
 for j in range(0, 2\*len(temp)): #列表扩大为原来两倍  
 if j % 2 == 0: #偶数下标位置存入原字符  
 temp1.append(temp[i])  
 i = i + 1  
 else:  
 k = random.randint(0, 500) #随机获得偏移值  
 temp1.append(chr(k + 19968)) #将偏移值加上19968后转化为汉字存入奇数下标位置  
 for c in range(0, len(temp1)): #加密过程开始  
 i = ord(temp1[c]) #字符转换为十进制数  
 if c % 2 == 1: #存偏移值的奇数下标位置跳过  
 continue  
 else:  
 if i>=19968 and i<=171941: #只有汉字加密  
 N = ord(temp1[c+1])-19968 #通过其下一位（奇数下标位置）来获得该字符的偏移地址  
 i = i + N  
 if i > 171941:  
 i = i - 151974 #进行加密，保证加密后仍为汉字  
 temp1[c] = chr(i) #转化为字符  
 s1 = ''.join(temp1) #转化为字符串  
 return s1  
  
def decode(s): #解密函数  
 temp = list(s) #将字符串转化为列表  
 for c in range(0, len(temp)): #解密过程开始  
 i = ord(temp[c]) #将字符转化为数字  
 if c % 2 == 1:  
 continue #奇数下标位置跳过  
 else:  
 N = ord(temp[c+1])-19968 #通过其下一位（奇数下标位置）来获取该字符的偏移地址  
 if i >= 19968 and i <= 171941: #只有汉字解密  
 i = i - N  
 if i < 19968:  
 i = i + 151974 #进行解密，保证解密后仍为汉字  
 temp[c] = chr(i) #将数字转化为字符  
 i = 0  
 temp1 = []  
 for j in range(0,len(temp)):  
 if j % 2 == 0:  
 temp1.append(temp[j])  
 i = i + 1 #偶数位置才是原字符串中元素，将其存入新列表  
 s1 = ''.join(temp1) #转化为字符串  
 return s1

**四．实验总结**

这次实验让我对于已学习的python语句包括输入输出语句、条件语句、字符串处理、列表处理等理论知识有了更深的理解，通过实践也对这些知识语句的运用更加熟练；除此之外，我对这次实验中使用的未学过的知识包括随机数获取、循环语句等有了大致的概念，这可以让我在后续学习理论知识时会有更深的理解；再者，这次加密方法（动态随机加密）也是拓宽了我对于加密知识的认识。