**人工智能程序设计实践**

**实验报告**

**实验题目： python中文凯撒密码编写**

**专 业： 人工智能**

**姓 名： 郑一境**

**学 号： 22920192204153**

**实验日期**： **2021/3/25**

1. **实验目的**

初步了解并实践python语言，尝试编写出具有实用性的程序

1. **实验内容**

***凯撒密码：***

按正常字母序列进行移位，给定移位长度N，设计实现凯撒密码的加密和解密程序

给定映射序列和移位长度N

Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ

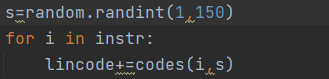
Ciphertext: COMPUTERABDFGHIJKLNQSVWXYZ

设计实现针对中文的凯撒密码的加密和解密程序

**三．实验步骤以及结果**

我的思路是，运用random产生随机数，将其设置为偏移量，由于直接传送偏移量会被轻松拦截并破解。于是我想到了在原有文本的末尾多加一个文字，这个文字专门为传输偏移量设计，是由文本的第二个已加密过的字再偏移一个偏移量而生成的字。这样避免头尾相减的惯性思维，也因文字的含义不定而使得密码难以破解。

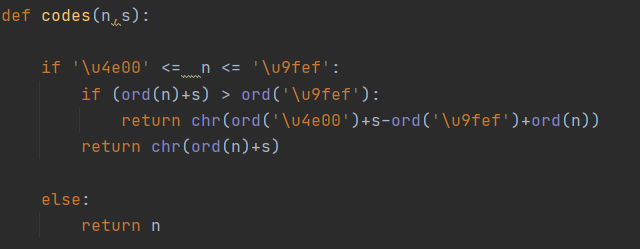
随机生成偏移量：



设置解密的钥匙：



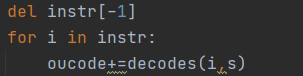
加密函数，每个字符依次偏移相同偏移量：



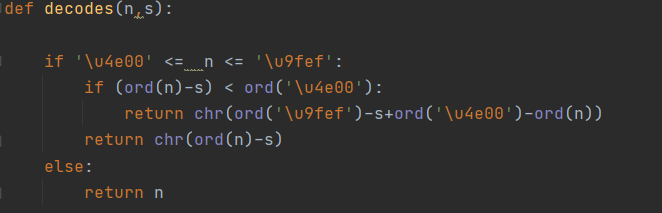
找出解密钥匙，即偏移量：



删除最后多余的文字：



解密函数：



附完整代码：

加密程序：

import random

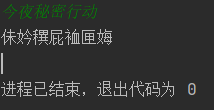
def codes(n,s):  
  
 if '\u4e00' <= n <= '\u9fef':  
 if (ord(n)+s) > ord('\u9fef'):  
 return chr(ord('\u4e00')+s-ord('\u9fef')+ord(n))  
 return chr(ord(n)+s)  
  
 else:  
 return n  
  
  
def main():  
  
 instr=input()  
 instr=list(instr)  
 lincode=""  
 s=random.randint(1,150)  
 for i in instr:  
 lincode+=codes(i,s)  
 lincode+=codes(instr[1],s+s)  
 print(lincode)  
  
if \_\_name\_\_== '\_\_main\_\_':  
 main()

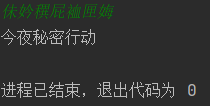
解密程序：

def decodes(n,s):

if '\u4e00' <= n <= '\u9fef':  
 if (ord(n)-s) < ord('\u4e00'):  
 return chr(ord('\u9fef')-s+ord('\u4e00')-ord(n))  
 return chr(ord(n)-s)  
 else:  
 return n  
  
def main():  
  
 instr=input()  
 instr=list(instr)  
 oucode=""  
 s=ord(instr[-1])-ord(instr[1])  
 del instr[-1]  
 for i in instr:  
 oucode+=decodes(i,s)  
 print(oucode)  
  
if \_\_name\_\_== '\_\_main\_\_':  
 main()

**四、实验结果与分析**





可以正常实现汉字的加密和解密，整体没有问题。但是老师指点可以通过大规模的数据找出偏移量异常的字的位置，但是知道异常位置，其实际含义也很难猜测，故我认为虽有瑕疵但不失为一个好方法，可以继续扩展改进。

**五．实验总结**

本次实验通过编写中文凯撒密码程序，完成了熟悉python程序的目的。并且用自己编写具有实用性代码的方式提高了我们对编程的的热情。提高了工程性思维，开拓了思维，增进了对密码学技术的认识。