**人工智能程序设计**

**实验报告**

**实验题目： 针对中文的凯撒密码加解密程序**

**专 业： 人工智能**

**姓 名： 王宇浩**

**学 号： 22920192204080**

**实验日期**： **2021/3/25**

**一. 实验目的**

1. 将前几节理论课所学的知识进行实际应用；

2. 熟悉python语言的语法和程序设计。

**二. 实验内容**

使用python语言，设计一个凯撒密码（Caesar cipher）加密和解密程序，使能够实现针对中文的凯撒密码进行加密和解密。

**三．实验步骤以及结果**

1.字符读取

由于所学有限，我在本实验中决定采用使用ord()函数将字符转化成对应的整数表示，加密之后再使用chr()函数将整数进行还原，生成加密之后的字符进行输出。

2.加密处理

因为只使用密钥进行简单处理会导致加密之后的字符串极易被反推出来，因此我在考虑加密方式的时候决定采用分段分情况加密，从而使加密所得字符串具有混淆性和更高的复杂度。

首先针对字符所在位置，根据字符下标的奇偶性对字符进行两种情况的处理，然后根据生成的随机数对整数进行处理。这种方式使相同字符在不同位置存在不同的加密结果，同时不同字符因为位置原因可能存在相同的加密结果，这样就使得加密之后的字符串具有了混淆性。

3.源码

import random

def enc(*string*):

    s1 = list(string)

    a1 = random.randint(0, 10)

    a2 = random.randint(0, 10)

    for i in range(0, len(s1)):

        num = ord(s1[i])

        if 19968 <= num <= 171941:

            if i % 2 == 0:

                num += a1

            else:

                num += a2

            s1[i] = chr(num)

    s2 = ''.join(s1)

    s3 = s2 + chr(a1) + chr(a2)

    return s3

def redu(*string*):

    s1 = list(string)

    a1 = ord(s1[-2])

    a2 = ord(s1[-1])

    for i in range(0, len(s1) - 1):

        num = ord(s1[i])

        if 19968 <= num <= 171941:

            if i % 2 == 0:

                num -= a1

            else:

                num -= a2

            s1[i] = chr(num)

    del s1[-1]

    del s1[-1]

    s2 = ''.join(s1)

    return s2

if \_\_name\_\_ == '\_\_main\_\_':

    c = input('请输入需要加密的字符串：')

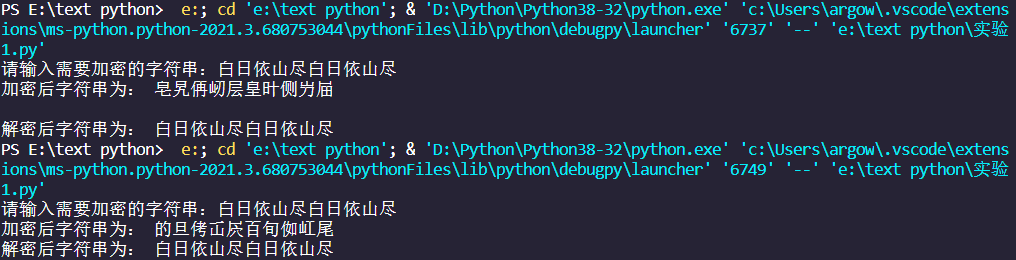
    c1 = enc(c)

    print('加密后字符串为：', c1)

    print('解密后字符串为：', redu(c1))

**四、实验结果与分析**

1. 结果展示



2. 分析及改进思路

由于时间有限，我并没有对加密算法进行更复杂的处理，但这种思路使得加密的复杂性具有很高的上限，通过更复杂的分段和位移量的多样性可以使加密后的字符串具有极高的复杂度。

此外，我认为可以利用随机数和密钥对字符串进行多重加密，也可以利用前面的字符对后面的字符加密处理产生影响。这些方式都能使加密的结果变得更复杂且难以破解。因此算法的完成的还比较低，可以完善的地方还有很多

**五．实验总结**

通过今天的实验，我熟悉了已学的python语法知识，并进行了操作。同时，能有机会将所学知识进行实际运用，收获了操作经验。