**python程序设计**

**实验报告**

**实验题目：** 凯撒加密与解密

**专 业：** 人工智能

**姓 名：** 蔡光磊

**学 号：** 22920192203899

**实验日期**： 2021.3.25

1. **实验目的**

熟悉python的一些操作指令与语法规则，例如列表的一些基本操作，简单条件判断与循环。

1. **实验内容**

凯撒加密法在过去通常用作一些特殊的加密工作，即使在今日，凯撒密码的应用范围仍旧非常广泛。现要求用python语言编写两个程序，分别用作对一段已知信息的加密和解密工作（**注意：输入的信息不仅包括英文字符，还应包括中文汉字**）。

1. **实验分析与步骤**

本题实验的难点有二：首先是对输入信息的要求，不仅能应对英文字符窜，还应该包含对中文汉字的处理。解决方案便是使用python针对中文译码的操作函数ord，该函数能将一个中文汉字转换成（19968，40870）区间中的一个数，再使用chr函数能将区间（19968,40870）中的数转换成汉字。其次困难之处在于加密与解密程序是两个不同的程序，因此映射函数应该通过怎样的方式从加密程序传到解密程序呢？解决方案便是在进行加密的过程中我们可以增加一个额外的空间来记录这个映射函数。具体代码如下：

**//加密程序**

import random

print("请输入加密明文：")  
P=input()   
lenth=len(P)  
ran=random.randint(19968,40870)  
i=0  
result=chr(ran)  
while i<lenth:  
   result=result+chr((ord(P[i])+i\*ran)%40870) //此处注意我们的映射函数，多加  
   i+=1 了一个变量i  
print("加密后的密文为：")  
print(result)

**//解密程序**  
print("请输入密文：")  
Q=input()  
lenth=len(Q)  
ran=ord(Q[0])  
i=1  
result=""  
while i<lenth:  
    result=result+chr((ord(Q[i])-(i-1)\*ran)%40870)  
    i+=1  
print("解密后的明文为：")  
print(result)

1. **运行结果截图**



显然针对同一信息加密两次，两次结果均不相同。同时，对两段不同密文的解密都成功得到了我们需要的明文。

1. **实验总结**

该实验如果仅仅要对已知信息进行加密再解密，实际上并不困难。我们还应该从hacker的角度看问题。即我们的加密程序容不容易被hacker破解呢？在我第一次编写完程序后，老师便指出了加密程序的简单性，映射函数一旦变为线性的便会非常容易破解。因此我在原有的映射函数中多加了一个变量i，i随着循环次数的变化而变化。虽然仅多增加了一个未知数，但该未知数是不断变化的，换言之，并不是简单的二元一次方程，而是n元方程。因此，再要破解映射函数便是一个非常困难的过程了。