**人工智能程序设计**

**（python）**

**实验报告**

**实验题目： 汉字凯撒密码**

**专 业： 人工智能**

**姓 名： 谢展豪**

**学 号： 22920192204100**

**实验日期**： 3.25

1. **实验内容**

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

设计实现凯撒密码的加密和解密程序

设计实现针对中文的凯撒密码的加密和解密程序

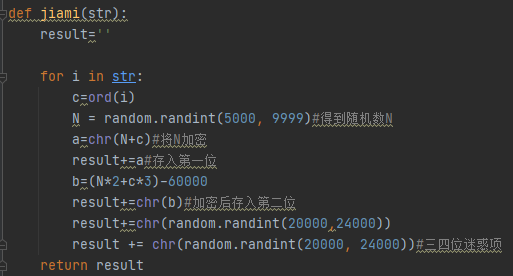
1. **程序分析和算法思路**

这个程序包含两个子程序，第一是需要我们去将一段正常的汉字字符串加密，得到密码，之后将密码传递给接受方，接受方通过将密码按照一定方法进行解密后，得到原来的原文，这个加密方法要足够安全防止中途被黑客截下，所以我们需要的是用凯撒密码的加密方式设计出加密方法并能安全的被解密。

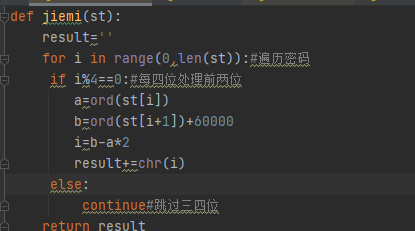
对于凯撒密码，需要一个偏移量来改变每一个字符的值，之前我遇到过存英文字母的问题，这次是存汉字，还是有很大的不同，后来了解到了unicode码是python中用来储存汉字的源码，每一个汉字在unicode中都有对应的数字，因此我才用先将输入字符串改变成unicode码后进行加密再转换回汉字这样的方法来产生密码。

经过查找，我学到了ord()函数和chr()函数，第一个是将汉字转化成Unicode码第二个是将Unicode码转换成汉字，基于对这两个函数的理解，展开了实验。

在一开始我在整个字符串中只采用一个偏移量N来进行加密，并将其存在密码的第一位，用随机函数生成一个N，然后用chr(N+25000)的方式将N变成一个汉字混入密码中，后来我发现这样的办法依旧不够安全，若被黑客发现规律有可能被看出，所以将密码改成了一个原文汉字对应一个N，将每个N进行加密同样存入字符串中，将原文汉字的unicode码和N组成一个二元一次方程存入密码的前两位中的再加入两个随机项，最后的密码长度是原文的四倍。



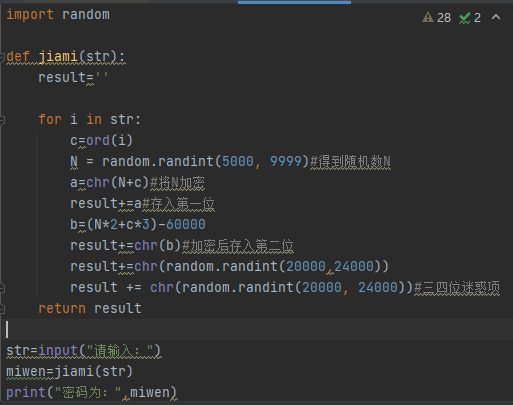
在最终的代码中，每四个密码代表一个原文的汉字的，先随机生成一个N和将原文的汉字转换成unicode码，这里用c代表，第一位是N+c再转换成为新的汉字，第二是2N+3c再减去60000，因为有超出的可能，再转换回去成为新汉字，三四位是无意义的随机字符。这就完成了编码过程。



在解码过程里，只要按方法返回原先的字符就可以了，将汉字串每四位统一处理先从第一位和第二位中反解出N和c再转换成汉字，三四位直接跳过就，最后拼凑出原先的汉字串可以了。

1. **实验结果展示**

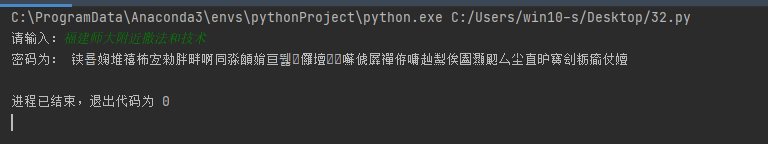
以下为加密代码



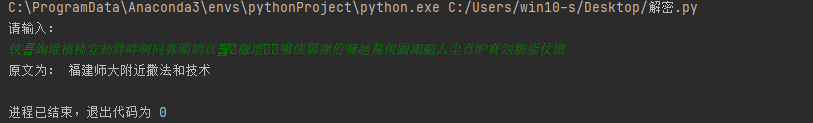
以下为解密代码



输入一个汉字串得到密码



得到源码



最后成功得出了结果

1. **总结**

在这次实验中，我通过各种渠道学习到了很多新的函数和使用方法，更加了熟悉python的编码方式，并将课上学到的东西和实际操作相互印证，对老师讲过的知识有了更深一层的认知，并培养了自己解决实际问题的能力。但总的来说，还是有很多不足，我认为我的编码方式还是有些不够复杂，N的加码方式还是有很大的提升空间，其次我的过程中还是犯了许多错误，尤其对编写python缺乏足够的实践，到编写时还是犯了许多小错误，例如写错函数名或者忘记写冒号。总而言之，希望以后可以加强这些不足，更快更好的完成实验内容