**人工智能程序设计(Python)**

**实验报告**

**实验题目： 恺撒密码加密解密**

**专 业： 人工智能**

**姓 名： 郭佳睿**

**学 号： 22920192203950**

**实验日期**： 2021.3.25

1. **实验目的**
2. 掌握python语言基础语句的使用方法
3. 熟悉利用恺撒密码的加密解密方法
4. 熟练使用恺撒密码加密解密中文字符串
5. **实验内容**
6. 实验背景：

在密码学中，恺撒密码（英语：Caesar cipher），或称恺撒加密、恺撒变换、变换加密，是一种最简单且最广为人知的加密技术。它是一种替换加密的技术，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。例如，当偏移量是3的时候，所有的字母A将被替换成D，B变成E，以此类推。这个加密方法是以罗马共和时期恺撒的名字命名的，当年恺撒曾用此方法与其将军们进行联系。

1. 实验内容：

使用恺撒密码加密解密中文字符串。加密过程即给出原文，输出加密后的密文；解密过程即给出密文，输出原文。

1. 实验要求：

要求不能仅根据密文，在未知解密程序及密钥的情况下，从密文中看出或统计出加密规律，并破解密码。

1. **实验步骤以及结果**
2. 题目分析

由实验要求可知，不能简单的使用恺撒密码做加密解密运算。

例如英文下的凯撒密码的偏移量最多有26种选择，那么要破解密码，只需要简单的暴力尝试破解26次即可，一定能够得到正确的原文。

那么我们就需要更加复杂的加密方式。

1. 算法思路

加密算法中

密钥：

将密钥设定为在汉字编码（19968 -- 40869）中随机出的一个等差数列。具体为随机出两个变量，分别为密钥在汉字编码中的起始位置（首项）secret\_pos 和 密钥的公差secret\_mul。然后利用首项和公差构造密钥。

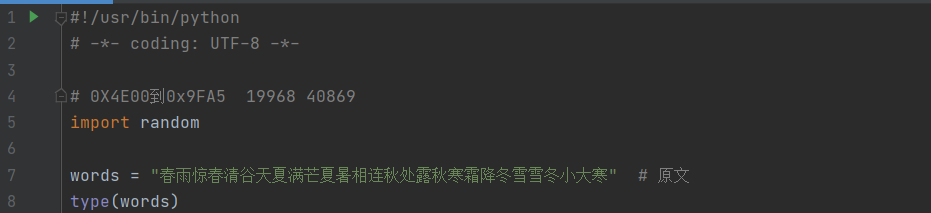
加密方法：

考虑到线性加密易被破解，采用多次重复加密的方法。随机出加密次数secret\_tim，然后将密文循环加密secret\_tim次。

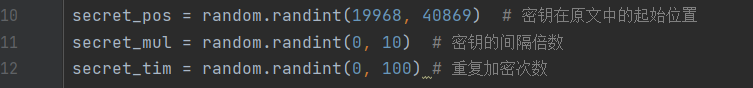
1. 算法

（一）加密算法

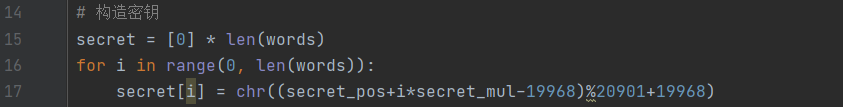
1. 考虑到原文不能暴露，所以将原文写入程序中，并用type函数将原文转成列表。



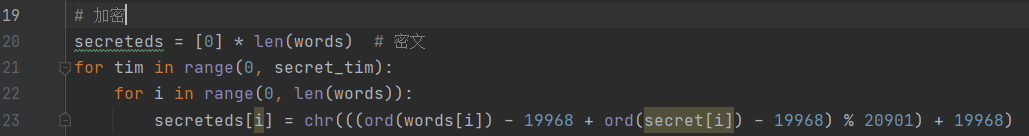
1. 随机出三个变量密钥的首项secret\_pos ，公差secret\_mul，加密次数secret\_tim。



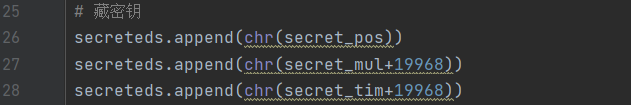
1. 构造密钥。利用chr函数将整数转换成汉字。



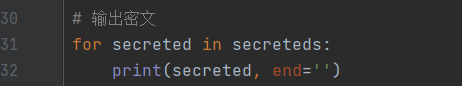
1. 循环重复加密。



1. 将密钥藏进密文中。



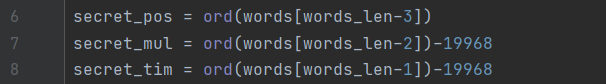
1. 输出密文



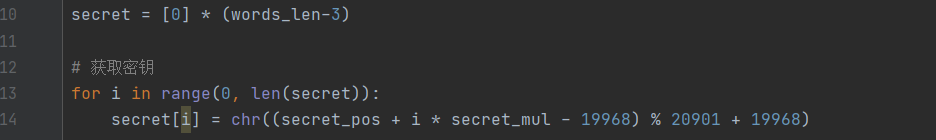
1. 解密算法
2. 解密算法的密文可以直接从输入中获得



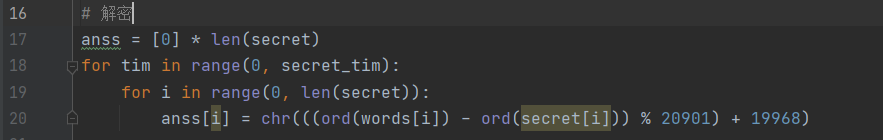
1. 同样按照步骤，先解出三个变量密钥的首项secret\_pos ，公差secret\_mul，加密次数secret\_tim。



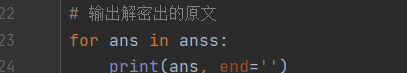
1. 按照加密算法的方法解出密钥



1. 加密算法的逆过程解密

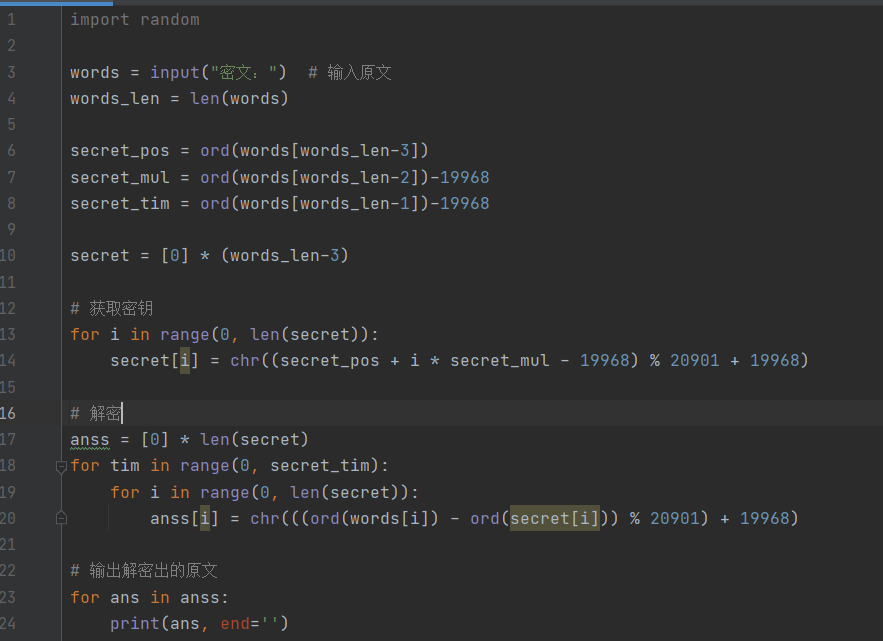


1. 解密完成

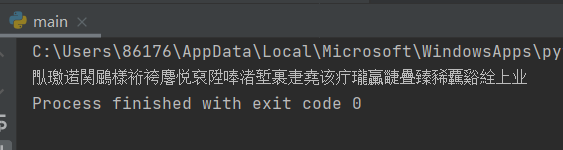


1. **实验结果**

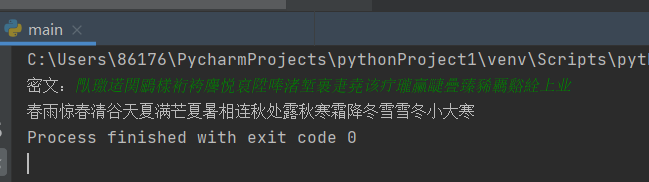




加密算法运行结果，得到密文：



解密算法解密：



成功解出原文

**五．实验总结**

通过本次实验，我熟练掌握了python语言的部分基本语句的书写和应用方法，能够运用python语言编写程序解决问题。了解了恺撒密码的原理、特点和不足，并能够用自己的方法编写程序进行加密解密运算。

这次实验中，暴露出了我对于中文编码掌握不熟练的问题，这个问题使得我在实验过程中浪费了很多不必要的时间，占用了非常多的实验、调试时间。这次试验之后，还应熟悉中文编码的使用并熟练掌握。

总的来说，从开始编写、修改恺撒密码的程序直到最终调试成功，我也体会到了密码学的魅力，