**人工智能程序设计（Python）**

**实验报告**

**实验题目： 凯撒密码**

**专 业： 人工智能**

**姓 名： 赵露丹**

**学 号： 22920192204146**

**实验日期**： 2021.3.25

1. **实验目的**

熟悉python编程的特点与各种语句的使用方法，同时了解信息传输过程中的加密环节与对应加密的方法，拓展学习现有的系统编码方式。

1. **实验内容**

实现凯撒密码的进阶版，具体要求为：

1. 加密信息中包含中文字符
2. 转移位数动态变化

**三．实验步骤以及结果**

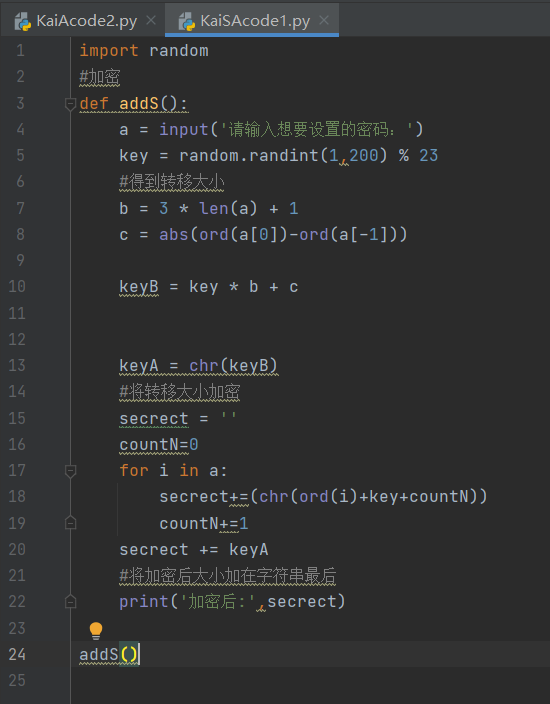
加密过程：

1. 输入想要加密的信息（密码）
2. 生成23以内的随机数，即位移量（可更改）
3. 由于位移量动态变化，若想要解密，则需将位移量以某种方式传递给解密程序。故需对位移量key进行加密传输。具体为：令b=3\*密码字符串长度+1；c=第一个字符与倒数第一个字符的ascii码之差的绝对值；得到加密后位移量的ascii码keyB=key\*b+c，将其转化为对应字符keyA；
4. 对密码字符串的i位字符（i=0…len(s)）进行移位操作：

利用ord函数将其转化为对应ascii码，加上位移量key，再加上其位置下标i（再次位移）后，最后将新字符利用chr函数转换回字符串类型，添加到加密后的新字符串中。

1. 最后，将加密后位移量字符串keyA添加到加密字符串末尾，以实现将位移量的传输

代码实现如下：



解密过程：

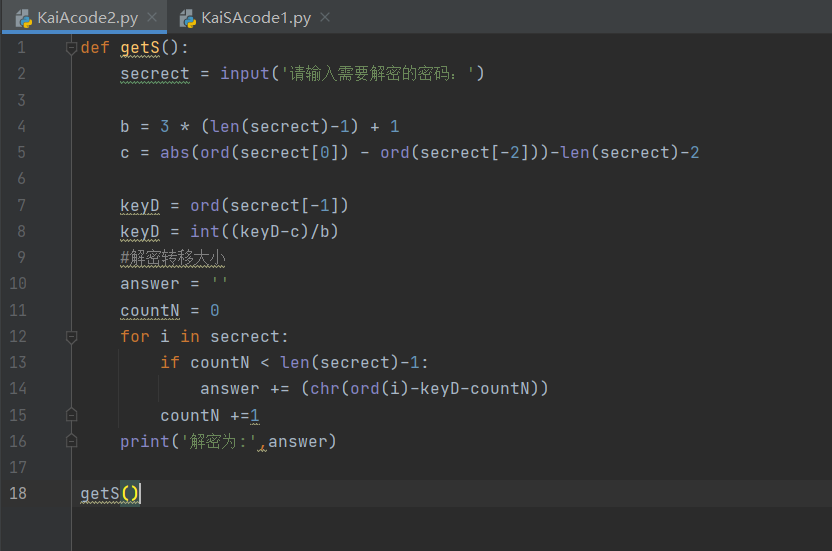
1. 由加密过程中b,c的计算过程，结合字符串反推得出b与c的值。

注意：此处加密字符串的长度增加了1，原倒数第一位字符现位于倒数第二位，且其与第一位字符ascii码之差的绝对值，增加了该字符的位置下标，故b，c的计算公式为：

b = 3 \* (len(secrect)-1) + 1  
c = abs(ord(secrect[0]) - ord(secrect[-2]))-len(secrect)-2

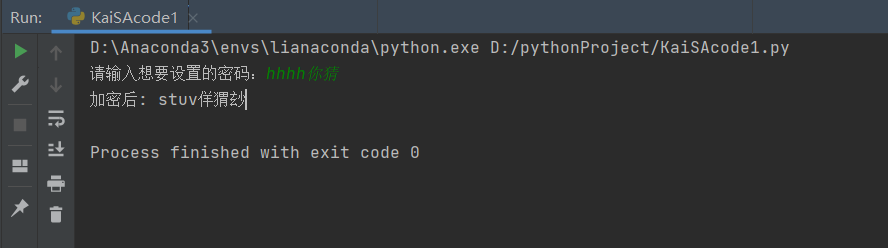
1. 将加密字符的最后一位转换为ascii码，并由keyB=key\*b+c的反函数计算得出位移量key
2. 遍历加密字符串（除去最后一位），将其转换为ascii码后减去位移量与其位置下标，再利用chr函数将其转换回字符串，即得到解密后的字符串

代码实现如下：

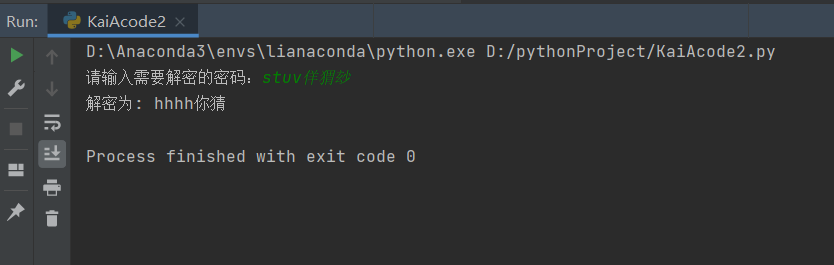


**四、实验结果与分析**

程序加密结果为：



对应解密结果为：



**五．实验总结**

此次实验，难点在于中文字符的添加与动态变化位移量的间接传递。在字符编码方面，通过查阅资料，对UTF-8，GBK，Unicode等编码标准与其在系统与python的应用有了一定的了解，此后通过查阅并利用python函数，实现了字符与其编码之间的转换，进一步实现位移。同时，在具体的加密过程中，最初采用的是固定线性函数来加密位移量，同时每个字符的位移量不变，但该方法在大范围统计下极易破解，故结合字符串本身，对加密过程复杂化，从而增大保密性，再将加密后的位移量字符加入加密字符串，实现位移量的间接传递。