**Python实验1报告**

**实验题目：**设计凯撒密码加密和解密程序

**专 业：**人工智能

**姓 名：**柯昭熙

**学 号：**22920192203977

**实验日期**：2021/3/25

1. **实验目的**

1.熟悉python语言的编写。

2.训练运行Python编写完整程序的能力。

1. **实验内容**

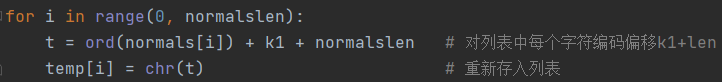
设计实现针对中文的凯撒密码的加密和解密程序。

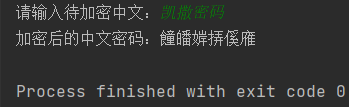
加密程序：对输入的中文字符串进行加密处理，输出加密后的字符串。

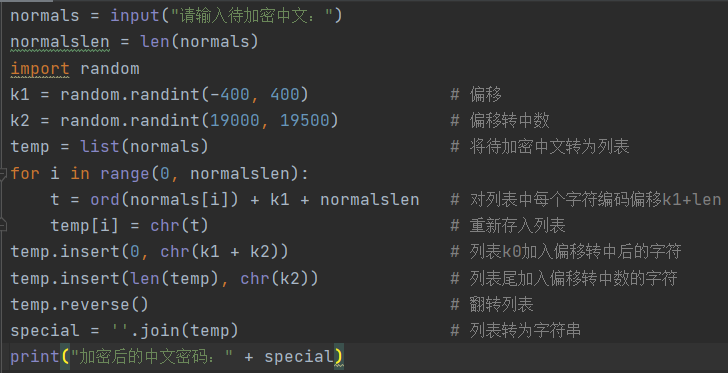
解密程序：对输入的密码字符串进行解密处理，输出解密后的中文字符串。

1. **实验步骤以及结果**

加密程序：

1. 将中文字符串转为列表1.1
2. 随机得到偏移（k1）和把k1偏移成中文的偏移数（k2）1.7
3. 对列表中每个字符的编码进行偏移（k1+字符串长度）
4. 将加密信息偏移成中文字符藏入1.3
5. 翻转列表1.4
6. 列表转为中文字符串1.5
7. 结果



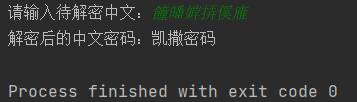
8.完整程序

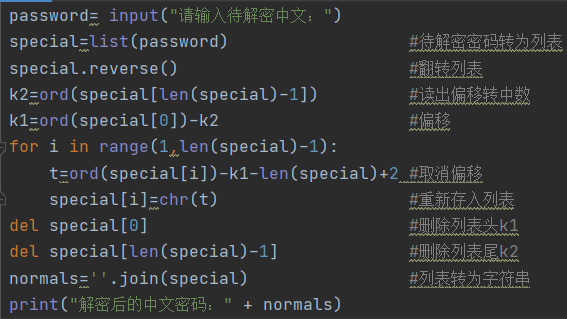
解密程序：

1. 字符串转为列表2.1
2. 翻转列表2.2
3. 读出k1和k2

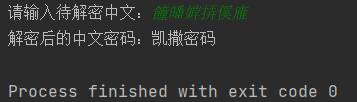
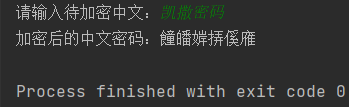
2.3

1. 取消偏移2.4
2. 删除列表头尾存储k1和k2信息的字符2.5
3. 列表转为字符串2.6
4. 结果



8.完整程序

**四、实验结果与分析**

1.结果

1. 分析
2. 加密和解密

加密：将一个中文字符串转为列表，对列表中每个字符编码偏移随机数k1+字符串长度，对偏移k1进行中文加密(偏移k2),将k1存入列表头，k2存入列表尾，翻转列表，最后转为中文字符串。

解密：将中文字符串转为列表，翻转列表，读出k2和k1信息，求出k1，取消列表中字符的偏移，删除列表头尾中存储的信息，最后转为中文字符串。

1. 加密之间关系

加密a：偏移k1+字符串len

加密b：偏移k2

加密c：翻转

加密a和加密c是平行关系，都是对中文字符串本身的加密。加密b是对加密a的加密。

1. 加密的方式存在被破译的可能。
2. 思考改进：

A:将字符串第二位再存入一个偏移k3，然后对列表的偏移改为，奇数位保持原来的k1+字符串len的偏移，偶数位偏移k3。

B：对偏移k1的位置进行加密，不固定存放在列表头。在列表头存入存储k1在字符串中位置信息的k3，来对k1位置进行加密。

C：对每个字符编码的偏移改为（k1+F(i)）%len，其中F(i)为斐波那契函数，i为字符在字符串中的位置。

**五．实验总结**

1.实现两个完整的凯撒密码加密解密程序，对python编码流程加深了认识。

2.对加密和解密的思想有了进一步的认识，了解了凯撒密码加密的原理。

3.熟练了python语言中输入(input),输出(print),整形随机数的产生(random.randint()),循环(for),字符转编码(ord),编码转字符(chr),对列表的插入(insert),翻转(reverse)和删除(del),字符串和列表的转化(list和join)。

4.体验到了python编码相对于c和c++编码的便利。

5.反思：python中各个数据类型的操作函数记忆不足，每次使用都需要查阅。