**实现对中文加密的恺撒密码**

1. **实验目的：**

**熟悉python知识点的应用**

1. **实验内容：**

**1.恺撒密码的简介**：

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。

**2.摘要：**

本文所使用的方法是恺撒密码的改进，原恺撒密码的每个英语字符有着相同的加密偏移量，在本文的改进方法中加入了随机性，增强了安全性。相对于英语的26个字符，中文的文字量更庞大，这大大增加了解密的难度性。

**三．实验步骤：**

**代码的实现：**

* **加密程序：**

import random

string1=input('请输入需加密的明文：')

n=len(string1)

l=[random.randint(1,n) for i in range(n)]

l1=[str(i\*\*2+n) for i in l]#加密后的偏移量

def jiami(string1):#加密函数

mi=''

for i in range(n):

mi+=chr(ord(string1[i])-l[i])

return mi

mi=jiami(string1)

print(mi)#输出加密后的密文

print(l1)#输出加密后的偏移量

* **解密程序：**

a=input()

l1=eval(input())

l=[int((int(i)-len(a))\*\*0.5) for i in l1]

def jiemi(a): # 解密函数

ming = ''

for i in range(len(a)):

ming += chr(ord(a[i]) + l[i])

print('解密后的明文：',ming)

jiemi(a)#调用解密函数

**两次相同的输入明文：**

1. 请输入需加密的明文：反方向的钟

及斸后皀钚

['14', '6', '14', '21', '30']

**对应的解密输入和输出：**

及斸后皀钚

['14', '6', '14', '21', '30']

解密后的明文： 反方向的钟

**2.**请输入需加密的明文：反方向的钟

叉斸吐癿钜

['21', '6', '6', '30', '14']

**对应的解密输入和输出：**

叉斸吐癿钜

['21', '6', '6', '30', '14']

解密后的明文： 反方向的钟

**四．实验结果及分析：**

本程序中借用随机函数，随机生成偏移量，假设明文的长度为n，那么就有n\*\*n种偏移量的组合搭配，随着明文的长度的增加，明文的安全性也随之增加。为了进一步减少被破译的风险，在偏移量的基础上，进行平方以及加上明文的长度，形成伪偏移量，并把伪偏移量转换成字符串，以增加它的迷惑性，最后存入列表。把伪偏移量列表和密文当做解密程序的输入，最终实现解密。

1. **实验总结：**

在进行该实验的过程中，没理解老师的意图，虽多次可进行加密和解密，但都没有符合老师的要求，因此浪费了较多时间。在最终完成该实验时，才发现实验并没有这么难。下次做实验前，还是得问清楚老师，以免在错的道路上越走越远。