**凯撒加密解密程序设计**

**实验报告**

**实验题目：凯撒加密解密程序设计**

**专 业：人工智能**

**姓 名：蔡偲劼**

**学 号：22920192203898**

**实验日期**：2021/3/27

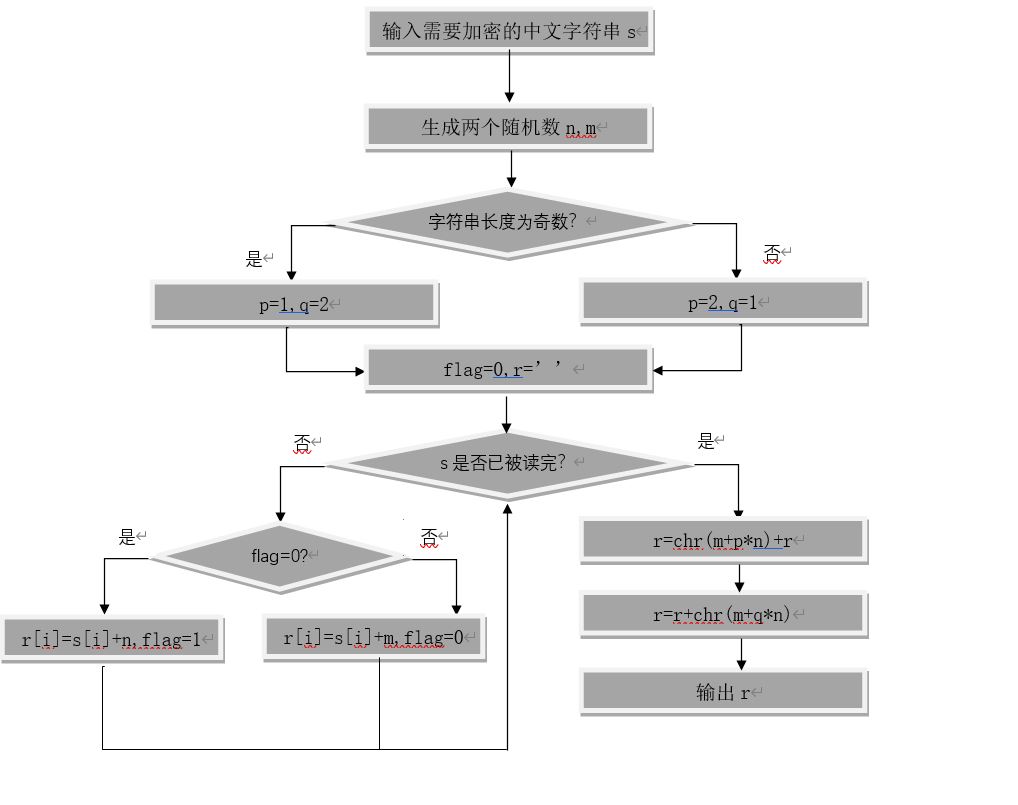
1. **实验目的**

利用python设计两个程序，一个用于对输入的中文字符串进行凯撒加密得到一串密文，另一个作为配套的解密程序用于对输入的密文进行破译

1. **实验内容**
2. 设计加密程序

加密方法为：首先利用随机数生成函数生成两个随机数n,m，同时根据输入的中文字符串的长度生成系数p和q（长度为奇数时p=1,q=2;长度为偶数时p=2,q=1）。然后字符串奇数位偏移步长n,偶数位偏移步长m，最后利用chr函数将（m+p\*n）%40870作为第一个字添加在结果的首位，将（m+q\*n）%40870作为第二个字添加在结果的末位，产生密文。

流程图如下：



源代码如下：

import random

initial=input("请输入需要加密的中文字符串：\n")

n=random.randint(19968,40870)

m=random.randint(19968,40870)

p=len(initial)%2

if p==0:

  p=2

  q=1

elif p==1:

    q=2

result=chr((m+p\*n)%40870)

flag=0

for i in initial:

    if flag==0:

        i=chr((ord(i)+n)%40870)

        flag=1

    elif flag==1:

        i=chr((ord(i)+m)%40870)

        flag=0

    result=result+i

result=result+chr((m+q\*n)%40870)

print(result)

1. 设计解密程序

利用密文长度为原文长度加二可以得到原文的长度，进而求出p值和q值，然后利用首位为m+p\*n和末位为m+q\*n的关系，求出n和m，然后逆推每一位的偏移量来得出结果

源代码如下：

initial=input("请输入需要解密的字符串：\n")

k=len(initial)-1

j=k-1

a=ord(initial[0])

b=ord(initial[k])

if j%2==1:

if b<a:

b=b+40870

n=b-a

if a<n:

a=a+40870

m=a-n

else:

if a<b:

a=a+40870

n=a-b

if b<n:

b=b+40870

m=b-n

flag=0

result=''

for i in initial[1:k]:

t=ord(i)

if flag==0:

if t<n:

t=t+40870

t=t-n

flag=1

elif flag==1:

if t<m:

t=t+40870

t=t-m

flag=0

result=result+chr(t)

print(result)

**三．实验步骤以及结果**

首先运行加密程序对同一字符串分别加密两次

然后在分别对两个结果进行解密



**四、实验结果与分析**

首先对于同一字符串，加密程序两次能产生不同的结果，满足要求，同时利用解密程序破译后，结果均正确。

**五．实验总结**

本次实验完成的凯撒加密程序和配套的解密程序基本达到要求，在过程中对于加密的复杂性有了更深的了解。