**python语言程序设计**

**实验报告**

**实验题目： 设计针对中文的凯撒密码加密和解密程序**

**专 业： 人工智能**

**姓 名： 潘东屿**

**学 号： 22920192204045**

**实验日期**： 2021年3月25日

1. **实验目的**
2. 通过设计该程序，使我们对于python中字符串，列表等结构，输入输出等基本操作有更深刻的理解。
3. 学习加密解密方式，了解操作原理。
4. **实验内容**

设计针对中文的凯撒密码加密和解密程序

1. 熟悉从键盘读入数据，以及数据类型之间的转换方式。
2. 了解加密解密方法，寻找较为完善，不易破译的加密方式。
3. 实现字符串与列表的转换，增加，删除操作。

**三．实验步骤以及结果**

1.编码源代码**：**

import random  
str=input("输入字符串： ")  
a=random.randint(2,20)  
key=pow(a,11,221)  
str2=""  
for i in range(len(str)):  
 str2 += chr(ord(str[i])-a)  
print("加密字符串为：{}".format(str2))  
print(key)

2.译码源代码：

s1=input()  
s2=input()  
key=int(s2)  
str3=""  
a=pow(key,35,221)  
for i in range(len(s1)):  
 str3 += chr(ord(s1[i])+a)  
  
print("原字符串为：{}".format(str3))

1. 代码步骤具体分析：

一：编码具体步骤

1. 从键盘读入字符串str。
2. 生成一个随机偏移量a。
3. 是字符串str的每一个字符都减去偏移量a得到一个加密字符串str2.
4. 使用rsa非对称加密方式对随即偏移量a通过公钥加密方式C ＝ ME mod N进行加密处理得到key。
5. 输出加密后的字符串str2，以及key。

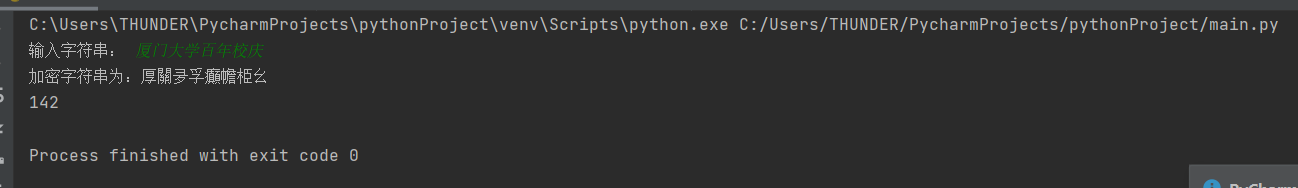
二：解码具体步骤

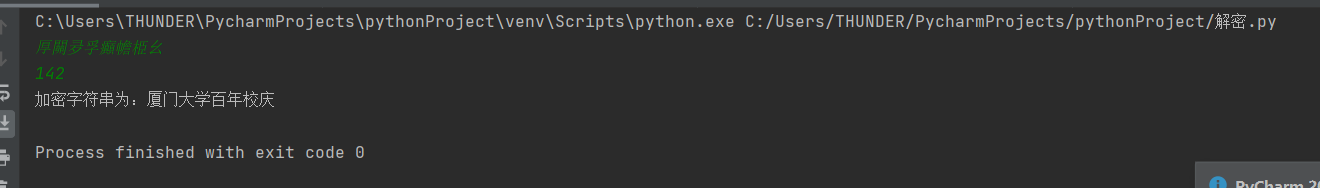
1. 读入编码得到的字符串str2以及key。
2. 将key通过私钥解密方式M ＝CD mod N得到真实偏移量a。
3. 是字符串str2的每一个字符都加上真实偏移量a还原得到原字符串。
4. 输出解密后的原字符串。
5. rsa非对称加密方式分析：



就以我的上述程序所采用的加密方式来看：

1. 选取两个质数P=13和Q=17。
2. 其公共模数为N=13\*17=221。
3. 欧拉函数的值为φ(N)=12\*16=192.
4. 计算公钥E。由于E的取值必须是整数，且E 和 φ(N) 必须是互质数，因此选取11为公钥E
5. 计算私钥D：私钥D需满足E \* D % φ(N) = 1这个条件。因此找到数字35。能够符合该条件。
6. 加密公式：C ＝ ME mod N将偏移量M加密，得到一个传递给解密程序，但除解密程序外他人无法破译数字C（也就是程序中的key）
7. 解密公式：M ＝CD mod N，通过加密公式传过来的c就能找到原本的偏移量M。
8. 分析可得，当两个素数较大时，几乎没有破译的可能性。
9. **实验结果与分析**

加密结果：

解密结果：

分析：

1. 该实验较好的完成了实验任务，能够较为安全的实现字符串的加密解密，并且破译难度较高。
2. 框架的编写让我能够熟悉python中字符串，列表，随机数等许多较为基本的操作，也是第一次较为完整的完成一个python程序。
3. 实验最困难的部分是在如何寻找一个良好的加密解密方式。大体框架编写完成后，我先试着能否在字符串中传递信息，但这样的方法极其容易被破译。后来试着使用较为复杂的函数。但是线性的函数安全性依然较低。因此最后选择了rsa加密的方法，从零开始阅读学习了解。最后发现，其实最终写在代码中只需key=pow(a,11,221)和a=pow(key,35,221)。便能够实现加密和解密的作用。这样一个学习探索的过程让我有了很大的收获。

**五．实验总结**

这是第一次的python上机实验，让我收获颇丰。第一，熟悉使用了python中字符串，列表等基本数据结构的操作。学会了随机数，取余等函数的使用。第二，对python语言有了更深刻的理解，知道了该语言与其它语言之间相比的优越性和不足。第三，自主学习了一种较为安全的编码译码方式，这也是第一次接触密码这个领域。摸索，研究的过程让我对将来的学习越来越感到憧憬。