**Python实验 实验报告**

**实验题目： 中文加密程序**

**专 业： 人工智能**

**姓 名： 吴浩**

**学 号： 22920192204092**

**实验日期**： 2021-3-25

1. **实验目的**

**设计一个程序来实现对中文字符串的加密和解密。要求一定的安全性，每次加密程序会出现不一样的密文。**

1. **实验内容**

**编写python程序，来实现加密和解密过程。**

**加密程序：**

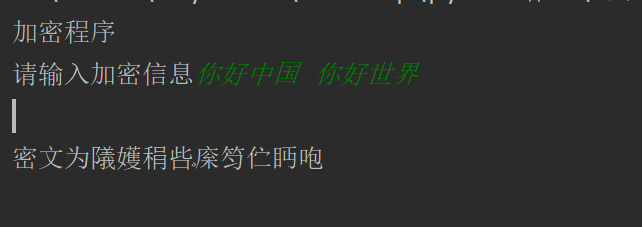
# 基本汉字的Unicode 编码范围为 19958 - 40869  
# 40869-19958=20911  
import random  
print("加密程序")  
code = input("请输入加密信息")  
lst = []  
for item in code:  
 lst.append(ord(item))  
ans = ''  
key0 = random.randint(0, 20000)  
key = key0  
for item in lst:  
 item = item ^ key  
 # 变成密文  
 # 下一个密钥为密文+key  
 key = (item + key) % 20000  
 ans = ans + chr(item)  
last =(key0 + len(ans)) % 20911 + 19958  
ans += chr(last)  
print(f"\n密文为{ans}")

**解密程序：**

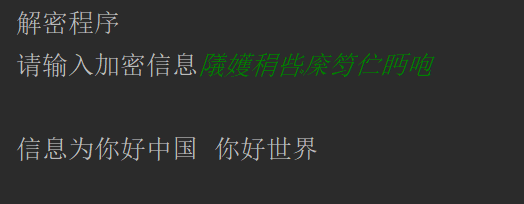
print("解密程序")  
code = input("请输入加密信息")  
lst = []  
length = len(code)  
key = ord(code[length-1])-19958-(length-1) % 20911  
key2 = key  
for item in code:  
 lst.append(ord(item))  
ans = ''  
for item in lst[:-1]:  
 #下一个密钥为 密文+key  
 key = (item + key) % 20000  
 item = item ^ key2  
 # 变成明文  
 key2 = key  
 ans = ans + chr(item)  
  
print(f"\n信息为{ans}")

1. **实验步骤以及结果**

**运行第一个程序，输入‘你好中国 你好世界’**



运行第二个程序，输入密文



其他测试也能很好的通过。

**加密过程是随机数生成密钥，每次可以得到不一样的密文。解密程序可以通过密文得到设定的随机数，这样就可以用加密程序的逻辑来进行解密。**

**同时，加密过程每一个字符都有一个单独的密钥。这个密钥必须要知道上个密钥和密文才能到。获取第一个密钥需要读取字符串最后一个字符，但是我通过加密的方式，将其置为中文，和其他密文在一起比较难辨别。**

**密文的Unicode码和源码相比，二进制码的后11位可能会发生变化，其他位置保持不变。这样保证了密文往往在中文字符范围内，不会出现不可识别的Unicode码。**

1. **实验结果与分析**

**实验结果还是很成功的，在测试过程中没有出现bug，面对非中文字符也能很好的加密。每次加密都是不同的字符串，这样可以防止被破解部分字符数据而得知全体的情况。**

**不足之处在于密文总是比原文长度大1，这样就可能猜出来密文的某一位存储着密钥。然后再通过二进制代码分析，就有可能知道密钥的具体值。**

**可以改进的方法，在存储第一位密钥时，可以根据原文的长度，将一份密钥分放好几位。或者密文在解密过程，可以按照非线性的方式进行解密，先解密头部，和尾部，在解密中间。**

**实验总结**

**在本次实验中，我们学好利用python来解决一些问题。相比于C/C++，python的代码量更少，可以让我们将更多的时间放在思考算法设计中，而不需要过多思考的程序设计方面的内容。节省了大量时间。**

**同时，这次实验也让我了解了不少关于密码学的知识，知道了现代加密的方式。知道了如何面对常见的破解密码方式。**