**Python程序设计实验报告**

**实验题目： 中文的凯撒加密与解密**

**专 业： 人工智能**

**姓 名： 莫松寅**

**学 号： 22920192204042**

**实验日期**： 3/25

1. **实验目的**

设计实现针对中文的凯撒密码的加密和解密程序。

1. **实验步骤以及结果**

思路分析：

实验要求用两个独立程序分别进行加密和解密，同时偏移量要求动态。

对于加密和解密，可以使用ord（）函数来使汉字转化为数字，在通过加减进行偏移，最后用chr()函数反过来把数字转化为汉字。

最大的难点在于如何隐藏偏移量，最开始的思路是将偏移量隐藏在加密的长码中，但是由于汉字的数字范围大概在2万至17万，数字难于隐藏，所以放弃这种方法，将思路转到了简单模仿现在银行使用的加密方式。

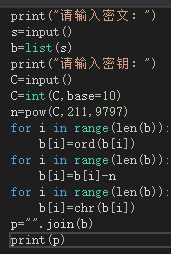
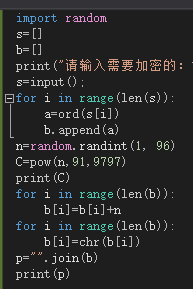
解决方法：

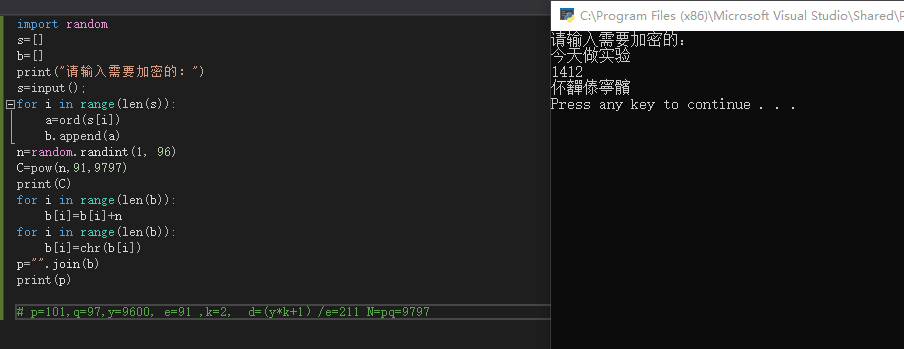
RSA加密算法。根据RSA算法的思想，可以利用两个素数塑造两个不相等的密钥，利用他们的乘积作为公钥，再找出一个素数作为加密暗码，就可以运用公式得出另一个不相等的解密暗码，通过公钥^暗码%乘积的方法就可以得出相同的偏移量。

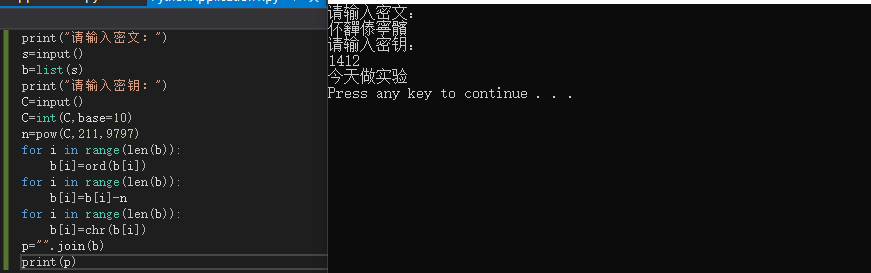
下图 为我选定的数据：

9_X2LN]7Q6S`~5AS8D_0]FU

从而可以写出代码



**三.实验结果与分析**

****

成功加密并解密

**四．实验总结**

成功完成了实验，做实验时了解了ord（）与chr（）的函数，学习了rsa算法，并初步尝试在了自己的代码中，成功进行了不对称加密。