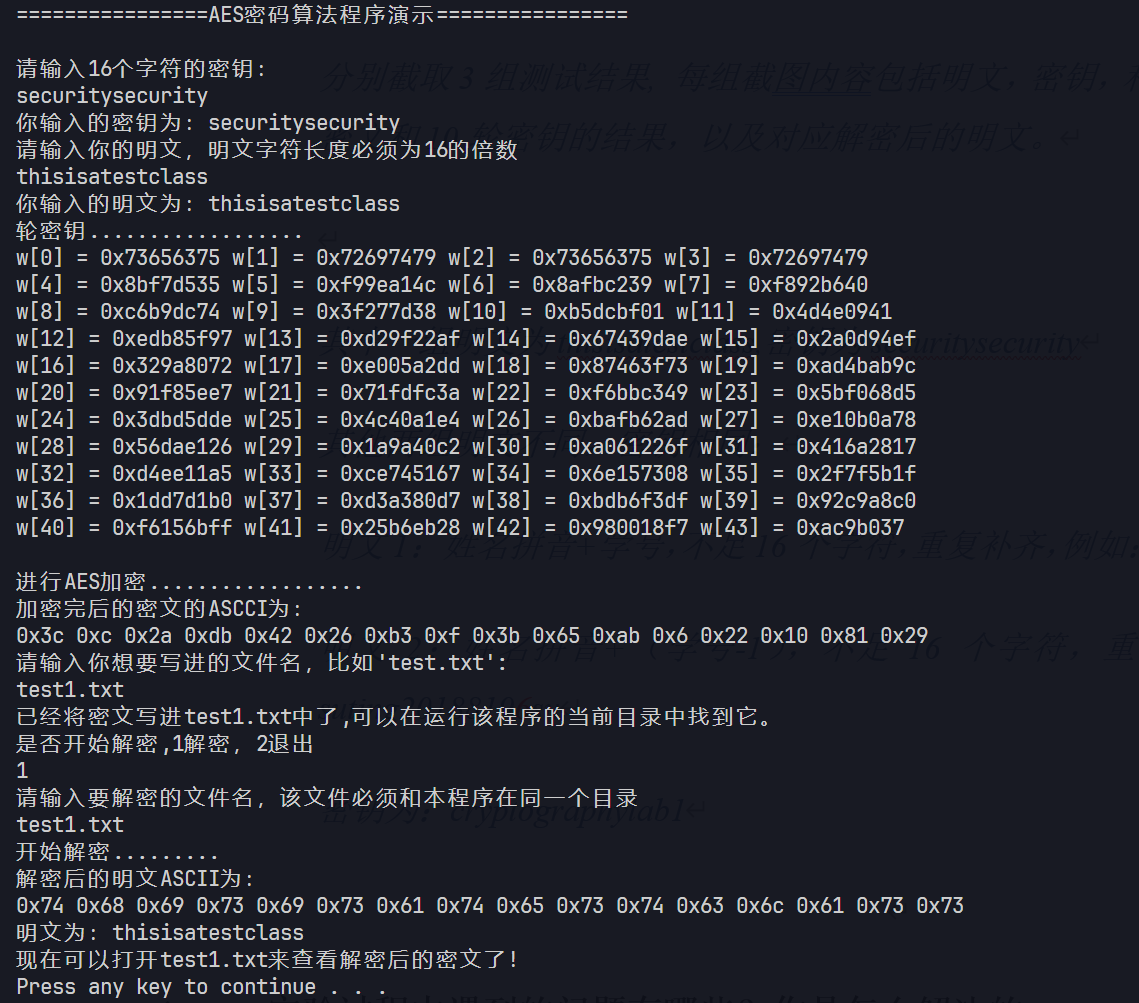
**实验一 AES密码算法**

**姓名：\_\_\_\_\_\_\_李子韬\_\_\_\_\_\_\_\_学号：\_\_\_\_\_\_220110609\_\_\_\_\_\_\_\_\_**

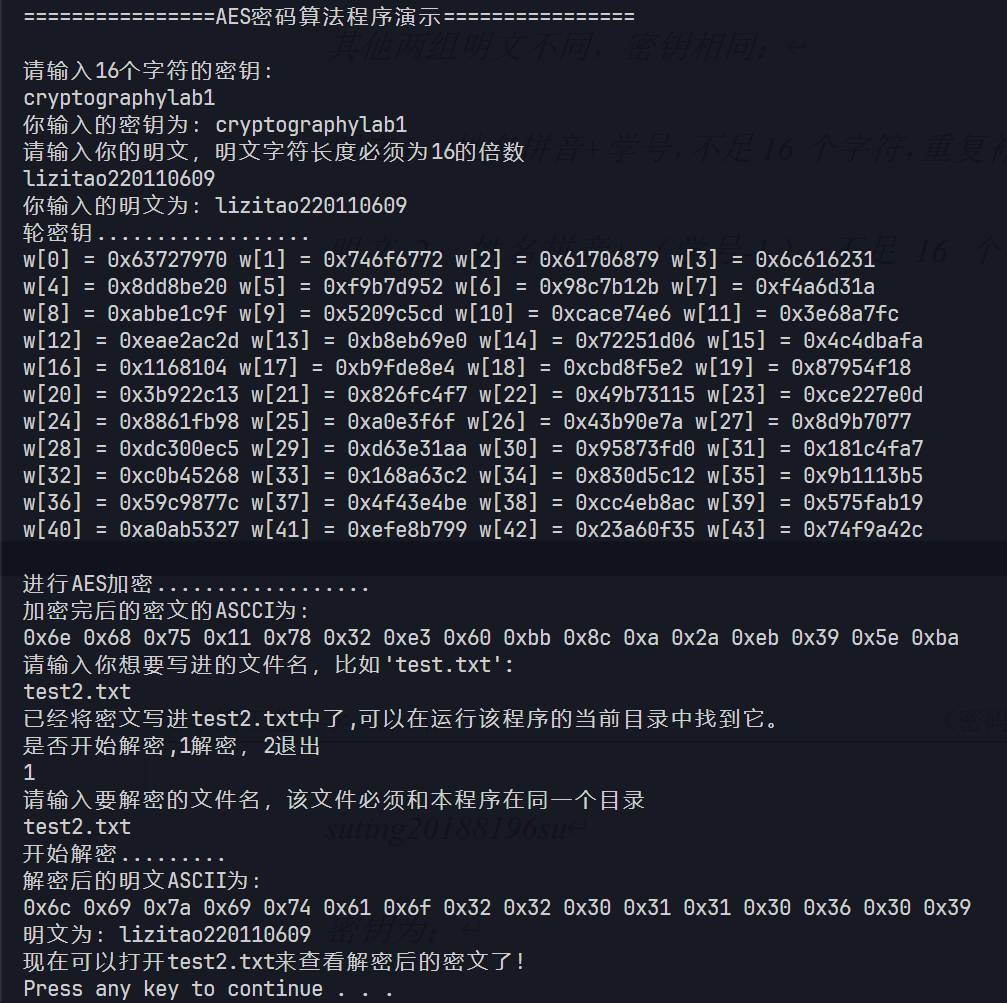
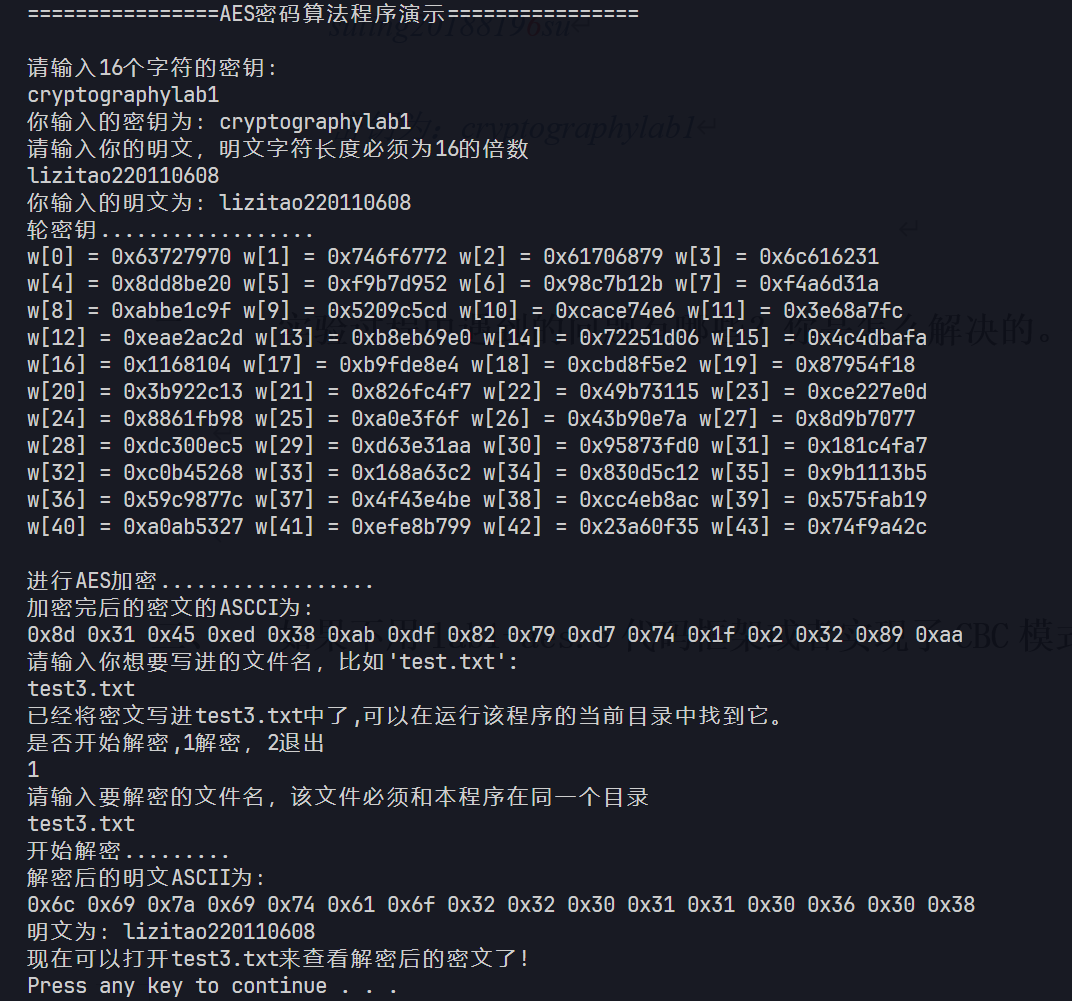
1. **运行截图**

*分别截取3组测试结果, 每组截图内容包括明文，密钥，和对应密钥加密的密文和10轮密钥的结果，以及对应解密后的明文。*

*其中一组明文为thisisatestclass,密钥为securitysecurity*

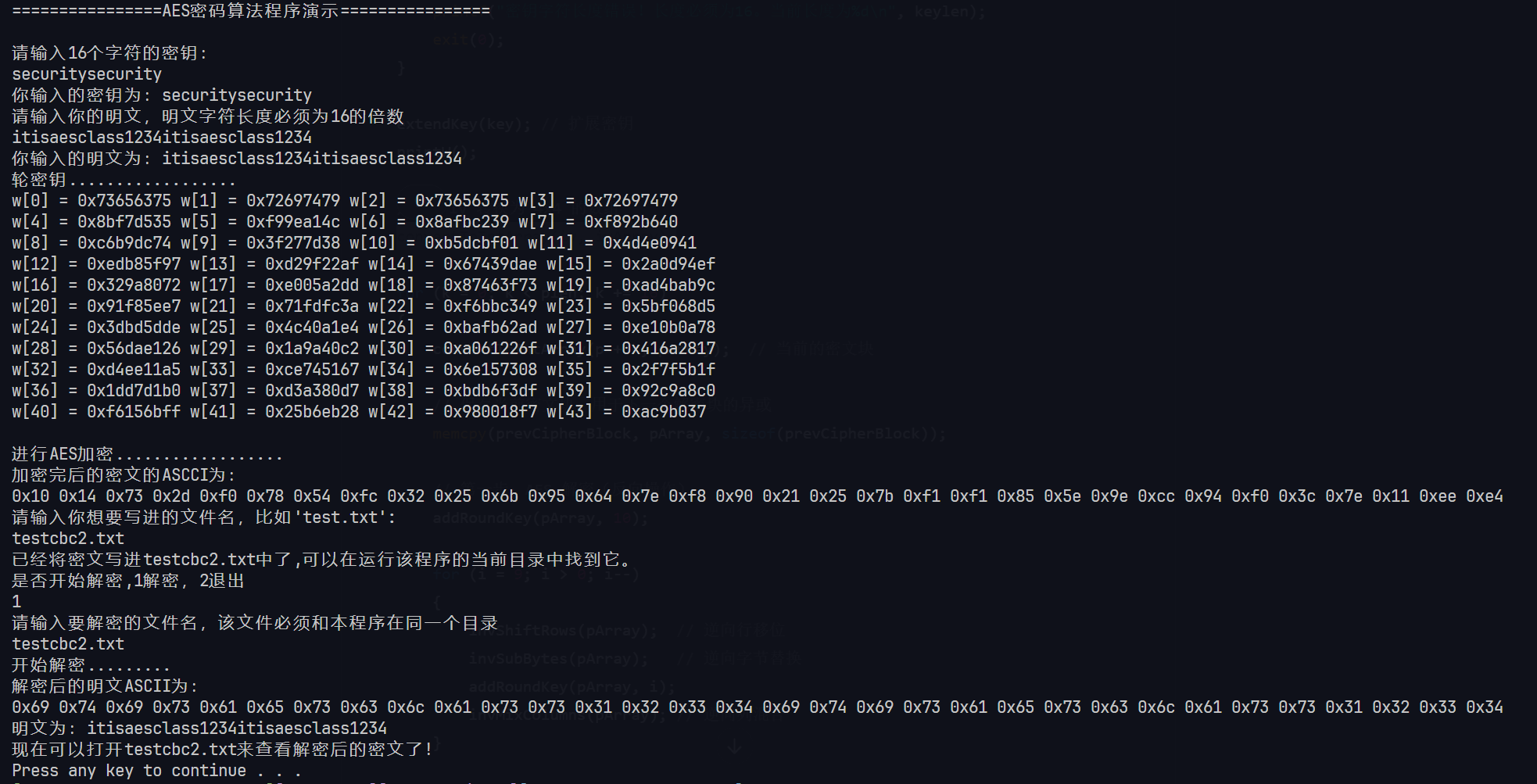
*其他两组明文不同，密钥相同：*

*明文1： 姓名拼音+学号，不足16个字符，重复补齐，例如：suting20188197su*

*明文2：姓名拼音+（学号-1），不足16个字符，重复补齐，例如：suting20188196su*

*密钥为：cryptographylab1*

1. **实验过程中遇到的问题有哪些？你是怎么解决的。**
2. *刚刚写完的时候，测试发现结果有误，观察轮密钥发现错误从第二轮开始产生，于是检查轮密钥算法，发现c语言右移对int不是逻辑右移，于是对右移24位的操作采用AND 0x000000ff的操作，并对轮密钥模块单元测试解决*
3. *Gcc编译时没有这个命令，发现是环境变量PATH之前没配好，索性配了后gcc -o编译成功*
4. **如果不用lab1-aes.c代码框架或者实现了CBC模式，请说明。**

*实现了cbc模式：*

*可以发现，这里测试使用的是验证样例的密钥和文本，不过我们将文本重复一遍，初始向量选择了0000 0000 0000 0000，这会使得循环密文的第一部分和验证样例一样，观察密文可知，两段密文不重复，可以判断cbc模式生效，解密也能解出两个循环的明文；*

*至于实现方式，则是新加入一个iv变量(char[16])做初始向量，在处理完每个分组的密文之后，将这个密文memcpy到ivArray内替代初始向量，循环执行即可；解密时，将过程反过来，不过需要保存当前的密文来为下一个循环做异或；（具体可参照lab1-aes-cbc.c）*