**实验一 AES密码算法**

**姓名：\_\_\_\_\_\_\_\_\_梁鑫嵘\_\_\_\_\_\_\_\_\_\_学号：\_\_\_\_\_\_\_\_\_200110619\_\_\_\_\_\_\_\_**

1. **运行截图**

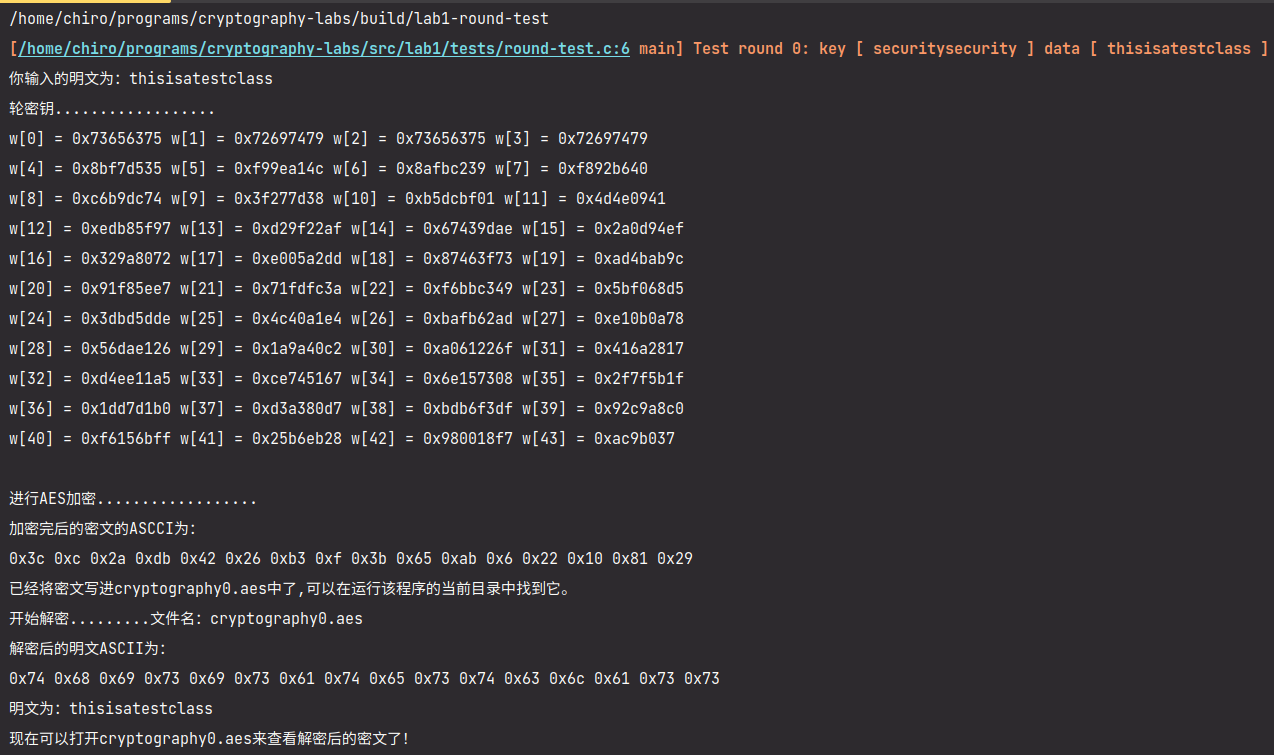
*分别截取3组测试结果, 每组截图内容包括明文，密钥，和对应密钥加密的密文和10轮密钥的结果，以及对应解密后的明文。*

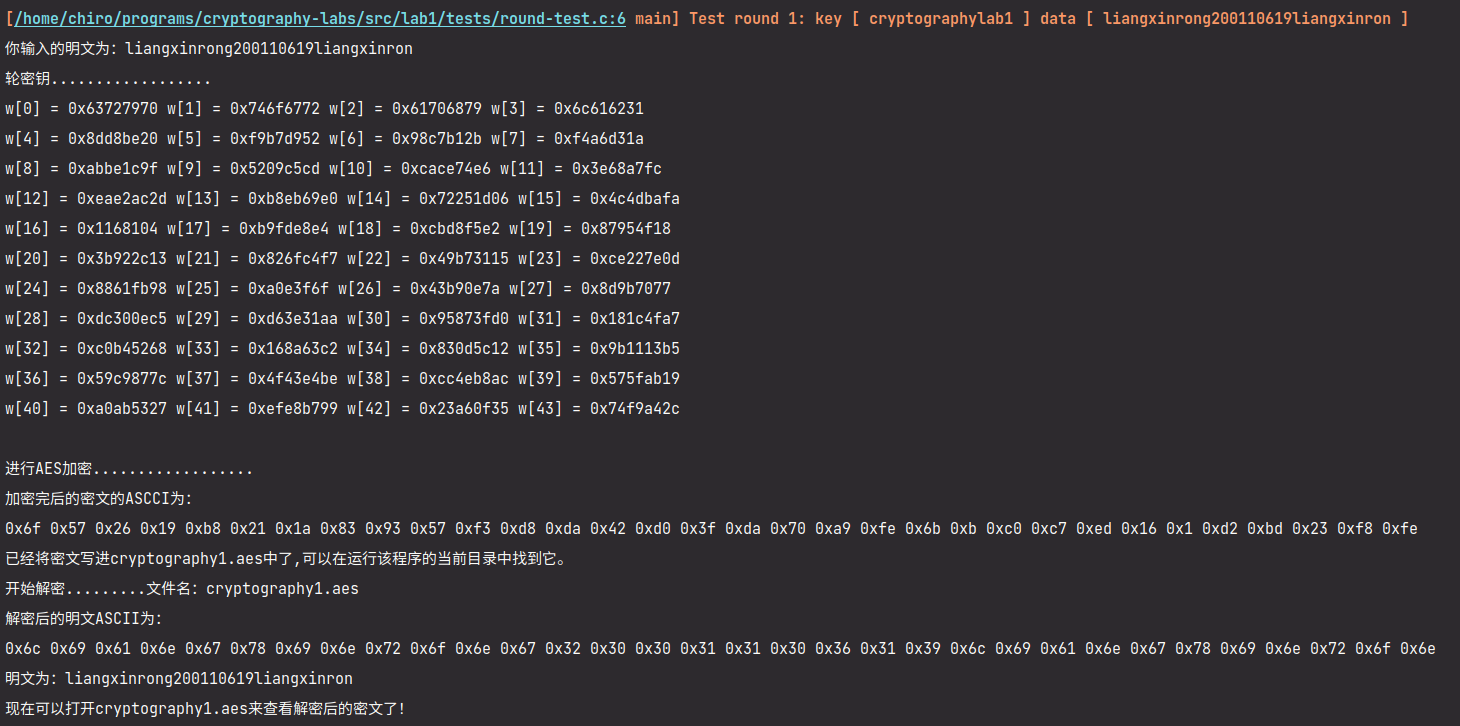
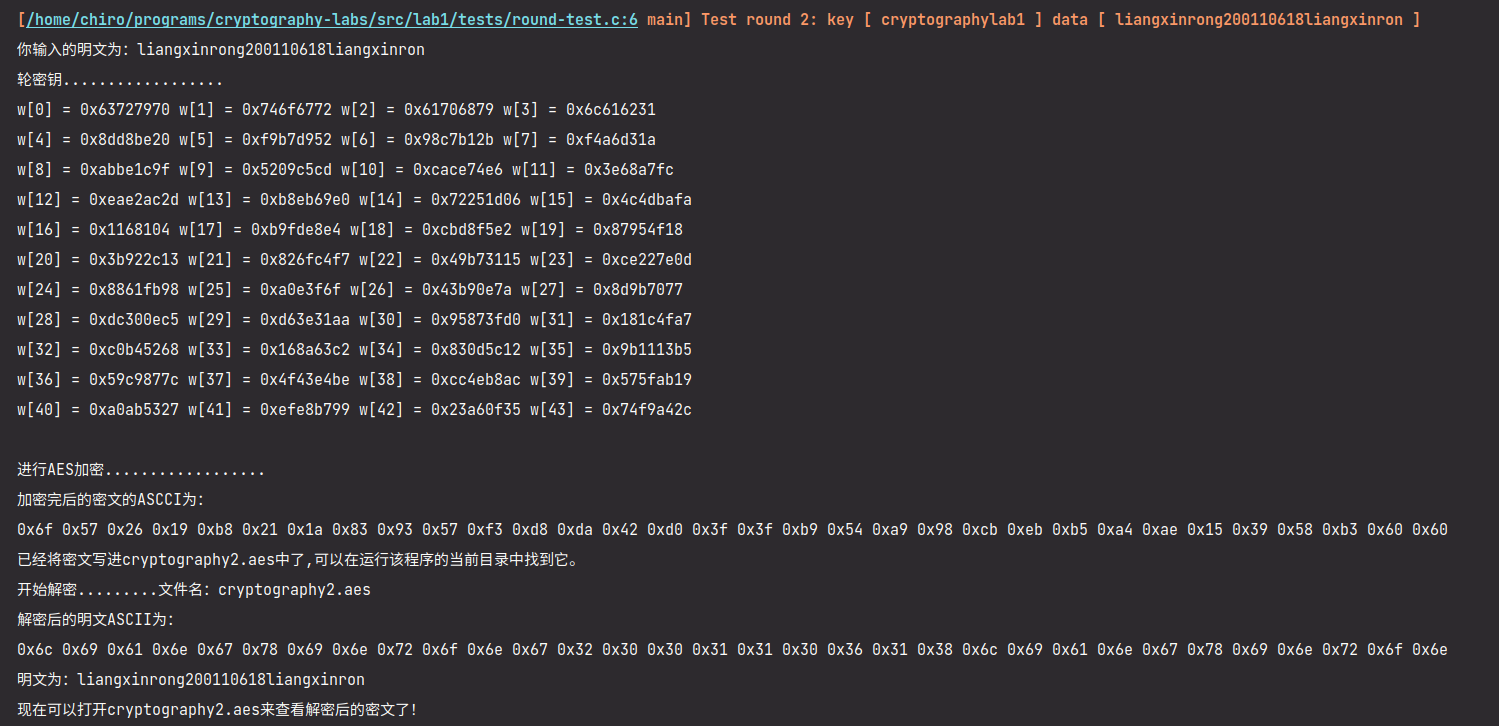
*其中一组明文为thisisatestclass,密钥为securitysecurity*

*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. *问题：程序测试每次都需要重新读取键盘输入数据*

*解决：每次运行的时候配置一个全局配置，忽略键盘输入。*

1. *问题：加密过程中怎么尝试结果都不正确*

*解决：Rcon数组的长度和 PPT 中式子没有对应上，需要给 Rcon[0] 补上*

1. **如果不用lab1-aes.c代码框架或者实现了CBC模式，请说明。**