**实验一 AES密码算法**

**姓名：\_\_\_\_\_吴梓滔\_\_\_\_\_\_\_学号：\_\_\_\_\_\_\_220110430\_\_\_\_\_\_\_\_\_\_**

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*

用例1： 明文 thisisatestclass，密钥securitysecurity

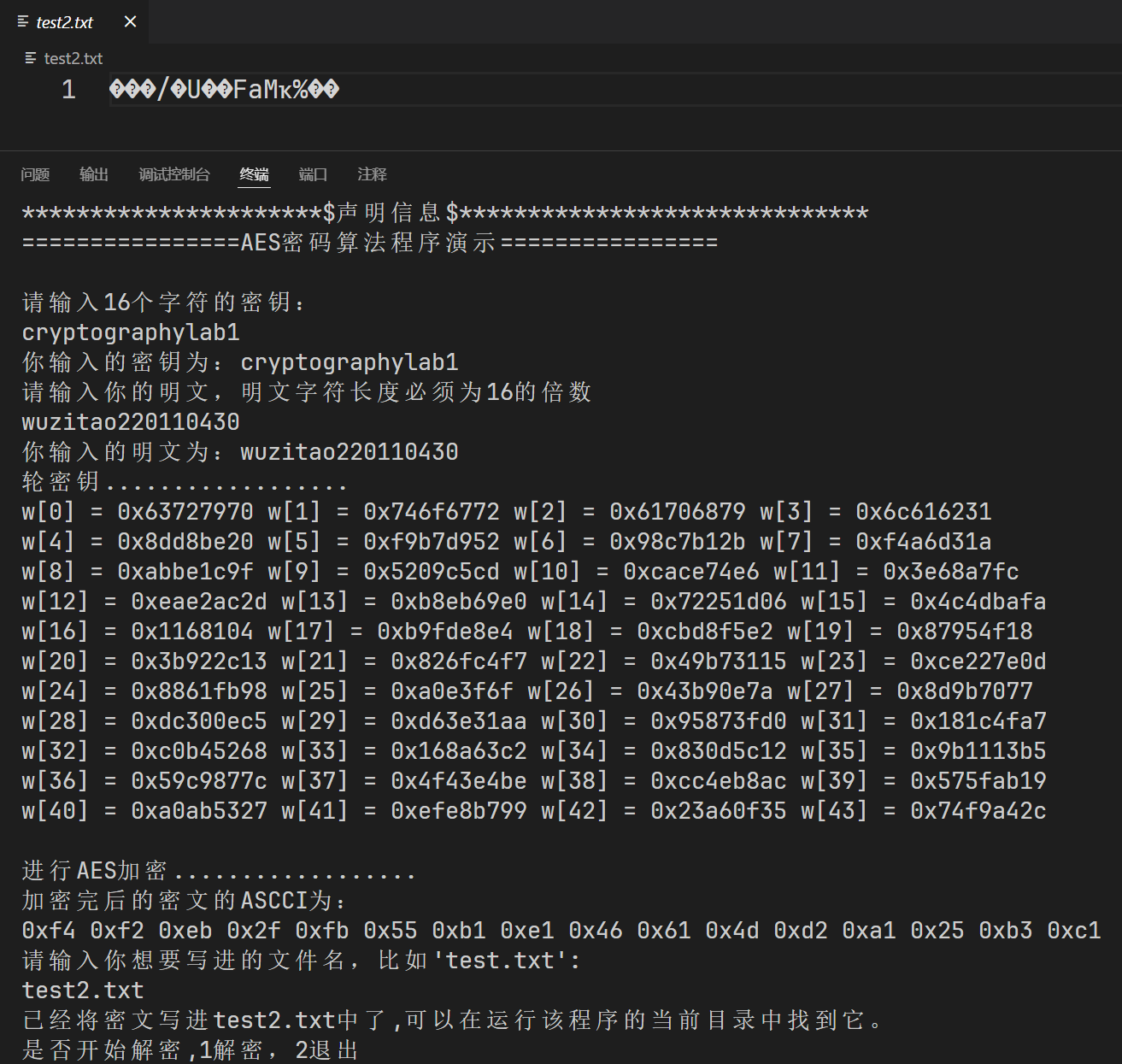
文本

描述已自动生成

文本

描述已自动生成

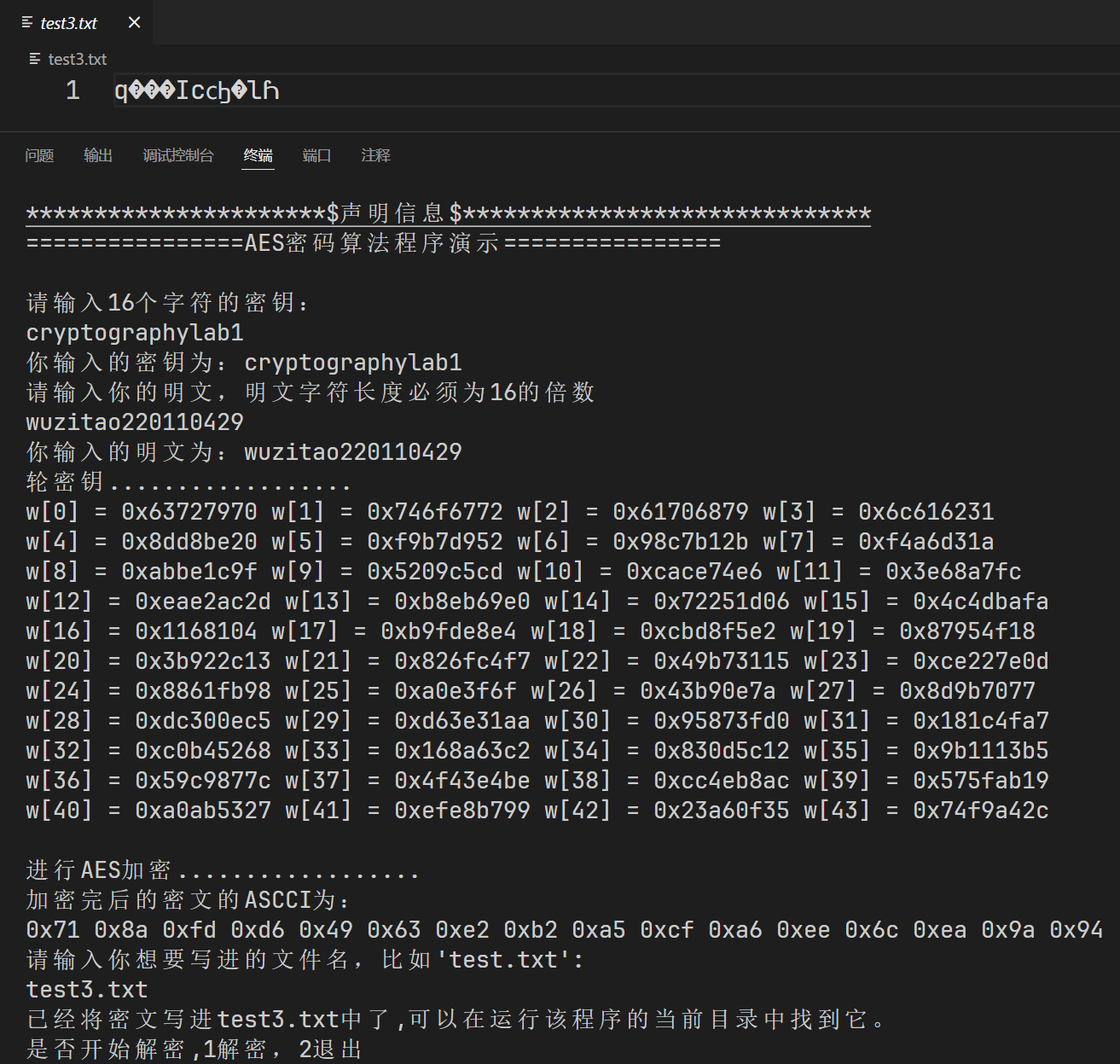
用例2 明文wuzitao220110430 密钥 cryptographylab1



文本

描述已自动生成

用例3 明文wuzitao220110429 密钥 cryptographylab1



文本

描述已自动生成

1. **实验过程中遇到的问题有哪些？你是怎么解决的。**

加密后解密得到的明文不正确。仔细对比了输出，发先密钥的前4个和参考案例是一致的，此后全部不一致。因此判断是密钥扩展环节出了问题。检查了实现的各个函数，发现是extendKey函数的实现出错，使得扩展密钥w[0:3]是正确的，后面全是错误的。修改了该函数后就得到了正确的输出。

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