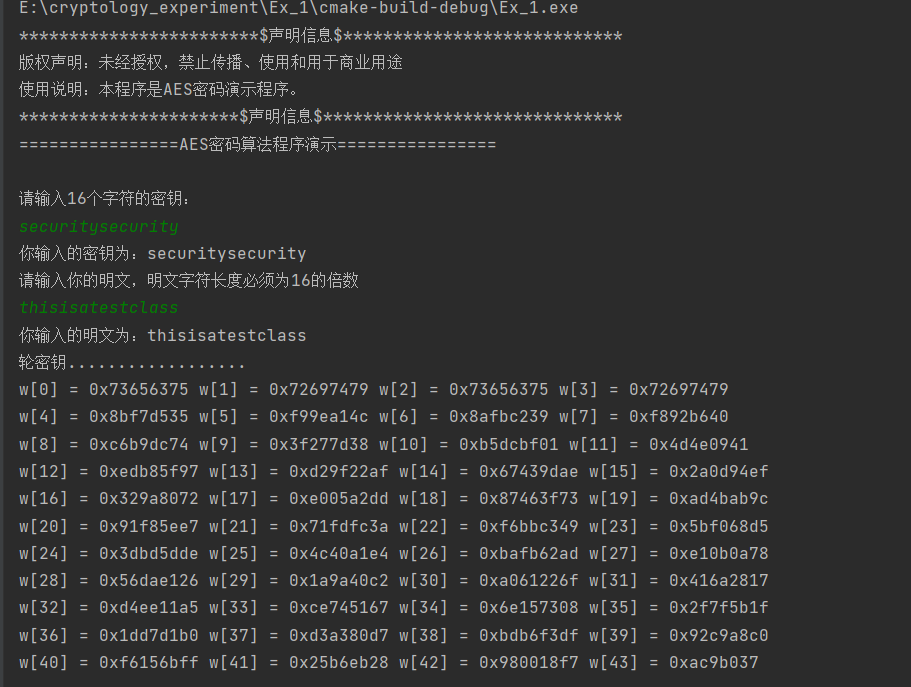
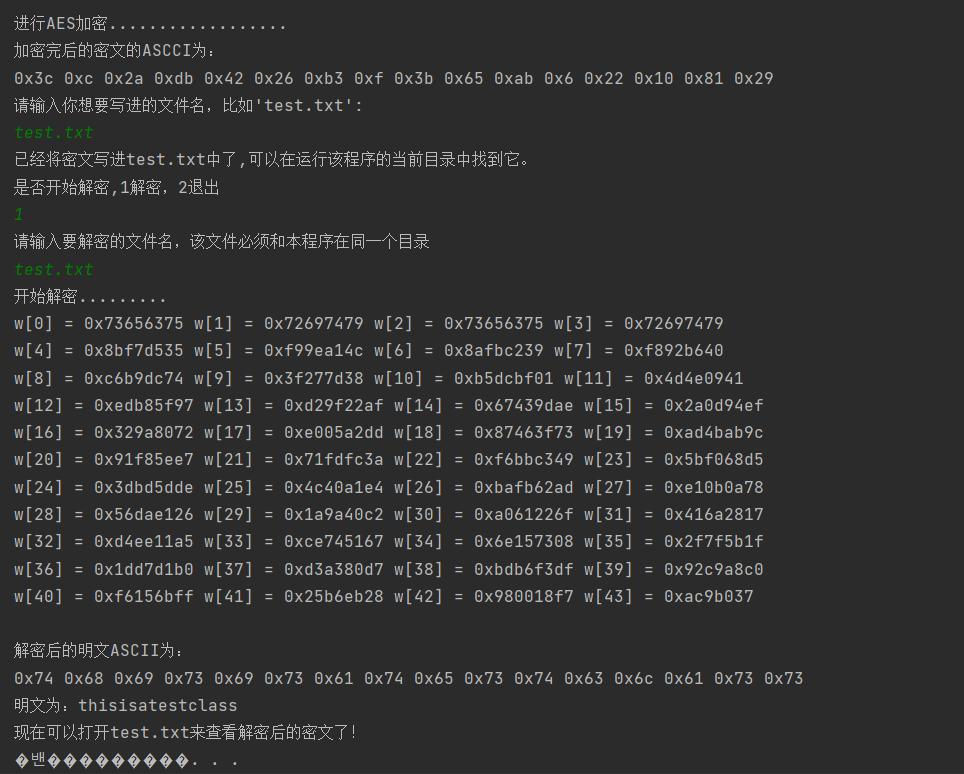
**实验一 AES密码算法**

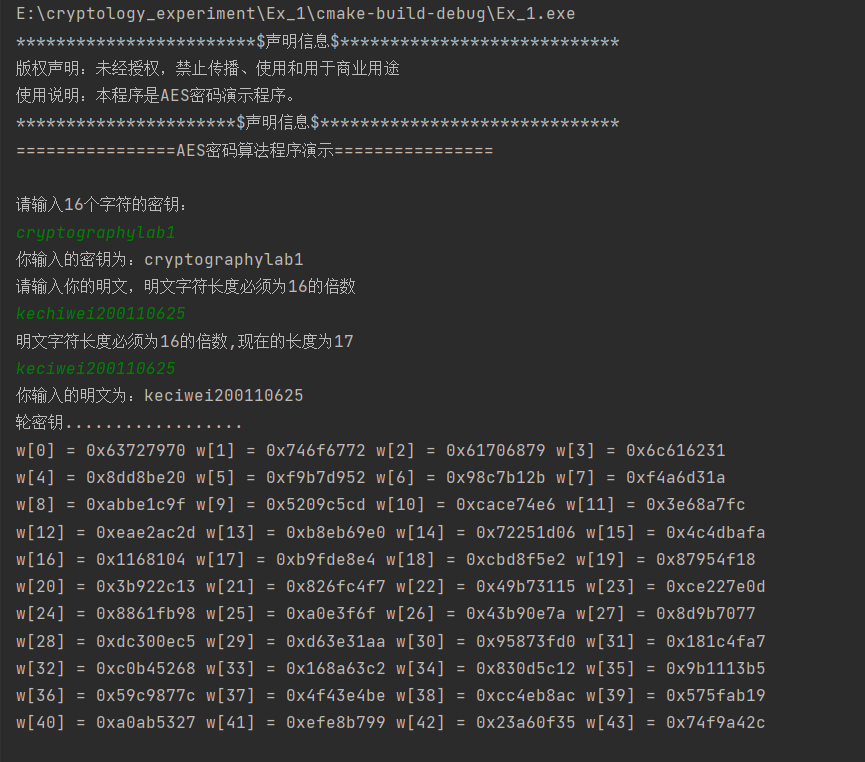
**姓名：\_\_\_\_\_\_\_\_\_\_柯炽炜\_\_\_\_\_\_\_\_\_\_\_学号：\_\_\_\_200110625\_\_\_\_\_\_\_**

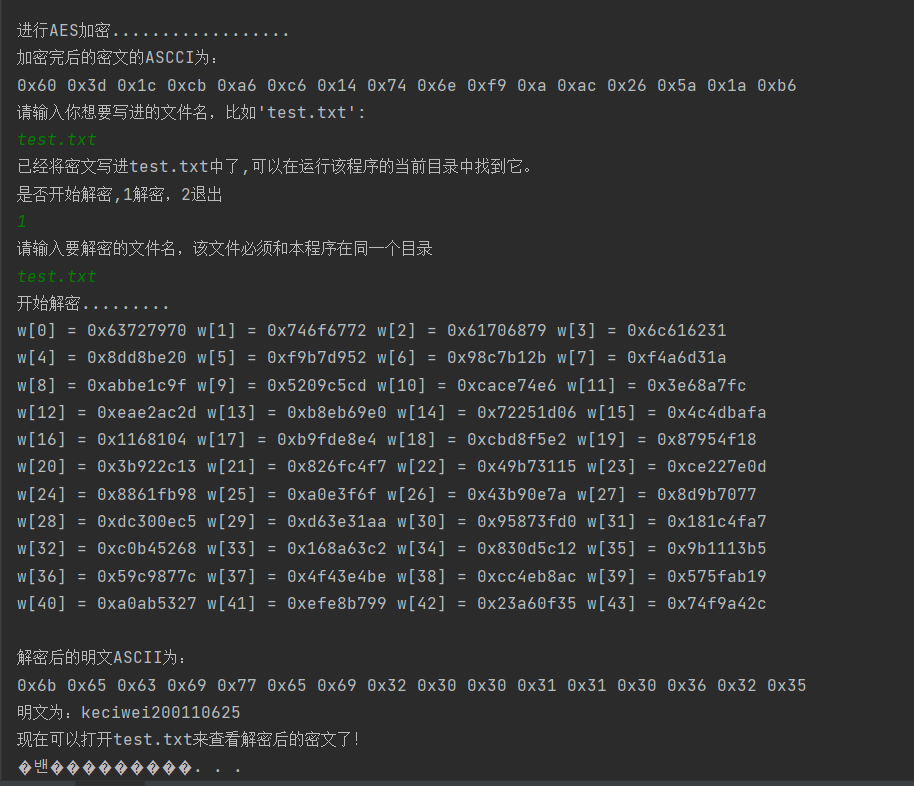
1. 运行截图
   1. 明文为thisisatestclass,密钥为securitysecurity



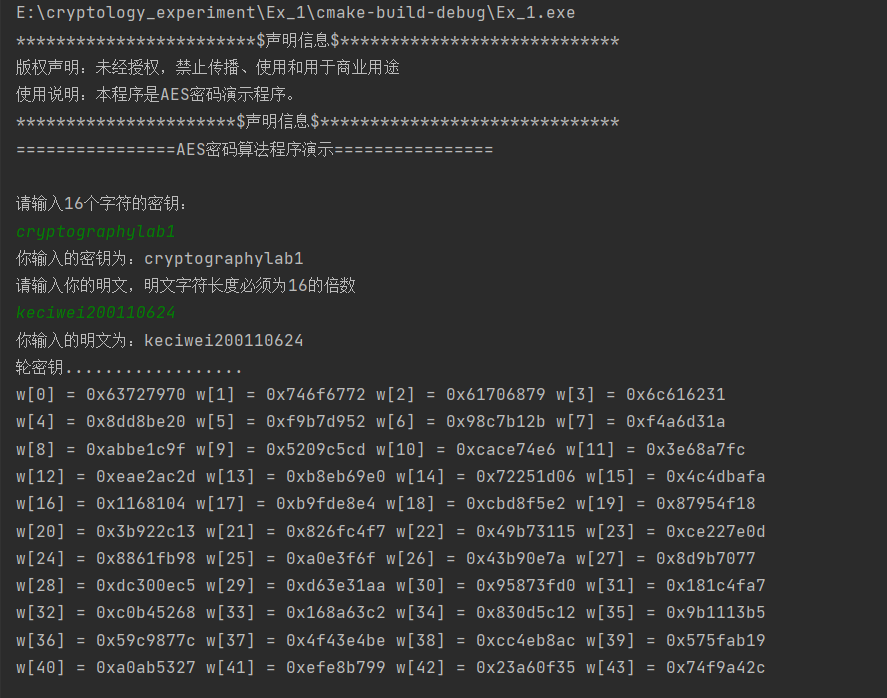


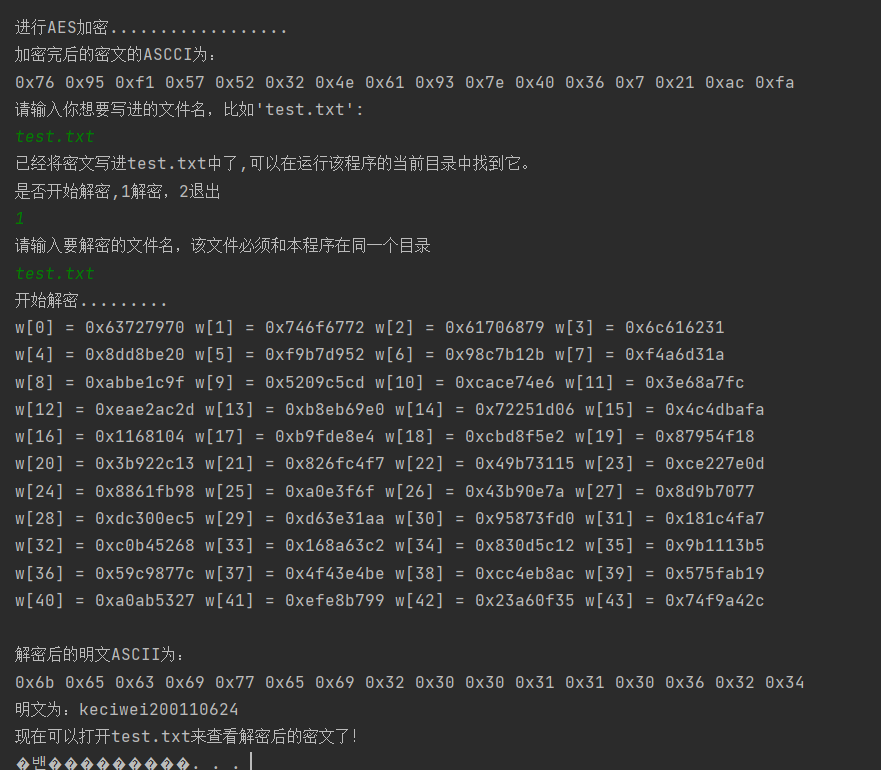
* 1. 明文：keciwei200110625，密钥：cryptographylab1





* 1. 明文：keciwei200110624，密钥：cryptographylab1





1. 实验过程中遇到的问题有哪些？你是怎么解决的。
2. 在列混淆函数中，需要实现4\*4的矩阵乘法，而在做实验时总是发现结果不正确。
   1. 解决措施：通过回看课件发现AES算法是在GF（2）域中进行，而在这个域中的加法为异或操作。将代码中的加法改为异或则结果正确
3. 在轮密钥加函数中，出现两个问题：
   1. 问题一同上：加法未改成异或（解决措施：将加法改成异或即可）
   2. 问题二：array矩阵在读入时结构为按列存储，而在代码中我一开始习惯性的按行读取，因此总是结果对不上（解决措施：通过进一步阅读源码从而发现bug所在）