实验一 AES 密码算法

姓名：_____房煊梓_____学号：_____210010101____ ____

一、 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:suting201881977su

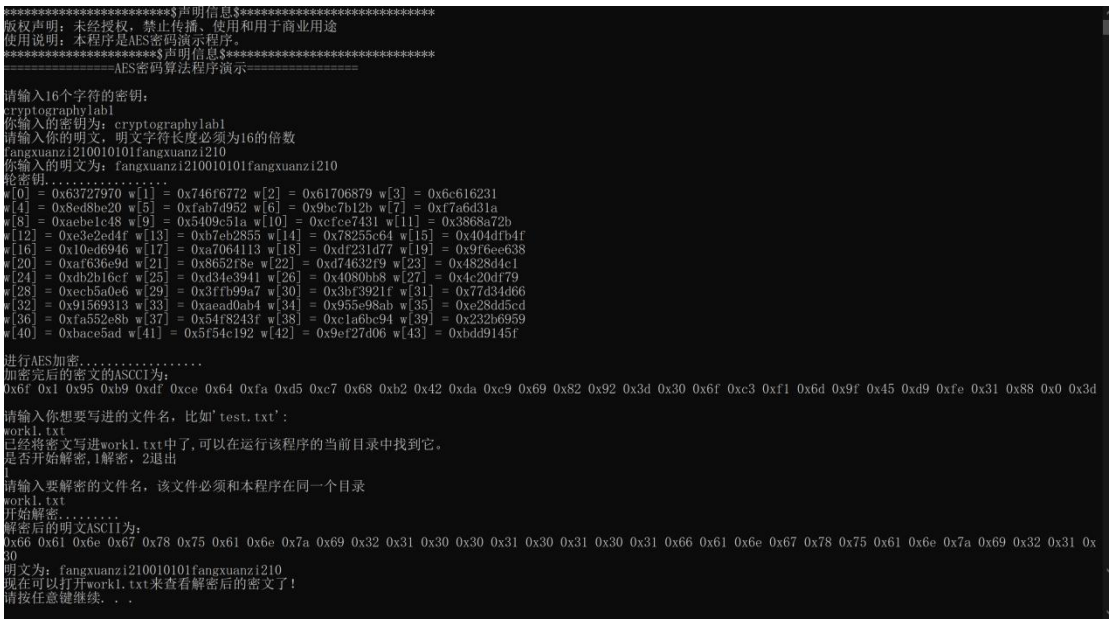
明文 2：姓名拼音+（学号-1），不足 16 个字符，重复补齐，例如：suting201881966su

密钥为：cryptographylab1

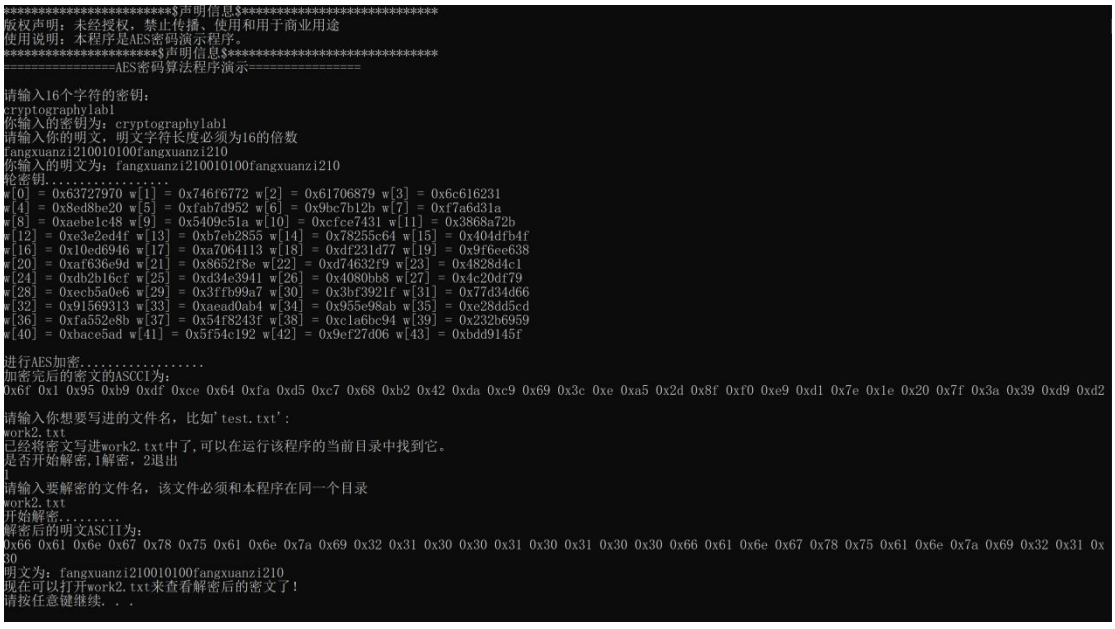
1.

```
**********$声明信息$**********
版权声明：未经授权，禁止传播、使用和用于商业用途
使用说明：本程序是AES密码演示程序。
**********$声明信息$**********
==========AES密码算法程序演示==========

请输入16个字符的密钥：
securitysecurity
你输入的密钥为：securitysecurity
请输入你的明文，明文字符长度必须为16的倍数
thisisatestclass
你输入的明文为：thisisatestclass
轮密钥.....
w[0] = 0x73656375 w[1] = 0x72697479 w[2] = 0x73656375 w[3] = 0x72697479
w[4] = 0x88f7d535 w[5] = 0xfa9ea14c w[6] = 0x89fbc239 w[7] = 0xfb92b640
w[8] = 0xc3b9dc3a w[9] = 0x39277d76 w[10] = 0xb0dcbf4f w[11] = 0x4b4e090f
w[12] = 0xe4b8aa89 w[13] = 0xdd9fd7ff w[14] = 0x6d4368b0 w[15] = 0x260d61bf
w[16] = 0x2357a27e w[17] = 0xfec87581 w[18] = 0x938b1d31 w[19] = 0xb5867c8e
w[20] = 0x4747bbab w[21] = 0xb98fce2a w[22] = 0x2a04d31b w[23] = 0x9f82af95
w[24] = 0x143e9170 w[25] = 0xadb15f5a w[26] = 0x87b58c41 w[27] = 0x183723d4
w[28] = 0xe18d9dd w[29] = 0xa3a98687 w[30] = 0x241c0ac6 w[31] = 0x3c2b2912
w[32] = 0xe4bd1036 w[33] = 0x471496b1 w[34] = 0x63089c77 w[35] = 0x5f23b565
w[36] = 0xf4685df9 w[37] = 0xb37ccb48 w[38] = 0xd074573f w[39] = 0x8f57e25a
w[40] = 0xaff0e38a w[41] = 0x1c8c28c2 w[42] = 0xccf87ffd w[43] = 0x43af9da7

进行AES加密.....
加密完后的密文的ASCCI为：
0xd2 0xcd 0xae 0x8c 0x68 0x19 0x5 0xce 0x60 0x78 0x57 0x4b 0xc2 0x83 0xb6 0x4a
请输入你想要写进的文件名，比如'test.txt'：
test.txt
已经将密文写进test.txt中了,可以在运行该程序的当前目录中找到它。
是否开始解密,1解密，2退出
1
请输入要解密的文件名，该文件必须和本程序在同一个目录
test.txt
开始解密.....
解密后的明文ASCII为：
0x74 0x68 0x69 0x73 0x69 0x73 0x61 0x74 0x65 0x73 0x74 0x63 0x6c 0x61 0x73 0x73
明文为：thisisatestclass
现在可以打开test.txt来查看解密后的密文了！
请按任意键继续. . .
```

2.



3.



二、 如果是不用模板或者实现了 CBC 模式，请说明。