实验一 AES 密码算法

姓名：_____李子韬_____学号：_____220110609_____

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。

```
================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] = 0x8bf7d535 w[5] = 0xf99ea14c w[6] = 0x8afbc239 w[7] = 0xf892b640
w[8] = 0xc6b9dc74 w[9] = 0x3f277d38 w[10] = 0xb5dcbf01 w[11] = 0x4d4e0941
w[12] = 0xedb85f97 w[13] = 0xd29f22af w[14] = 0x67439dae w[15] = 0x2a0d94ef
w[16] = 0x329a8072 w[17] = 0xe005a2dd w[18] = 0x87463f73 w[19] = 0xad4bab9c
w[20] = 0x91f85ee7 w[21] = 0x71fdfc3a w[22] = 0xf6bbc349 w[23] = 0x5bf068d5
w[24] = 0x3dbd5dde w[25] = 0x4c40a1e4 w[26] = 0xbafb62ad w[27] = 0xe10b0a78
w[28] = 0x56dae126 w[29] = 0x1a9a40c2 w[30] = 0xa061226f w[31] = 0x416a2817
w[32] = 0xd4ee11a5 w[33] = 0xce745167 w[34] = 0x6e157308 w[35] = 0x2f7f5b1f
w[36] = 0x1dd7d1b0 w[37] = 0xd3a380d7 w[38] = 0xbdb6f3df w[39] = 0x92c9a8c0
w[40] = 0xf6156bff w[41] = 0x25b6eb28 w[42] = 0x980018f7 w[43] = 0xac9b037

进行AES加密..................
加密完后的密文的ASCCI为:
0x3c 0xc 0x2a 0xdb 0x42 0x26 0xb3 0xf 0x3b 0x65 0xab 0x6 0x22 0x10 0x81 0x29
请输入你想要写进的文件名，比如'test.txt':
test1.txt
已经将密文写进test1.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
test1.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test1.txt来查看解密后的密文了!
Press any key to continue . . .
```

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：

```
================AES密码算法程序演示================

请输入16个字符的密钥:
cryptographylab1
你输入的密钥为: cryptographylab1
请输入你的明文，明文字符长度必须为16的倍数
lizitao220110609
你输入的明文为: lizitao220110609
轮密钥..................
w[0] = 0x63727970 w[1] = 0x746f6772 w[2] = 0x61706879 w[3] = 0x6c616231
w[4] = 0x8dd8be20 w[5] = 0xf9b7d952 w[6] = 0x98c7b12b w[7] = 0xf4a6d31a
w[8] = 0xabbe1c9f w[9] = 0x5209c5cd w[10] = 0xcace74e6 w[11] = 0x3e68a7fc
w[12] = 0xeae2ac2d w[13] = 0xb8eb69e0 w[14] = 0x72251d06 w[15] = 0x4c4dbafa
w[16] = 0x1168104 w[17] = 0xb9fde8e4 w[18] = 0xcbd8f5e2 w[19] = 0x87954f18
w[20] = 0x3b922c13 w[21] = 0x826fc4f7 w[22] = 0x49b73115 w[23] = 0xce227e0d
w[24] = 0x8861fb98 w[25] = 0xa0e3f6f w[26] = 0x43b90e7a w[27] = 0x8d9b7077
w[28] = 0xdc300ec5 w[29] = 0xd63e31aa w[30] = 0x95873fd0 w[31] = 0x181c4fa7
w[32] = 0xc0b45268 w[33] = 0x168a63c2 w[34] = 0x830d5c12 w[35] = 0x9b1113b5
w[36] = 0x59c9877c w[37] = 0x4f43e4be w[38] = 0xcc4eb8ac w[39] = 0x575fab19
w[40] = 0xa0ab5327 w[41] = 0xefe8b799 w[42] = 0x23a60f35 w[43] = 0x74f9a42c

进行AES加密..................
加密完后的密文的ASCCI为:
0x6e 0x68 0x75 0x11 0x78 0x32 0xe3 0x60 0xbb 0x8c 0xa 0x2a 0xeb 0x39 0x5e 0xba
请输入你想要写进的文件名，比如'test.txt':
test2.txt
已经将密文写进test2.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
test2.txt
开始解密.........
解密后的明文ASCII为:
0x6c 0x69 0x7a 0x69 0x74 0x61 0x6f 0x32 0x32 0x30 0x31 0x31 0x30 0x36 0x30 0x39
明文为: lizitao220110609
现在可以打开test2.txt来查看解密后的密文了!
Press any key to continue . . .
```

```
================AES密码算法程序演示================

请输入16个字符的密钥:
cryptographylab1
你输入的密钥为: cryptographylab1
请输入你的明文，明文字符长度必须为16的倍数
lizitao220110608
你输入的明文为: lizitao220110608
轮密钥..................
w[0] = 0x63727970 w[1] = 0x746f6772 w[2] = 0x61706879 w[3] = 0x6c616231
w[4] = 0x8dd8be20 w[5] = 0xf9b7d952 w[6] = 0x98c7b12b w[7] = 0xf4a6d31a
w[8] = 0xabbe1c9f w[9] = 0x5209c5cd w[10] = 0xcace74e6 w[11] = 0x3e68a7fc
w[12] = 0xeae2ac2d w[13] = 0xb8eb69e0 w[14] = 0x72251d06 w[15] = 0x4c4dbafa
w[16] = 0x1168104 w[17] = 0xb9fde8e4 w[18] = 0xcbd8f5e2 w[19] = 0x87954f18
w[20] = 0x3b922c13 w[21] = 0x826fc4f7 w[22] = 0x49b73115 w[23] = 0xce227e0d
w[24] = 0x8861fb98 w[25] = 0xa0e3f6f w[26] = 0x43b90e7a w[27] = 0x8d9b7077
w[28] = 0xdc300ec5 w[29] = 0xd63e31aa w[30] = 0x95873fd0 w[31] = 0x181c4fa7
w[32] = 0xc0b45268 w[33] = 0x168a63c2 w[34] = 0x830d5c12 w[35] = 0x9b1113b5
w[36] = 0x59c9877c w[37] = 0x4f43e4be w[38] = 0xcc4eb8ac w[39] = 0x575fab19
w[40] = 0xa0ab5327 w[41] = 0xefe8b799 w[42] = 0x23a60f35 w[43] = 0x74f9a42c

进行AES加密..................
加密完后的密文的ASCCI为:
0x8d 0x31 0x45 0xed 0x38 0xab 0xdf 0x82 0x79 0xd7 0x74 0x1f 0x2 0x32 0x89 0xaa
请输入你想要写进的文件名，比如'test.txt':
test3.txt
已经将密文写进test3.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
test3.txt
开始解密.........
解密后的明文ASCII为:
0x6c 0x69 0x7a 0x69 0x74 0x61 0x6f 0x32 0x32 0x30 0x31 0x31 0x30 0x36 0x30 0x38
明文为: lizitao220110608
现在可以打开test3.txt来查看解密后的密文了!
Press any key to continue . . .
```

密钥为：cryptographylab1

二、 实验过程中遇到的问题有哪些？你是怎么解决的。

1. *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*
2. *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*

三、 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：

```
==============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
itisaesclass1234itisaesclass1234
你输入的明文为: itisaesclass1234itisaesclass1234
轮密钥.................
w[0] = 0x73656375 w[1] = 0x72697479 w[2] = 0x73656375 w[3] = 0x72697479
w[4] = 0x8bf7d535 w[5] = 0xf99ea14c w[6] = 0x8afbc239 w[7] = 0xf892b640
w[8] = 0xc6b9dc74 w[9] = 0x3f277d38 w[10] = 0xb5dcbf01 w[11] = 0x4d4e0941
w[12] = 0xedb85f97 w[13] = 0xd29f22af w[14] = 0x67439dae w[15] = 0x2a0d94ef
w[16] = 0x329a8072 w[17] = 0xe005a2dd w[18] = 0x87463f73 w[19] = 0xad4bab9c
w[20] = 0x91f85ee7 w[21] = 0x71fdfc3a w[22] = 0xf6bbc349 w[23] = 0x5bf068d5
w[24] = 0x3dbd5dde w[25] = 0x4c40a1e4 w[26] = 0xbafb62ad w[27] = 0xe10b0a78
w[28] = 0x56dae126 w[29] = 0x1a9a40c2 w[30] = 0xa061226f w[31] = 0x416a2817
w[32] = 0xd4ee11a5 w[33] = 0xce745167 w[34] = 0x6e157308 w[35] = 0x2f7f5b1f
w[36] = 0x1dd7d1b0 w[37] = 0xd3a380d7 w[38] = 0xbdb6f3df w[39] = 0x92c9a8c0
w[40] = 0xf6156bff w[41] = 0x25b6eb28 w[42] = 0x980018f7 w[43] = 0xac9b037

进行AES加密.................
加密完后的密文的ASCCI为:
0x10 0x14 0x73 0x2d 0xf0 0x78 0x54 0xfc 0x32 0x25 0x6b 0x95 0x64 0x7e 0xf8 0x90 0x21 0x25 0x7b 0xf1 0xf1 0x85 0x5e 0x9e 0xcc 0x94 0xf0 0x3c 0x7e 0x11 0xee 0xe4
请输入你想要写进的文件名，比如'test.txt':
testcbc2.txt
已经将密文写进testcbc2.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
testcbc2.txt
开始解密.........
解密后的明文ASCII为:
0x69 0x74 0x69 0x73 0x61 0x65 0x73 0x63 0x6c 0x61 0x73 0x73 0x31 0x32 0x33 0x34 0x69 0x74 0x69 0x73 0x61 0x65 0x73 0x63 0x6c 0x61 0x73 0x73 0x31 0x32 0x33 0x34
明文为: itisaesclass1234itisaesclass1234
现在可以打开testcbc2.txt来查看解密后的密文了!
Press any key to continue . . .
```

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）