实验一 AES 密码算法

姓名：王木一 学号：200210231

一、 运行截图

TEST-1

明文：thisisatestclass

密钥：securitysecurity

```
==========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':
test-1.txt
已经将密文写进test-1.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-1.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-1.txt来查看解密后的密文了！
Press any key to continue . . .
```

TEST-2

明文：
wangmy+200210231

密钥：
cryptographylab1

```
==========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
wangmy+200210231
你输入的明文为：wangmy+200210231
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：
0x40 0x2e 0xbe 0x55 0x90 0x74 0xe2 0xa3 0xad 0xbd 0x65 0x68 0xf8 0xf0 0x1d 0x39
请输入你想要写进的文件名，比如'test.txt':
test-2.txt
已经将密文写进test-2.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-2.txt
开始解密.........
解密后的明文ASCII为：
0x77 0x61 0x6e 0x67 0x6d 0x79 0x2b 0x32 0x30 0x30 0x32 0x31 0x30 0x32 0x33 0x31
明文为：wangmy+200210231
现在可以打开test-2.txt来查看解密后的密文了！
Press any key to continue . . .
```

TEST-3

明文：
wangmy+200210230

密钥：
cryptographylab1

```
================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
wangmy+200210230
你输入的明文为：wangmy+200210230
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：
0xfb 0x4b 0x5 0x24 0xac 0x1e 0xeb 0xc9 0x19 0xa 0x5 0x63 0x6d 0x4a 0x4f 0x3a
请输入你想要写进的文件名，比如'test.txt':
test-3.txt
已经将密文写进test-3.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-3.txt
开始解密.........
解密后的明文ASCII为：
0x77 0x61 0x6e 0x67 0x6d 0x79 0x2b 0x32 0x30 0x30 0x32 0x31 0x30 0x32 0x33 0x30
明文为：wangmy+200210230
现在可以打开test-3.txt来查看解密后的密文了！
Press any key to continue . . .
```

二、 实验过程中遇到的问题有哪些？你是怎么解决的。

1. 列混淆计算

   计算列混淆时要用到矩阵乘法，需设置 tmp 来存储部分积，即 tmp = tmp ^ GFMul(colM[][], a[][])。算完后将 tmp 值赋给 array[][]。每计算一个 array 矩阵元素的值都要将 tmp 重新置零。之前加密错误就出现在这里。

2. CBC

   实现 CBC 模式时，每次 AES 加密前需要在原有分组明文中加上一个向量，此向量来自 IV 或前一组加密的结果。相反的，解密时 deAES 的结果还要加上上一组的密文（或 IV）才能成为本组明文。由于代码函数参数传入的是指针，解密后的明文直接覆盖之前的密文，就不能直接把它加给下一组的解密结果。故需要使用单独的变量提前复制一份当前组的密文。之前 CBC 解密错误就在这里。

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

在原有代码框架下，实现了 CBC 模式。

1. 将加解密功能分别从 aes()和 deAes()方法中提取出，分别为 void AES(char *p)和 void deAES(char *c)，单独完成加解密任务。
2. 在原有 aes()和 deAes()方法中增加对明文/密文长度判断。若长度为 16，就执行一般加解密操作，不涉及 IV（初始向量）的加入；若长度为大于 16 且为 16 倍数，就执行 CBC 模式。
3. 增加了新的方法来辅助实现 CBC 模式。void addVector(char *p, char *v)用于将向量 v 加到 p 中。void copyVector(char *c, char *out)用于将 c 串复制给 out 串（解决上面的问题 2）

测试结果：

明文：wangmuyi200210231wangmy200210231wangmuyi200210231wangmy200210231
密钥：cryptographylab1

```
================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
wangmuyi200210231wangmy200210231wangmuyi200210231wangmy200210231
你输入的明文为：wangmuyi200210231wangmy200210231wangmuyi200210231wangmy200210231
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：
0x4c 0x17 0x7b 0x96 0xef 0x86 0xb3 0xf6 0x22 0x7e 0x8 0x6c 0xa7 0x8e 0xa4 0xe 0xae 0x95 0x34 0x8d 0xa6 0x7e 0xc4 0x31 0x20 0x38 0x2c 0x67 0x61 0
xf7 0xab 0xd3 0x12 0x1c 0x57 0x1d 0xa4 0x4c 0xbd 0x18 0x3e 0x8 0xb8 0x9e 0x60 0x71 0xb0 0xfe 0x53 0xc7 0x2b 0x90 0xf0 0x0 0xe1 0xeb 0xca 0x14 0x
78 0x7 0xd3 0xde 0x8f 0x9e
请输入你想要写进的文件名，比如'test.txt'：
test-4.txt
已经将密文写进test-4.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-4.txt
开始解密.........
解密后的明文ASCII为：
0x77 0x61 0x6e 0x67 0x6d 0x75 0x79 0x69 0x32 0x30 0x30 0x32 0x31 0x30 0x32 0x33 0x31 0x77 0x61 0x6e 0x67 0x6d 0x79 0x32 0x30 0x30 0x32 0x31 0x30
 0x32 0x33 0x31 0x77 0x61 0x6e 0x67 0x6d 0x75 0x79 0x69 0x32 0x30 0x30 0x32 0x31 0x30 0x32 0x33 0x31 0x77 0x61 0x6e 0x67 0x6d 0x79 0x32 0x30 0x3
0 0x32 0x31 0x30 0x32 0x33 0x31
明文为：wangmuyi200210231wangmy200210231wangmuyi200210231wangmy200210231
现在可以打开test-4.txt来查看解密后的密文了！
Press any key to continue . . .
```

注：CBC 初始向量 IV 设置为“abcdefghijklmnop”，具体实现详见 lab1-aes.c