

实验一 AES 密码算法

姓名： 杨行 学号： 2001111325

一、运行截图

第一组：明文为 thisisatestclass,密钥为 securitysecurity

```
E:\lab_1\bin\Debug\lab_1.exe
*****$声明信息$*****
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] = 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] = 0x71fdcf3a w[22] = 0xf6bbbc349 w[23] = 0x5bf068d5
w[24] = 0x3bd5d5de w[25] = 0x4c40a1e4 w[26] = 0xbaf6b62ad w[27] = 0xe10b0a78
w[28] = 0x50dae126 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] = 0xf6156b7f w[41] = 0x25b6eb28 w[42] = 0x980018f7 w[43] = 0xac9b037

进行AES加密.....
加密完后的密文的ASCII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.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. . .
```

第二组：姓名拼音+学号（16 位不够补为 32 位） 密钥为：cryptographylab1

```
E:\lab_1\bin\Debug\lab_1.exe
*****$声明信息$*****
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：
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
yanghang20011325
明文长度必须为16的倍数，现在的长度为17
yanghang20011325yanghang200113
你输入的明文为: yanghang20011325yanghang200113
轮密钥.....
w[0] = 0x63727970 w[1] = 0x746f6772 w[2] = 0x61706879 w[3] = 0x6c616231
w[4] = 0x8a8b8a20 w[5] = 0xf36f4952 w[6] = 0x98c7b12b w[7] = 0xf4a6d31a
w[8] = 0xabba1c9f w[9] = 0x5309e5cd w[10] = 0xace74e6 w[11] = 0x3e68a7fc
w[12] = 0xae2ac2d w[13] = 0xb8ab69e0 w[14] = 0x72251d06 w[15] = 0x4c4dhafa
w[16] = 0x1168104 w[17] = 0xb9fde8e4 w[18] = 0xcdb8f5e2 w[19] = 0x87954f18
w[20] = 0x3b922c13 w[21] = 0x826fc4f7 w[22] = 0x49673115 w[23] = 0xce22e0d
w[24] = 0x3b61f998 w[25] = 0xa0e3f6f w[26] = 0x4b90e7a w[27] = 0x36957077
w[28] = 0x2c300e5 w[29] = 0x63e31aa w[30] = 0xd6877fd0 w[31] = 0x181e1e7f
w[32] = 0xc0b45268 w[33] = 0x18a6a3c2 w[34] = 0x30a5c12 w[35] = 0x9b113b5
w[36] = 0x59e9877c w[37] = 0x4f43e4be w[38] = 0xcc4eb8ac w[39] = 0x575fab19
w[40] = 0xa0ab5327 w[41] = 0xefeb799 w[42] = 0x23a60f35 w[43] = 0x7479a42c

进行AES加密.....
加密完后的密文的ASCII为:
0x2e 0x46 0xdc 0xa5 0x46 0xda 0x16 0x6d 0x3f 0x9a 0x9a 0xf4 0x35 0xa 0xb6 0x30 0x79 0x6 0xe6 0xd7 0x37 0x68 0x2a 0x7a 0xbb 0xf4 0xaf 0xc0 0x81 0xbb 0xc7 0xaf
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:
0x79 0x61 0x6e 0x67 0x68 0x61 0x6e 0x67 0x32 0x30 0x30 0x31 0x31 0x31 0x33 0x32 0x35 0x79 0x61 0x6e 0x67 0x68 0x61 0x6e 0x67 0x32 0x30 0x30 0x31 0x31 0x31 0x33
明文为: yanghang20011325yanghang200113
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. . .
```

第三组: 姓名拼音+(学号-1)(16位不够补为32位) 密钥为:cryptographylab1

```
EXLab, F:\bin\Debug\lab_1.exe
*****$声明信息$*****
版权所有: 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:
cryptographylab1
你输入的密钥为: cryptographylab1
请输入你的明文, 明文长度必须为16的倍数
yanghang200111324yanghang2001113
你输入的明文为: yanghang200111324yanghang2001113
轮密钥:
w[0] = 0x63727970 w[1] = 0x746f6772 w[2] = 0x61706879 w[3] = 0x6c616231
w[4] = 0x5d4d8be20 w[5] = 0xf97d952 w[6] = 0x98c7b12b w[7] = 0xf4a6d31a
w[8] = 0xab0e1d93d w[9] = 0x2093d3d w[10] = 0xcac74e6 w[11] = 0x3e08a7fc
w[12] = 0xae2ac2d w[13] = 0xb8eb69e0 w[14] = 0x72251d06 w[15] = 0x4c4dbafa
w[16] = 0x1168104 w[17] = 0xb9fde8e4 w[18] = 0xcb8f5e2 w[19] = 0x87954f18
w[20] = 0x3b922c13 w[21] = 0x826fc4f7 w[22] = 0x49b73115 w[23] = 0xce227e0d
w[24] = 0x8861fb98 w[25] = 0xa0c3f5f w[26] = 0x4b9067a w[27] = 0x9d9b7077
w[28] = 0xcd300ec8 w[29] = 0xa6381aa w[30] = 0x98373fd0 w[31] = 0x181c4e47
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] = 0xa0b53327 w[41] = 0xefe8b799 w[42] = 0x23a60f35 w[43] = 0x74f9a42c

进行AES加密.....
加密完后的密文的ASCCI为:
0x2e 0x46 0xdc 0xa5 0x46 0xda 0x16 0x6d 0x3f 0xbd 0x9a 0xfd 0x35 0xa 0x6b 0x30 0x59 0x13 0xbe 0xea 0x3c 0x7e 0x81 0x7e 0xab 0x7e 0x87 0x9f 0x5a 0x43 0x82 0x63
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ASCCI为:
0x79 0x61 0x6e 0x67 0x68 0x61 0x6e 0x67 0x32 0x30 0x30 0x30 0x31 0x31 0x31 0x33 0x32 0x34 0x79 0x61 0x6e 0x67 0x68 0x61 0x6e 0x67 0x32 0x30 0x30 0x31 0x31 0x31 0x33
明文为: yanghang200111324yanghang2001113
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. . .
```

二、实验过程中遇到的问题有哪些？你是怎么解决的。

答：实验过程主要遇到的问题大多在于对理论的不熟悉导致根据模板代码补全时存在一定问题，通过回顾知识点得以解决。实验中遇到的一个有意思的问题是原有的 readStrFromFile 函数读取文件中有一句读的结束判断如下：

```
for(i = 0; i < MAXLEN && (str[i] = getc(fp)) != EOF ; i++);
```

由于 str 定义为 char，因为文本文件中存储的是 ASCII 码，而 ASCII 码中 FF 代表空值（blank），也就是说，在语句“(str[i]=getc(fp))!=EOF”中，当读取的字符为 0xFF（空格）时，“getc(fp)”的值由 0x000000FF 转换为 char 类型（0xFF）；而在执行语句“str[i] != EOF”时，字符与整数比较，str[i]被转换为 0xFFFFFFFF，条件成立，遇到空格字符时就退出。导致密文中存在空格则无法解密。如下图：

```
进行AES加密.....
加密完后的密文的ASCCI为:
0x15 0x83 0xff 0xc5 0x3e 0xaf 0xa2 0xd7 0x33 0xb6 0x89 0x96 0xe5 0x64 0x77 0xcc
请输入你想要写进的文件名, 比如' test.txt ':
23
已经将密文写进23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
23
开始解密.....
密文长度必须为16的倍数! 现在的长度为2
Process returned 0 (0x0)   execution time : 31.816 s
Press any key to continue.
```

密文第三位出现 0xFF,无法解密

```
for(i = 0; i < MAXLEN ; i++){
    str[i] = getc(fp);
    if (feof(fp)) {
        break;
    }

    // printf("%c", str[i]);
};

rewind(fp);
```

改为用 feof 判断文本结尾可以有效解决密文中间出现 0xff 现象。

但如果密文结尾出现 0xff 现象，则依旧无法判断，这种情况想到的解决办法是在文本追加末尾字符保存明文长度，依此保证读入字符个数正确，或读取时自动判断是否为 16 的倍数，但两者都存在对错误文件解密的可能，故不为采用。

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