

实验一 AES 密码算法

姓名：____宗晴____ 学号：____ 200110513____

一、运行截图

(1) 明文为 *thisisatestclass*, 密钥为 *securitysecurity*

```
*****$声明信息$*****
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] = 0x71dfc3a w[22] = 0xf6bbc349 w[23] = 0x5bf068d5
w[24] = 0x3bd5dde 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. . .
```

（2）明文为 zongqing200110513zongqing2001105, 密钥为 cryptography1

```
*****$声明信息$*****
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：
cryptography1
你输入的密钥为： cryptography1
请输入你的明文，明文长度必须为16的倍数
zongqing200110513zongqing2001105
你输入的明文为： zongqing200110513zongqing2001105
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] = 0xae2ac2d 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] = 0xfe8b799 w[42] = 0x23a60f35 w[43] = 0x74f9a42c

进行AES加密.....
加密完后的密文的ASCII为：
0xc7 0x81 0xa7 0x41 0xf1 0x4c 0x5f 0xee 0xe1 0x61 0x7a 0x65 0x78 0x37 0x73 0xfd 0x5 0x22 0x66 0x45 0xd2 0x84 0xd 0xb8 0x
4e 0x14 0xb8 0xf1 0xfb 0xba 0xf9 0x43
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：
0x7a 0x6f 0x6e 0x67 0x71 0x69 0x6e 0x67 0x32 0x30 0x30 0x31 0x31 0x30 0x35 0x31 0x33 0x7a 0x6f 0x6e 0x67 0x71 0x69 0x6e
0x67 0x32 0x30 0x30 0x31 0x31 0x30 0x35
明文为： zongqing200110513zongqing2001105
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. . .
```

（3）明文为 zongqing200110512zongqing2001105, 密钥为 cryptography1

```
*****$声明信息$*****
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：
cryptography1
你输入的密钥为： cryptography1
请输入你的明文，明文长度必须为16的倍数
zongqing200110512zongqing2001105
你输入的明文为： zongqing200110512zongqing2001105
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] = 0xae2ac2d 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] = 0xfe8b799 w[42] = 0x23a60f35 w[43] = 0x74f9a42c

进行AES加密.....
加密完后的密文的ASCII为：
0xc7 0x81 0xa7 0x41 0xf1 0x4c 0x5f 0xee 0xe1 0x61 0x7a 0x65 0x78 0x37 0x73 0xfd 0xe7 0x28 0x58 0xb3 0xde 0xd3 0x7 0x8f 0
xa4 0x63 0x76 0x23 0x10 0x86 0x70 0x79
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：
0x7a 0x6f 0x6e 0x67 0x71 0x69 0x6e 0x67 0x32 0x30 0x30 0x31 0x31 0x30 0x35 0x31 0x32 0x7a 0x6f 0x6e 0x67 0x71 0x69 0x6e
0x67 0x32 0x30 0x30 0x31 0x31 0x30 0x35
明文为： zongqing200110512zongqing2001105
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。

起初，我的代码输出的 44 轮的密钥就不太正确。为此我使用了单步调试，同时仔细对比指导书，最终发现，明文矩阵和子密钥矩阵都是纵向排列的，而我在代码实现时却没有注意到这一点。在纠正这一错误后，我的前四轮密钥输出正确了，然后后 40 轮密钥却依然不对。我再次通过单步调试，并仔细对比了指导书，发现在密钥扩展的字节代换中，是需要对每个字节分别进行代换，而我错写成了对整个该轮密钥进行代换。在纠正这一错误后，44 轮密钥完全正确，同时加密后的密文和解密后的明文也都正确了。

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

用了 lab1-aes.c 代码框架。并未实现 CBC 模式。