

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: *suting20188197su*

明文 2: 姓名拼音+ (学号-1), 不足 16 个字符, 重复补齐, 例如: *suting20188196su*

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] = 0xad15f5a 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.

```
*****$声明信息$*****
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
fangxuanzi210010101fangxuanzi210
你输入的明文为：fangxuanzi210010101fangxuanzi210
轮密钥.....
w[0] = 0x63727970 w[1] = 0x746f6772 w[2] = 0x61706879 w[3] = 0x6c616231
w[4] = 0x8ed8be20 w[5] = 0xfab7d952 w[6] = 0x9bc7b12b w[7] = 0xf7a6d31a
w[8] = 0xaebe1c48 w[9] = 0x5409c51a w[10] = 0xcfc7431 w[11] = 0x3868a72b
w[12] = 0xe3e2ed4f w[13] = 0xb7eb2855 w[14] = 0x78255c64 w[15] = 0x404dfb4f
w[16] = 0x10ed6946 w[17] = 0xa7064113 w[18] = 0xdf231d77 w[19] = 0x9f6ee638
w[20] = 0xaf636e9d w[21] = 0x8652f8e w[22] = 0xd74632f9 w[23] = 0x4828d4c1
w[24] = 0xdb2b16cf w[25] = 0xd34c3941 w[26] = 0x4080bb8 w[27] = 0x4c20df79
w[28] = 0xecb5a0e6 w[29] = 0x3fb99a7 w[30] = 0x3bf3921f w[31] = 0x77d34d66
w[32] = 0x91569313 w[33] = 0xaea0ab4 w[34] = 0x955e98ab w[35] = 0xe28dd5cd
w[36] = 0xfa552e8b w[37] = 0x54f8243f w[38] = 0x1a6bc94 w[39] = 0x232b6959
w[40] = 0xbace5ad w[41] = 0x5f54c192 w[42] = 0x9ef27d06 w[43] = 0xbdd9145f

进行AES加密.....
加密完后的密文的ASCII为：
0x6f 0x1 0x95 0xb9 0xdf 0xce 0x64 0xfa 0xd5 0xc7 0x68 0xb2 0x42 0xda 0xc9 0x69 0x82 0x92 0xd3 0x30 0x6f 0xc3 0xf1 0x6d 0x9f 0x45 0xd9 0xfe 0x31 0x88 0x0 0x3d

请输入你想要写进的文件名，比如'test.txt':
work1.txt
已经将密文写进work1.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
work1.txt
开始解密.....
解密后的明文ASCII为：
0x66 0x61 0x6e 0x67 0x78 0x75 0x61 0x6e 0x7a 0x69 0x32 0x31 0x30 0x30 0x31 0x30 0x31 0x30 0x31 0x66 0x61 0x6e 0x67 0x78 0x75 0x61 0x6e 0x7a 0x69 0x32 0x31 0x
30
明文为： fangxuanzi210010101fangxuanzi210
现在可以打开work1.txt来查看解密后的密文了！
请按任意键继续. . .
```

3.

```
*****$声明信息$*****
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
fangxuanzi210010100fangxuanzi210
你输入的明文为：fangxuanzi210010100fangxuanzi210
轮密钥.....
w[0] = 0x63727970 w[1] = 0x746f6772 w[2] = 0x61706879 w[3] = 0x6c616231
w[4] = 0x8ed8be20 w[5] = 0xfab7d952 w[6] = 0x9bc7b12b w[7] = 0xf7a6d31a
w[8] = 0xaebe1c48 w[9] = 0x5409c51a w[10] = 0xcfc7431 w[11] = 0x3868a72b
w[12] = 0xe3e2ed4f w[13] = 0xb7eb2855 w[14] = 0x78255c64 w[15] = 0x404dfb4f
w[16] = 0x10ed6946 w[17] = 0xa7064113 w[18] = 0xdf231d77 w[19] = 0x9f6ee638
w[20] = 0xaf636e9d w[21] = 0x8652f8e w[22] = 0xd74632f9 w[23] = 0x4828d4c1
w[24] = 0xdb2b16cf w[25] = 0xd34c3941 w[26] = 0x4080bb8 w[27] = 0x4c20df79
w[28] = 0xecb5a0e6 w[29] = 0x3fb99a7 w[30] = 0x3bf3921f w[31] = 0x77d34d66
w[32] = 0x91569313 w[33] = 0xaea0ab4 w[34] = 0x955e98ab w[35] = 0xe28dd5cd
w[36] = 0xfa552e8b w[37] = 0x54f8243f w[38] = 0x1a6bc94 w[39] = 0x232b6959
w[40] = 0xbace5ad w[41] = 0x5f54c192 w[42] = 0x9ef27d06 w[43] = 0xbdd9145f

进行AES加密.....
加密完后的密文的ASCII为：
0x6f 0x1 0x95 0xb9 0xdf 0xce 0x64 0xfa 0xd5 0xc7 0x68 0xb2 0x42 0xda 0xc9 0x69 0x3c 0xe 0xa5 0x2d 0x8f 0xf0 0xe9 0xd1 0x7e 0x1e 0x20 0x7f 0x3a 0x39 0xd9 0xd2

请输入你想要写进的文件名，比如'test.txt':
work2.txt
已经将密文写进work2.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
work2.txt
开始解密.....
解密后的明文ASCII为：
0x66 0x61 0x6e 0x67 0x78 0x75 0x61 0x6e 0x7a 0x69 0x32 0x31 0x30 0x30 0x31 0x30 0x31 0x30 0x30 0x66 0x61 0x6e 0x67 0x78 0x75 0x61 0x6e 0x7a 0x69 0x32 0x31 0x
30
明文为： fangxuanzi210010100fangxuanzi210
现在可以打开work2.txt来查看解密后的密文了！
请按任意键继续. . .
```

二、 如果是不用模板或者实现了 CBC 模式，请说明。