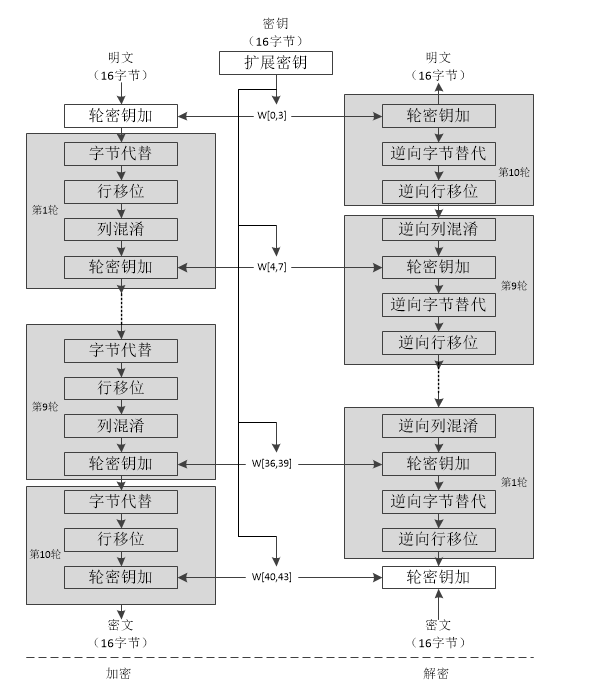
AES算法说明文档

蒋东旭 1120172100

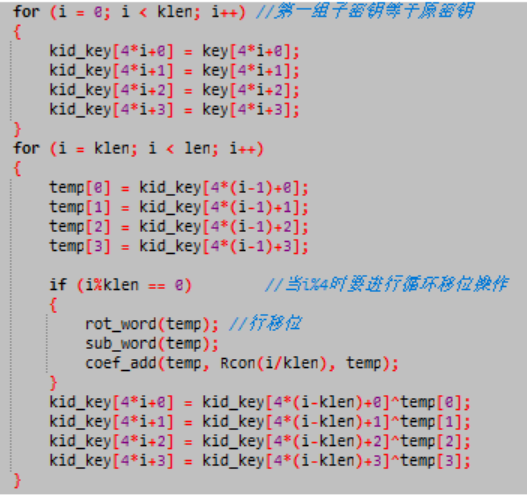
程序流程图：

AES是一个对称加密算法，所以算法加密过程和解密过程所用的密钥k为同一值，一下为AES算法的流程图：

AES具体流程如下所示



图片来源于资料部分的博客

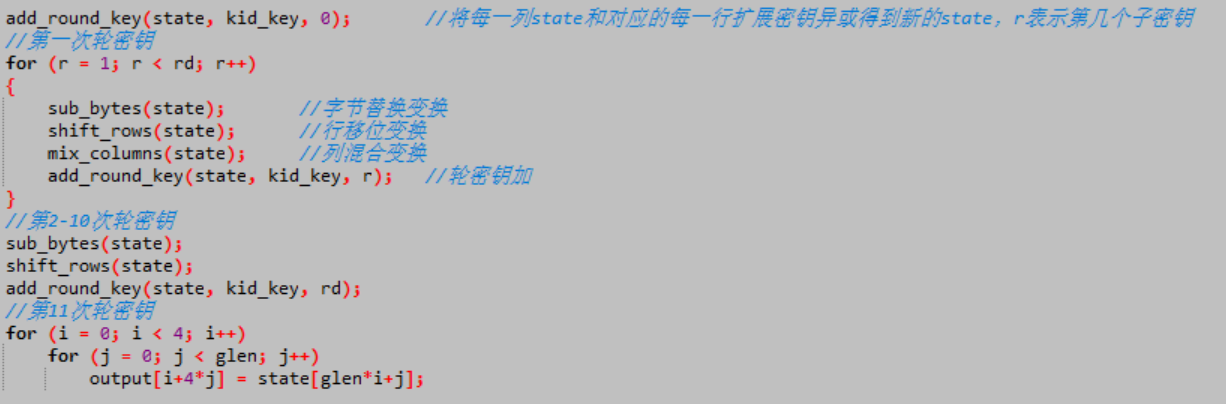
子密钥的扩展算法：  


将128位密钥扩展为11个128位的子密钥得到子密钥后开始加密算法：

加密步骤是以下四个方法的循环：

1. 字节代替变换
2. 行移位变换
3. 列混合变换
4. 轮密钥加

具体代码部分如下所示



关于解密算法：

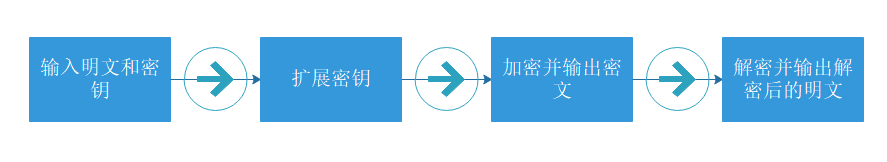
步骤为上述算法的逆运算

1. 逆向行移位
2. 逆向字节代替
3. 轮密钥加（其逆向变换为本身）
4. 逆向混合变换

代码同上述部分相似

程序流程图

大致流程如下：



加解密具体流程见第一张图

测试用例和测试结果：

1. 固定用例

密钥：

unsigned char key[] =

{

0x00, 0x01, 0x02, 0x03,

0x04, 0x05, 0x06, 0x07,

0x08, 0x09, 0x0a, 0x0b,

0x0c, 0x0d, 0x0e, 0x0f

};

明文：

unsigned char input[] =

{

0x00, 0x01, 0x02, 0x03,

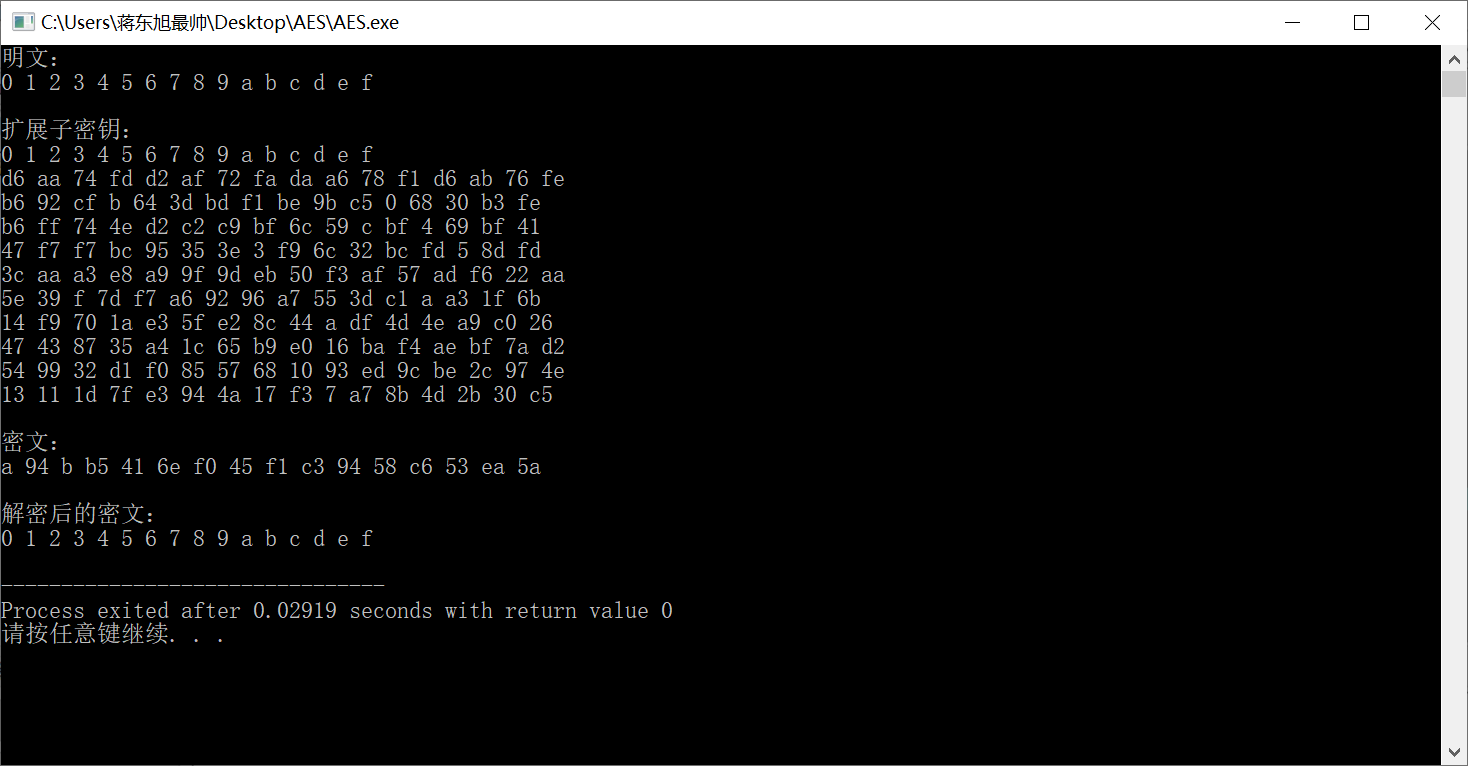
0x04, 0x05, 0x06, 0x07,

0x08, 0x09, 0x0a, 0x0b,

0x0c, 0x0d, 0x0e, 0x0f

};

结果



1. 输入用例

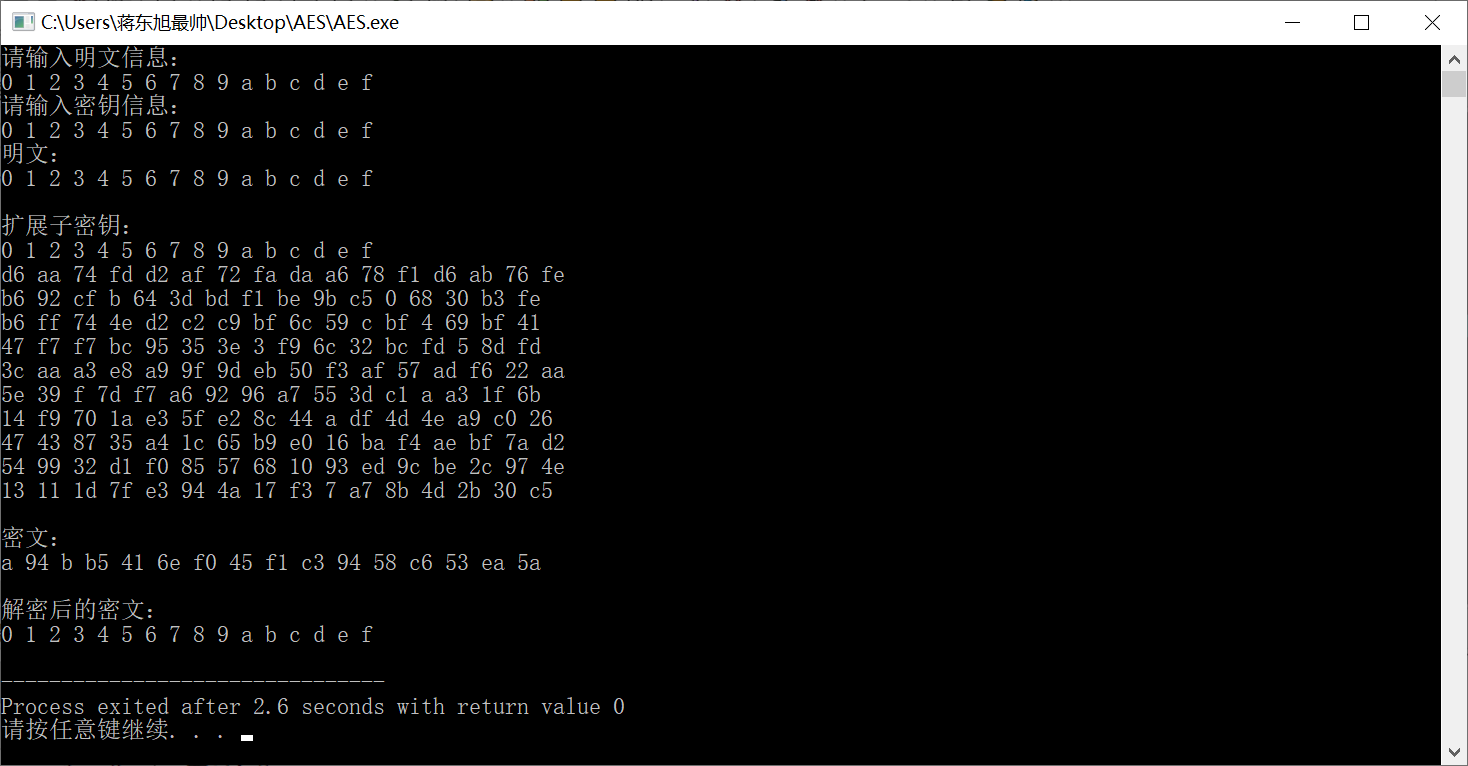
1.

用以上用例进行一次实验

明文： 0 1 2 3 4 5 6 7 8 9 a b c d e f

密钥： 0 1 2 3 4 5 6 7 8 9 a b c d e f

结果：

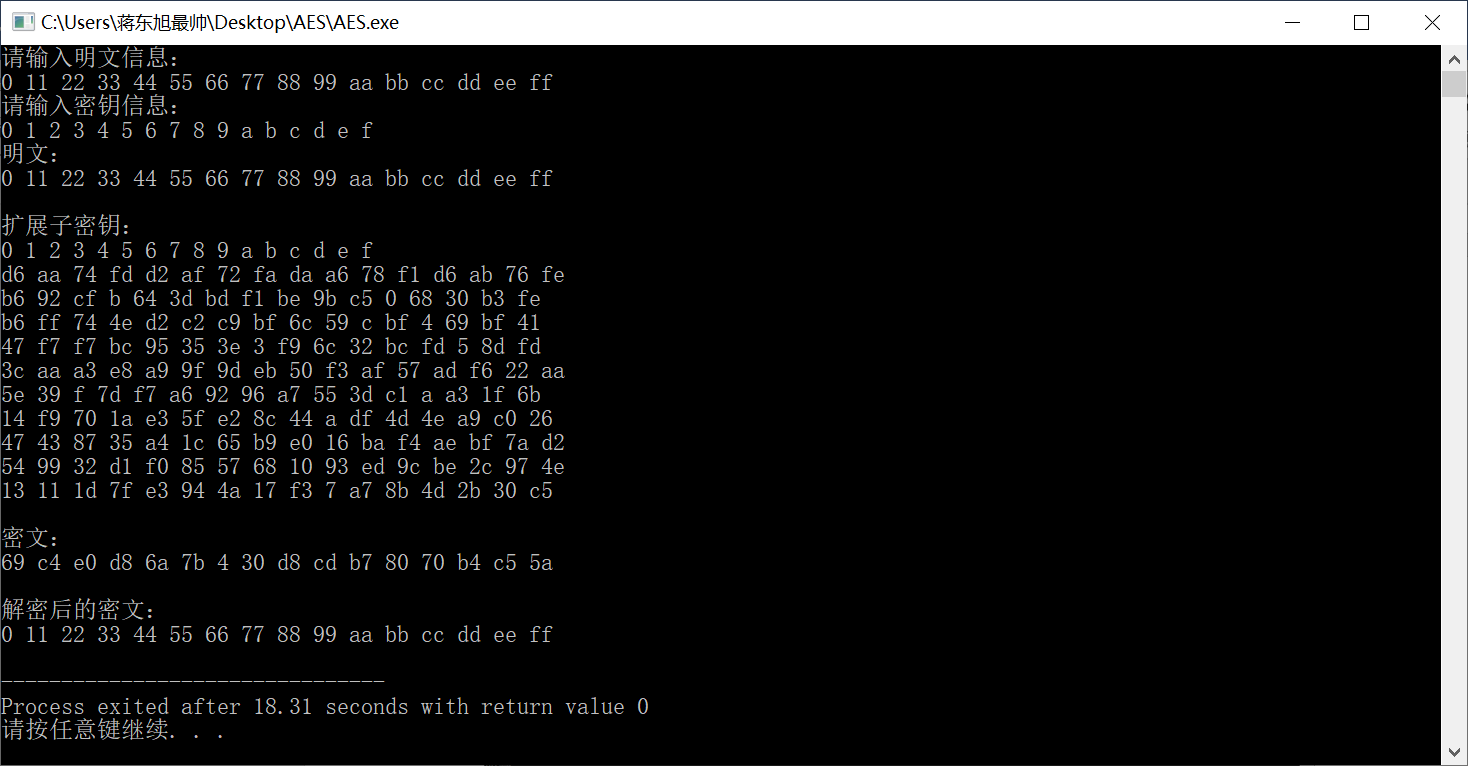


2.

明文： 0 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff

密钥： 0 1 2 3 4 5 6 7 8 9 a b c d e f

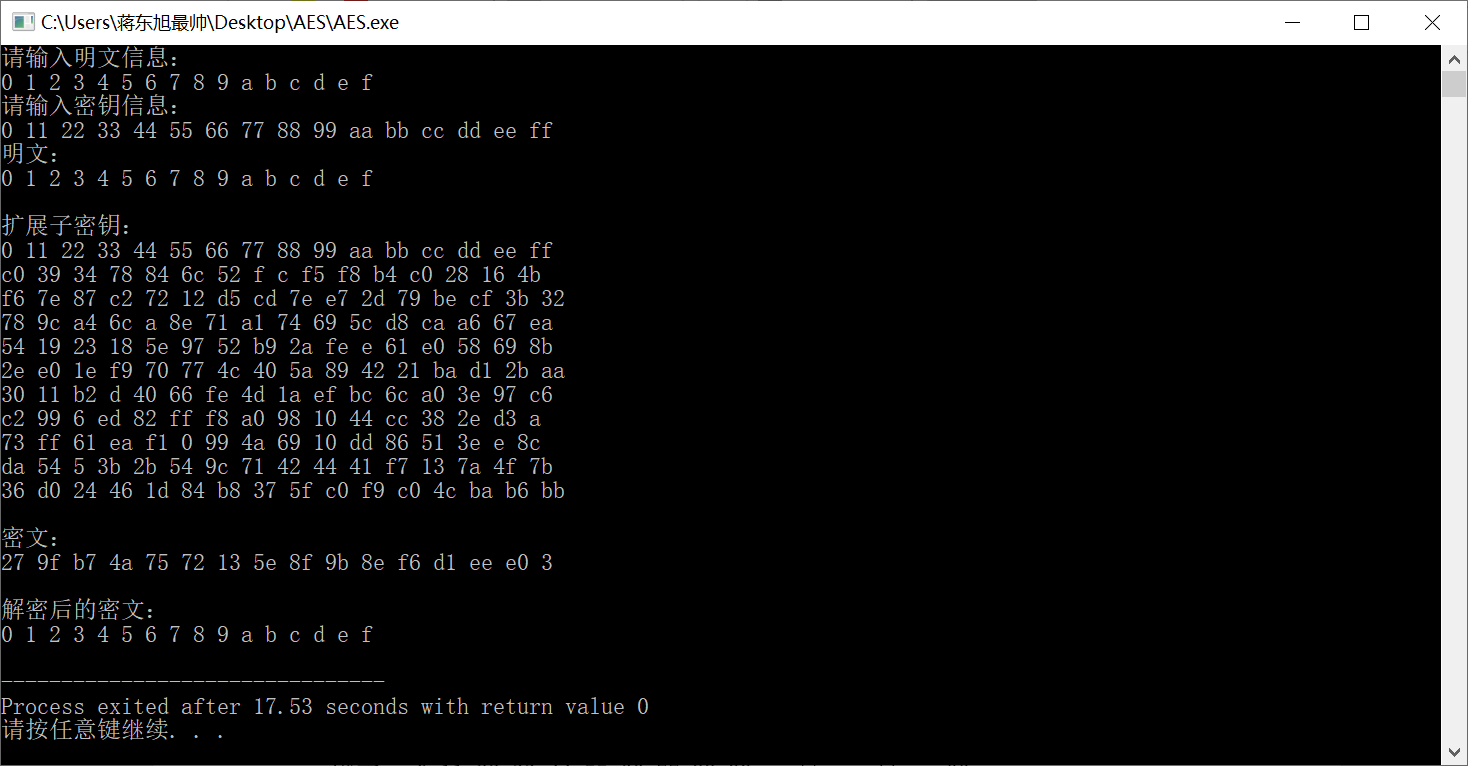
结果：



3

明文： 0 1 2 3 4 5 6 7 8 9 a b c d e f

密钥： 0 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff

结果：

参考资料：

AES博客

<https://blog.csdn.net/gulang03/article/details/81175854>

<https://www.cnblogs.com/luop/p/4334160.html>

参考了源代码

https://github.com/dhuertas/AES