**实验三 分组密码算法AES**

1. **实验目的**

通过用AES算法对实际的数据进行加密和解密来深刻了解AES的运行原理。

1. **实验环境**

运行Windows操作系统的PC机，具有VC等语言编译环境



图1 AES加密/解密流程

1. **实验原理**

AES算法本质上是一种对称分组密码体制，采用代替/置换网络，每轮由三

层组成：线性混合层确保多轮之上的高度扩散，非线性层由16个S盒并置起到混淆的作用，密钥加密层将子密钥异或到中间状态。Rijndael是一个迭代分组密码，其**分组长度和密钥长度都是可变的**，只是**为了满足AES的要求才限定处理的分组大小为128位**，而**密钥长度为128位、192位或256位**，相应的迭代轮数N，为10轮、12轮、14轮。AES汇聚了安全性能、效率、可实现性、灵活性等优点。最大的优点是可以给出算法的最佳差分特征的概率，并分析算法抵抗差分密码分析及线性密码分析的能力。其实现的加密流程图如图-1所示。

加密的主要过程包括：对明文状态的一次密钥加，轮轮加密和末尾轮轮加密，最后得到密文。其中轮轮加密每一轮有四个部件，包括字节代换部件ByteSub、行移位变换ShiftRow、列混合变换NixColumn和一个密钥加AddRoundKey部件，末尾轮加密和前面轮加密类似，只是少了一个列混合变换NixColumn部件。下面具体介绍这几个部件的实现方法：

1. 字节代换ByteSub部件

字节代换是非线形变换，独立地对状态的每个字节进行。代换表（即S-盒）是可逆的，由以下两个变换的合成得到：

1. 首先，将字节看作GF(28)上的元素，映射到自己的乘法逆元，‘00’映射到自己。

（2）其次，对字节做如下的（GF(2)上的，可逆的）仿射变换：



该部件的逆运算部件就是先对自己做一个逆仿射变换，然后映射到自己的乘法逆元上。

1. 行移位变换ShiftRow

行移位是将状态阵列的各行进行循环移位，不同状态行的位移量不同。第0

行不移动，第1行循环左移C1个字节，第2行循环左移C2个字节，第3行循环左移C3个字节。位移量C1、C2、C3的取值与Nb有关，由教材中表3.10给出。

ShiftRow的逆变换是对状态阵列的后3列分别以位移量Nb-C1、Nb-C2、Nb-C3进行循环移位，使得第i行第j列的字节移位到(j+Nb-Ci) mod Nb。

1. 列混合变换NixColumn

在列混合变换中，将状态阵列的每个列视为系数为GF(28)上的多项式，再与

一个固定的多项式c(x)进行模x4+1乘法。当然要求c(x)是模x4+1可逆的多项式，否则列混合变换就是不可逆的，因而会使不同的输入分组对应的输出分组可能相同。Rijndael的设计者给出的c(x)为（系数用十六进制数表示）：

c(x)=‘03’x3+‘01’x2+‘01’x+‘02’

c(x)是与x4+1互素的，因此是模x4+1可逆的。列混合运算也可写为矩阵

乘法。设b(x)= c(x)a(x)，则



这个运算需要做GF(28)上的乘法，但由于所乘的因子是3个固定的元素02、03、01，所以这些乘法运算仍然是比较简单的。

列混合运算的逆运算是类似的，即每列都用一个特定的多项式d(x)相乘。d(x)满足

(03x3+01x2+01x+02)d(x)=‘01’

由此可得

d(x)=‘0B’x3+‘0D’x2+‘09’x+‘0E’

4、密钥加AddRoundKey部件

密钥加是将轮密钥简单地与状态进行逐比特异或。轮密钥由种子密钥通过密钥编排算法得到，轮密钥长度等于分组长度Nb。密钥加运算的逆运算是其自身。

5、密钥编排

密钥编排指从种子密钥得到轮密钥的过程，它由密钥扩展和轮密钥选取两部分组成。其基本原则如下：

1. 轮密钥的字数（4比特32位的数）等于分组长度乘以轮数加1；
2. 种子密钥被扩展成为扩展密钥；

（3） 轮密钥从扩展密钥中取，其中第1轮轮密钥取扩展密钥的前Nb个字，第2轮轮密钥取接下来的Nb个字，如此下去。

密钥扩展的方法和密钥的取法具体请参考教材和ppt。

6、解密过程

AES算法的解密过程和加密过程是相似的，也是先经过一个密钥加，然后进行轮轮解密和末尾轮轮解密，最后得到明文。和加密不同的是轮轮解密每一轮四个部件都需要用到它们的逆运算部件，包括字节代换部件的逆运算、行移位变换的逆变换、逆列混合变换和一个密钥加部件，末尾轮加密和前面轮加密类似，只是少了一个逆列混合变换部件。

在解密的时候，还要注意轮密钥和加密密钥的区别，设加密算法的初始密钥加、第1轮、第2轮、…、第Nr轮的子密钥依次为

k(0), k(1), k(2), …, k(Nr-1), k(Nr)

则解密算法的初始密钥加、第1轮、第2轮、…、第Nr轮的子密钥依次为

k(Nr), InvMixColumn (k(Nr-1)), InvMixColumn (k(Nr-2)), …,

InvMixColumn (k(1)), k(0)。

1. **实验环境**

运行Windows操作系统的PC机，具有VC等语言编译环境

1. **实验内容和步骤，**

1．算法分析：

对课本中AES算法进行深入分析，对其中用到的**基本数学算法、字节代**

**换、行移位变换、列混合变换原理**进行详细的分析，并考虑如何进行编程实

现。对**轮函数、密钥生成**等环节要有清晰的了解，并考虑其每一个环节的实现

过程。

1. AES实现程序的总体设计：

在第一步的基础上，对整个AES加密函数的实现进行总体设计，**考虑数据**

**的存储格式，参数的传递格式，程序实现的总体层次等**，画出程序实现的流程图。

1. 在总体设计完成后，开始具体的编码，在编码过程中，注意要尽量使用

高效的编码方式。

1. 利用3中实现的程序，对AES的密文进行雪崩效应检验。即固定密

钥，仅改变明文中的一位，统计密文改变的位数；固定明文，仅改变密钥中的一位，统计密文改变的位数。

1. **实验报告和要求**
   * 1. 实现**AES的加密和解密**，提交程序代码和执行结果。
     2. 在检验**雪崩效应**中，要求至少改变明文和密文中各八位，给出统计结果并计算出平均值。