

# 高级加密标准

- DES与AES的区别：DES的分组左右迭代，存在不可逆操作。AES整个分组迭代，所有操作可逆。

## AES总体流程（非重点）

- 明文分组具有4列字节方阵，每列4个字节，并被复制到状态矩阵数组，

### 2.3 AES总体流程（数据预处理）

AES的处理单位是字节，128位的输入明文分组 $M$ 和输入密钥 $K$ 都被分成16个字节，表示为：

$$M=m_0, m_1, \dots, m_{15}, \quad K=k_0, k_1, \dots, k_{15}$$

按列依次组成明文状态矩阵和密钥状态矩阵，如：

$m_0$	$m_4$	$m_8$	$m_{12}$
$m_1$	$m_5$	$m_9$	$m_{13}$
$m_2$	$m_6$	$m_{10}$	$m_{14}$
$m_3$	$m_7$	$m_{11}$	$m_{15}$

$k_0$	$k_4$	$k_8$	$k_{12}$
$k_1$	$k_5$	$k_9$	$k_{13}$
$k_2$	$k_6$	$k_{10}$	$k_{14}$
$k_3$	$k_7$	$k_{11}$	$k_{15}$

(子密钥扩展)

$w[0]$	$w[1]$	$w[2]$	$w[3]$	...	$w[42]$	$w[43]$
--------	--------	--------	--------	-----	---------	---------

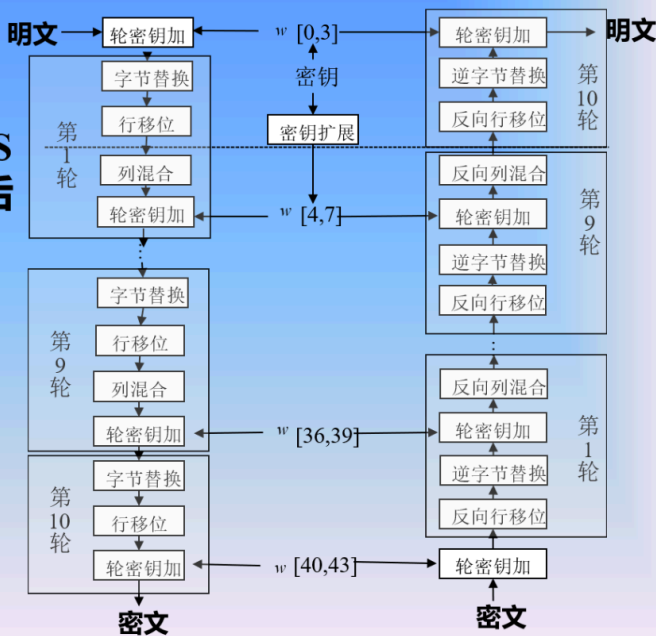
计算机安全导论

9/71

- 然后根据密钥长度进行9/11/13轮运算，包括：

### 2.3 AES总体流程

- 128比特密钥长度的AES执行9轮运算，还有最后不完整的一轮运算。
- 原始密钥扩展为44个字（一个字32比特数据）的子密钥，分别用于每轮运算。



计算机安全导论

10/70

#### 1. 字节替换 (对每个字节使用一个置换)

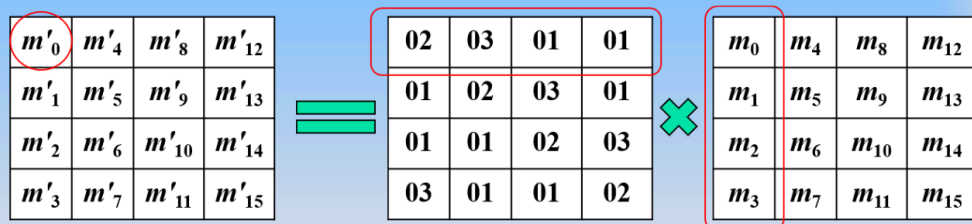
- AES的字节替换就是一个查表替换操作，通过定义一个S盒和一个逆S盒进行明文替换与还原。
- 状态矩阵中每个字节的高4位作为行值，低4位作为列值，对应取出S盒或者逆S盒中对应的元素作为输出

#### 2. 行移位 (对行做简单的移位)



3. 列混合 (对列的每个字节做替换)

列混合是通过矩阵相乘来实现的，经过行移位后的状态矩阵与固定的矩阵相乘，新状态矩阵的每一个列元素都是原状态矩阵的列混合值，然后得到混淆后的状态矩阵，如下：



这里涉及的矩阵元素的乘法和加法都是定义在基于GF(2^8)上的二元运算上

4. 轮密钥加 (将当前分组与一部分扩展密钥简单地按位异或)

轮密钥加是将轮密钥与状态矩阵中的数据进行逐位异或操作。在第*i*轮运算中，使用的扩展子密钥为 $w[4i]$ ,  $w[4i+1]$ ,  $w[4i+2]$ ,  $w[4i+3]$ ，每个子密钥数组包含32位比特。此操作如下：

$$\begin{aligned}
 [m'_0 \ m'_1 \ m'_2 \ m'_3] &= [m_0 \ m_1 \ m_2 \ m_3] \oplus w[4i] \\
 [m'_4 \ m'_5 \ m'_6 \ m'_7] &= [m_4 \ m_5 \ m_6 \ m_7] \oplus w[4i+1] \\
 [m'_8 \ m'_9 \ m'_{10} \ m'_{11}] &= [m_8 \ m_9 \ m_{10} \ m_{11}] \oplus w[4i+2] \\
 [m'_{12} \ m'_{13} \ m'_{14} \ m'_{15}] &= [m_{12} \ m_{13} \ m_{14} \ m_{15}] \oplus w[4i+3]
 \end{aligned}$$

#### ■ 子密钥生成

AES首先将初始密钥输入到一个4\*4的状态矩阵中，然后每列依次保存在 $w[0]$ ,  $w[1]$ ,  $w[2]$ ,  $w[3]$ 中，即：

$$\begin{aligned}
 w[0] &= [k_0 \ k_1 \ k_2 \ k_3] \\
 w[1] &= [k_4 \ k_5 \ k_6 \ k_7] \\
 w[2] &= [k_8 \ k_9 \ k_{10} \ k_{11}] \\
 w[3] &= [k_{12} \ k_{13} \ k_{14} \ k_{15}]
 \end{aligned}$$

之后生成每一轮的子密钥 $w[4i]$ ,  $w[4i+1]$ ,  $w[4i+2]$ ,  $w[4i+3]$ 。

基于 $w[0], w[1], w[2], w[3]$ ，生成每一轮的子密钥 $w[4i], w[4i+1], w[4i+2], w[4i+3]$ ，如下：

$$w[i] = \begin{cases} w[i-4] \oplus T(w[i-1]) & \text{if } i \bmod 4 == 0 \\ w[i-4] \oplus w[i-1] & \text{otherwise} \end{cases}$$

其中T是一个复杂函数，包括三个操作：字循环、字节替换和轮常量异或。

5. 可以看作是交替异或密钥和扰乱消息字)

- 最后一轮不完整，只有三个操作，缺少列混合。
- AES的解密操作

## 2.4 AES轮运算（解密操作）

AES轮运算中的四个操作（字节替换，行移位，列混合和轮密钥加）都是可逆操作。

- 字节替换-查找逆S盒
- 行移位-相应执行右移操作
- 列混合-乘以逆矩阵恢复
- 轮密钥加-简单异或操作

因此，AES的解密正确性可以保证。