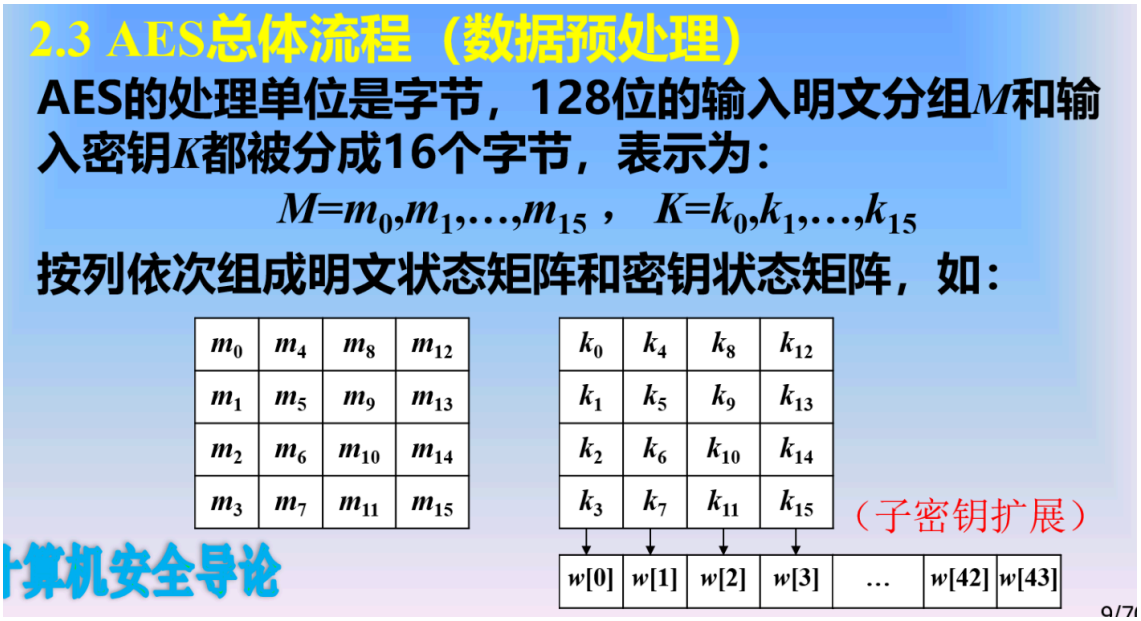
高级加密标准

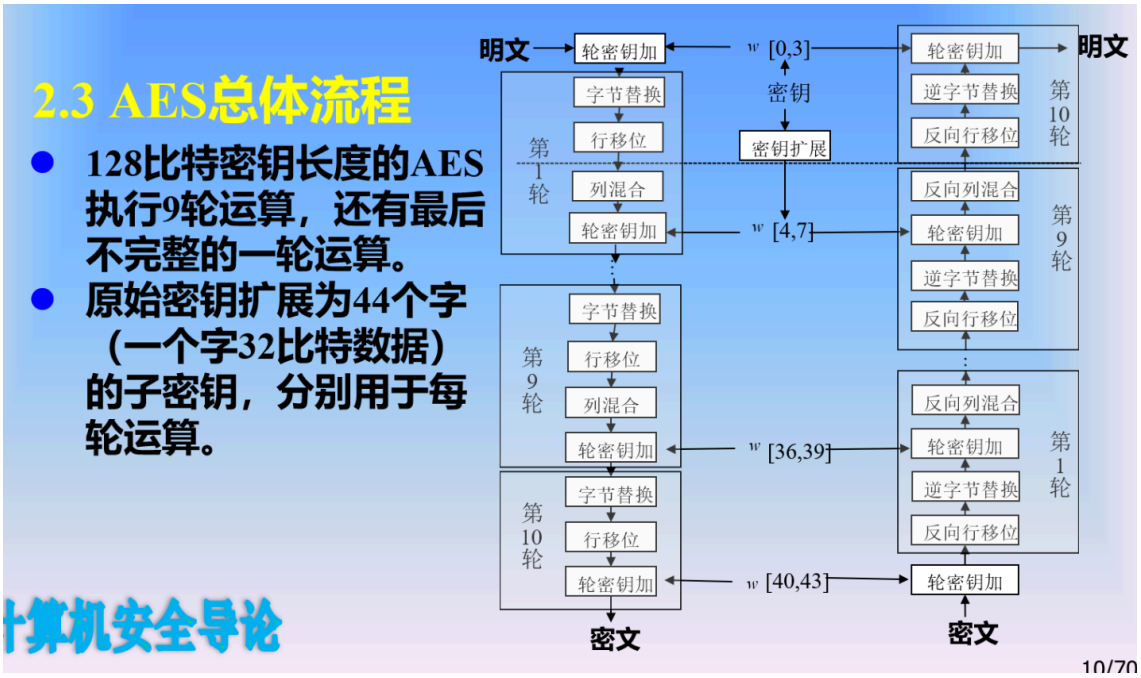
- DES与AES的区别：DES的分组左右迭代，存在不可逆操作。AES整个分组迭代，所有操作可逆。

AES总体流程（非重点）

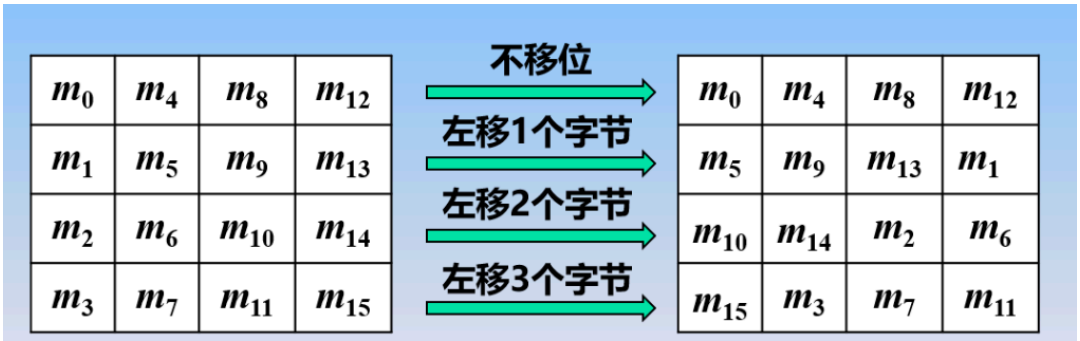
- 明文分组具有4列字节方阵，每列4个字节，并被复制到状态矩阵数组，



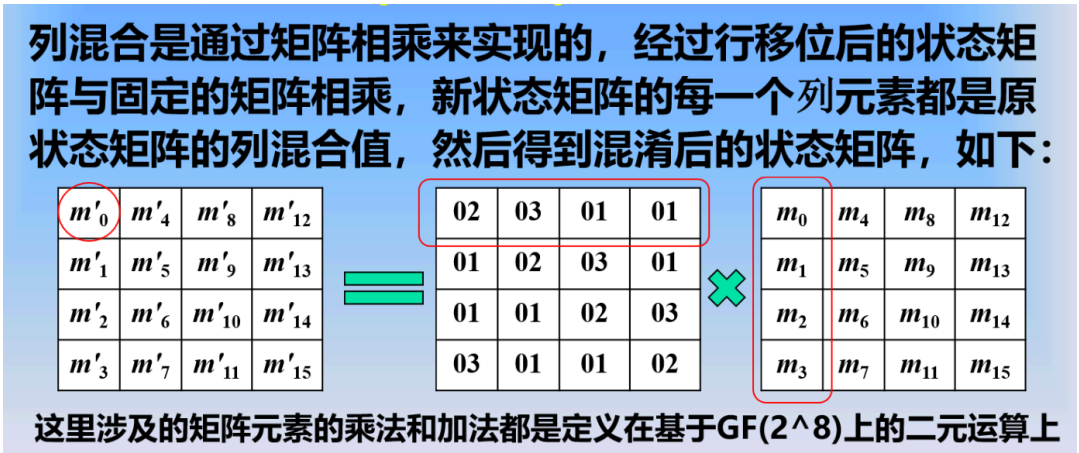
- 然后根据密钥长度进行9/11/13轮运算，包括：



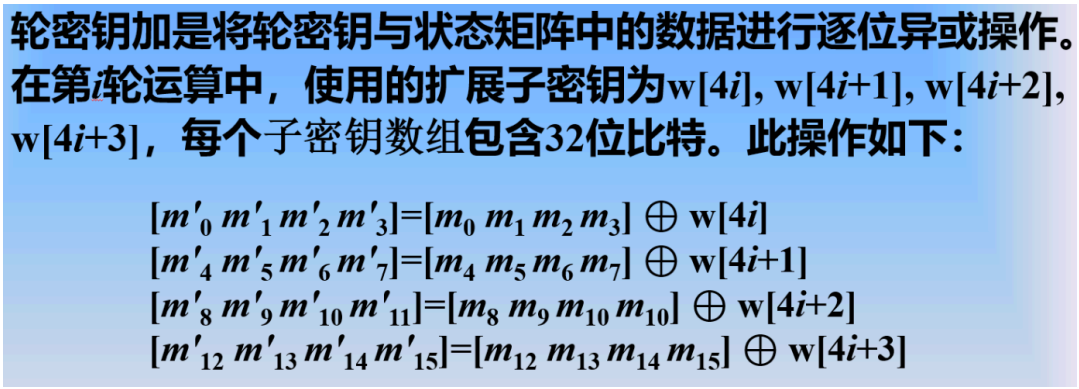
1. 字节替换 (对每个字节使用一个置换)
    - AES的字节替换就是一个查表替换操作，通过定义一个S盒和一个逆S盒进行明文替换与还原。
    - 状态矩阵中每个字节的高4位作为行值，低4位作为列值，对应取出S盒或者逆S盒中对应的元素作为输出
2. 行移位 (对行做简单的移位)



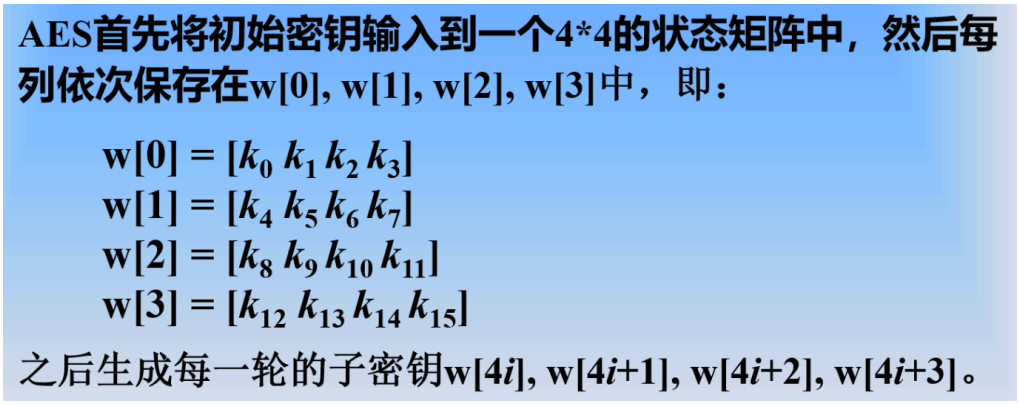
3. 列混合 (对列的每个字节做替换)



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)



- 子密钥生成



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

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

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，列混合和轮钥密加）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。