1 AES 基本原理

AES 的全称是 Advanced Encryption Standard，意思是高级加密标准。它的出现主要是为了取代 DES 加密算法的，因为我们都知道 DES 算法的密钥长度是 56Bit，因此算法的理论安全强度是 2 的 56 次方。但二十世纪中后期正是计算机飞速发展的阶段，元器件制造工艺的进步使得计算机的处理能力越来越强，虽然出现了 3DES 的加密方法，但由于它的加密时间是 DES 算法的 3 倍多，64Bit 的分组大小相对较小，所以还是不能满足人们对安全性的要求。于是 1997 年 1 月 2 号，美国国家标准技术研究所宣布希望征集高级加密标准，用以取代 DES。AES 也得到了全世界很多密码工作者的响应，先后有很多人提交了自己设计的算法。最终有 5 个候选算法进入最后一轮：Rijndael，Serpent，Twofish，RC6 和 MARS。最终经过安全性分析、软硬件性能评估等严格的步骤，Rijndael 算法获胜。

(1)基本运算：四个基本运算单元

- 字节代换 SubBytes
- 行移位 ShiftRows
- 列混合 MixColumns
- 轮密钥加 AddRoundKey

(2)基本流程：有 10/12/14 轮迭代

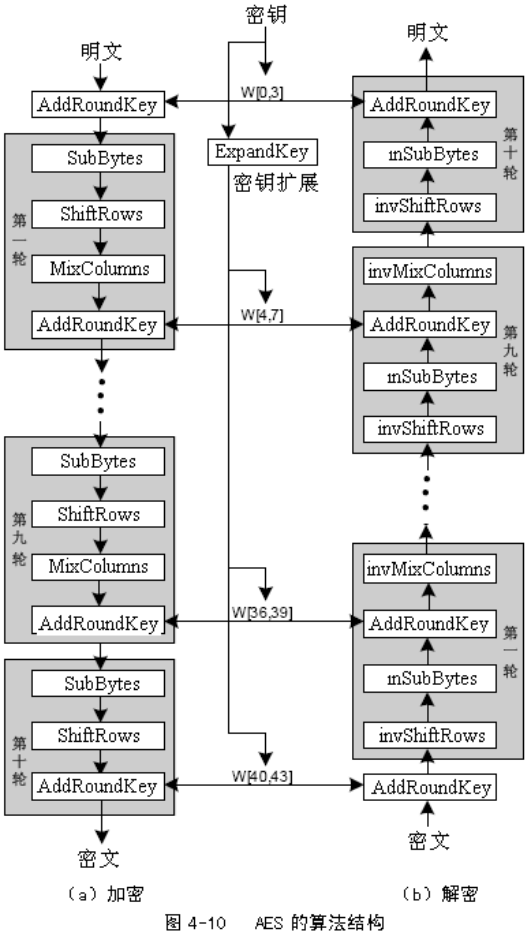

图 4-10　AES 的算法结构

(3)基本特点

- 采用乘积密码迭代，实现扩散与混淆。

- 每一轮都使用代换和混淆技术并行地处理整个数据分组。
- 无论是加密还是解密，除了最后一轮少了列混合运算外，其它各轮都是按照相同顺序依次执行四种基本运算（解密时为四种基本运算的逆运算）。
- 解密算法完全是加密算法的倒推，加、解密原理清晰，便于理解。
- 和其它分组密码相同，轮密钥在解密时颠倒顺序使用。

2 AES 加密推导

若待加密的明文是{000102030405060708090A0B0C0D0E0F}，加密的密钥为{01010101010101010101010101010101}（均为 16 进制表示），并使用 AES 进行加密。

(1)用4×4的矩阵来描述State的最初内容

$$State=\begin{bmatrix}00 & 04 & 08 & 0C\\ 01 & 05 & 09 & 0D\\ 02 & 06 & 0A & 0E\\ 03 & 07 & 0B & 0F\end{bmatrix}$$

$$Key=\begin{bmatrix}01 & 01 & 01 & 01\\ 01 & 01 & 01 & 01\\ 01 & 01 & 01 & 01\\ 01 & 01 & 01 & 01\end{bmatrix}$$

(2)给出初始化轮密钥加密后的值。

$$State\oplus Key=\begin{bmatrix}01 & 05 & 09 & 0D\\ 00 & 04 & 08 & 0C\\ 03 & 07 & 0B & 0F\\ 02 & 06 & 0A & 0E\end{bmatrix}$$

(3)给出字节代换后的值。

$$SubBytes=\begin{bmatrix}7C & 6B & 01 & D7\\ 63 & F2 & 30 & FE\\ 7B & C5 & 2B & 76\\ 77 & 6F & 67 & AB\end{bmatrix}$$

(4)给出行移位后的值。

$$ShiftRows=\begin{bmatrix}7C & 6B & 01 & D7\\ F2 & 30 & FE & 63\\ 2B & 76 & 7B & C5\\ AB & 77 & 6F & 67\end{bmatrix}$$

(5)给出列混和变换后的值。

$$MixColur=\begin{bmatrix}75 & 87 & 0F & B2\\ 55 & E6 & 04 & 22\\ 3E & 2E & B8 & 8C\\ 10 & 15 & 58 & 0A\end{bmatrix}$$

(6)给出第一轮中使用的轮密钥

$$RoundKey=\begin{bmatrix}7C & 7D & 7D & 7D\\ 7D & 7C & 7C & 7C\\ 7C & 7D & 7D & 7D\\ 7D & 7C & 7C & 7C\end{bmatrix}$$