AES and WI-FI protected access

13331233 孙中阳

AES

AES是 `Advanced Encryption Standard` 的英文缩写，可译为“高级加密标准”，于2002年被美国联邦政府所采用，是目前对称密钥加密中最流行的算法之一。相对前任标准DES，AES在软件及硬件上都能快速地加解密，更易于实作，且只需要很少的存储器。

WI-FI

Wi-Fi是一种允许电子设备连接到一个无线局域网（WLAN）的技术，通常使用2.4G UHF或5G SHF ISM 射频频段，目的是改善基于IEEE 802.11标准的无线网路产品之间的互通性。目前绝大多数移动设备都支持WI-FI上网，是当今使用最广的一种无线网络传输技术

目标

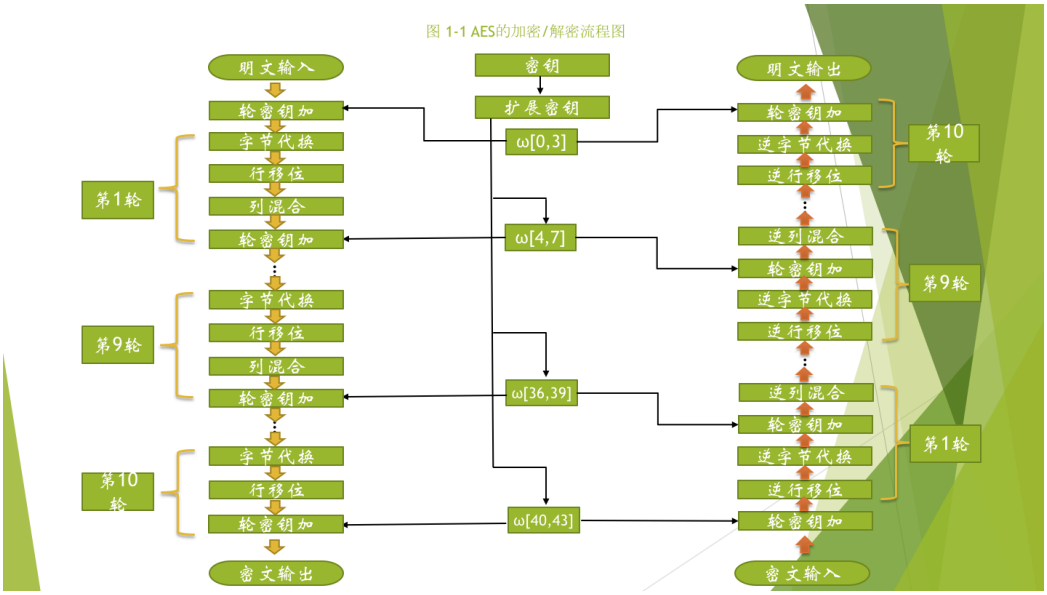
AES的密码设计力求满足以下3条标准：
① 抵抗所有已知的攻击
② 在多个平台上速度快，编码紧凑
③ 设计简单

WI-FI的主要目标有：
②信号较强
③更低的功耗
④改进的安全性

WI-FI工作于无线环境，易被侦听窃取，故需要使用加密手段防止传输的信息被泄露，如 `WEP` ， `WPA-PSK` ， `WPA2-PSK` ， `WPA-PSK + WPA2-PSK` 等，其中AES是WI-FI的重要加密手段

原理

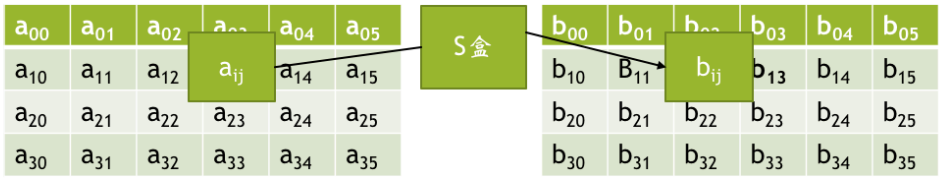
AES的加密/解密流程图



主要有四个步骤

一、字节代换(byteSub)

状态矩阵按照下面的方式映射成为一个新的字节：把该字节的高4位作为行值，低4位作为列值，得到S盒或逆S盒的对应元素作为输出



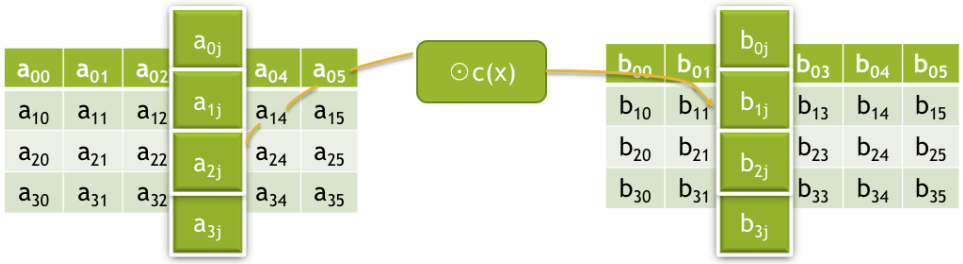
二、行移位(ShiftRow)

在行循环移位变换中，状态阵列的后3行循环移位不同的偏移量。第0行不移动。第1行循环移位C1字节，第2行循环移位C2字节，第3行循环移位C3字节。偏移量C1、C2、C3与分组长度Nb有关

三、列混合(MixColumn)

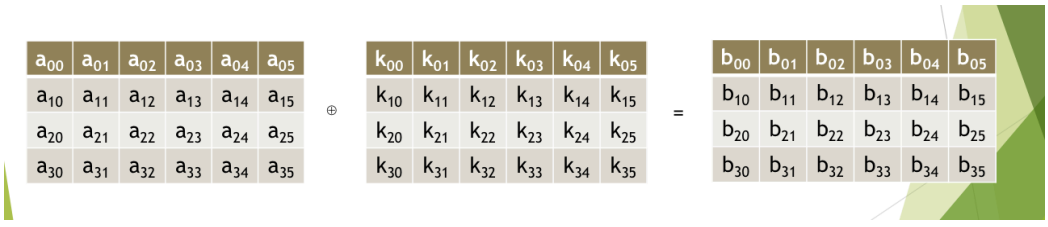
列混合运算将状态(State)的列看作是有限域GF(28)上的多项式a(x)，与多项式 `c(x) = '03' x3 + '01' x2 + '01' x +'02'` 相乘(在模 `(x4+1)` 下)

`b(x)=c(x) x a(x)(mod x4 + 1)`



四、密钥加

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



AES的密钥调度

密钥bit的总数 = 分组长度 x (轮数Round + 1)

当分组长度为128bit且轮数为10时，轮密钥长度为:

`128 x ( 10 + 1 ) = 1408 bit`

将初始密钥扩展成扩展密钥

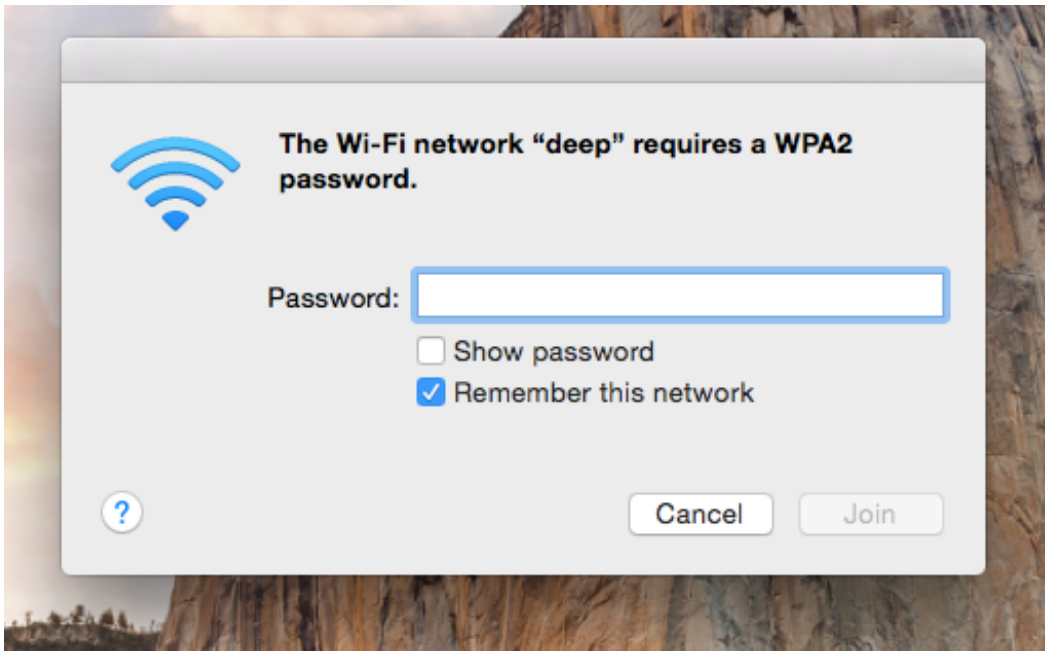
轮密钥从扩展密钥中取，第1轮轮密钥取扩展密钥的前Nb个字，第2轮轮密钥取

接下来的Nb个字，以此类推

密钥扩展
函数T由三部分组成：字循环移位、字节代换和轮常量异或
(1)字循环移位：将1个字中的4个字节循环左移1个字节，即将输入字 `[b0, b1 , b2 , b3]` 变换为 `[b1, b2 , b3 , b0]`
(2)字节代换：对字循环的结果使用S盒进行字节代换
(3)轮常量异或：将前两步的结果同轮常量Rcon[j]进行异或，其中j表示轮数
轮常量是一个字，使用轮常量是为了防止不同轮中产生的轮密钥的对称性或相似性

应用

连接到无线局域网通常是有密码保护的，在WI-FI所使用的几种加密方法中，WPA2-PSK即基于AES进行加密



据称：WPA2是WPA的升级版，目前的新型的网卡、AP都支持WPA2加密。其采用了更为安全的算法。CCMP取代了WPA的MIC、AES取代了WPA的TKIP。同样的因为算法本身几乎无懈可击,所以也只能采用暴力破解和字典法来破解。暴力破解是“不可能完成的任务”