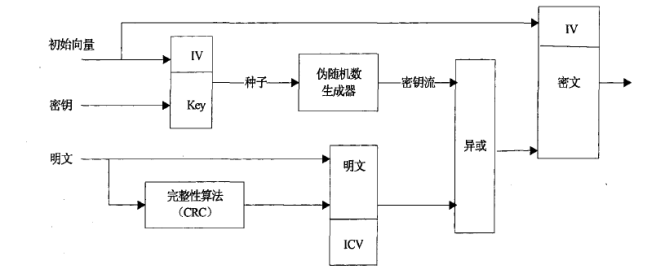
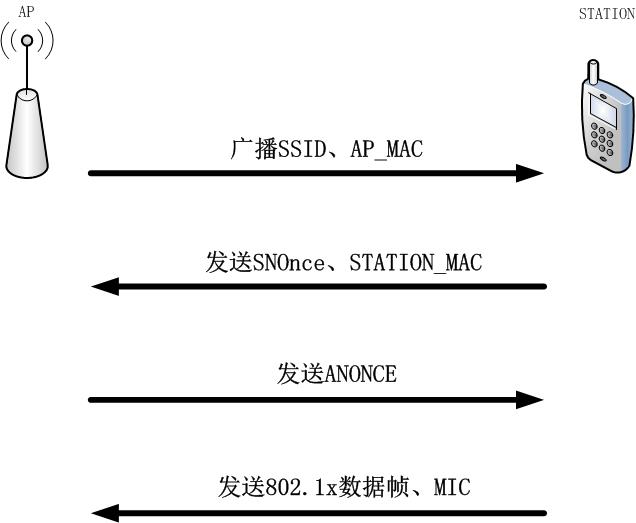
 **无线安全技术**   
**1) WEP(Wired Equivalent Privacy有线对等保密)**   
  
最早的无线加密体制，由于[**算法**](http://lib.csdn.net/base/datastructure)的缺陷很容易被破解。抓包获取在数据流中明文传输的IV，再通过统计学方法用IV得到密钥。

**2) WPA**   
在不升级硬件的前提下，WAP使用TKIP(Temporal Key Integrity Protocol临时密钥集成协议) 来实现WLAN的访问控制、密钥管理和数据加密来增强WEP的安全性。WPA加密算法有两个版本。   
**a) WPA = 802.1x + EAP + TKIP + MIC = Pre-shared Key + TKIP + MIC**   
**b) WPA2 = 802.1x + EAP + AES + CCMP = Pre-shared Key + AES + CCMP**

**注：**   
802.1x + EAP、Pre-shared Key：身份校验算法   
TKIP、AES：数据传输加密算法   
MIC、CCMP：数据完整性校验算法

802.1x + EAP （工业级的，安全要求高的地方用。需要认证服务器）EAP 扩展认证协议，是一种[**架构**](http://lib.csdn.net/base/architecture)，而不是具体算法。常见的有LEAP，MD5，TTLS，TLS，PEAP，SRP，SIM，AKA 其中的TLS 和TTLS 是双向认证模式。这种认证方式不怕网络劫持和字典攻击。   
Pre-shared Key （家庭用的，用在安全要求低的地方。不需要服务器）。容易被字典攻击

 **WPA-PSK**   
**1) WPA的四次握手过程**   
WPA 握手过程是基于802.1X 协议，使用eapol key进行封装传输。   
  
**a) AP初始化：**   
使用 SSID 和passphares作为入参，通过哈希算法产生PSK。在WPA-PSK 中**PSK=PMK=pdkdf2\_SHA1(passphrase, SSID, SSID length, 4096)**

**b) 第一次握手：**   
AP广播SSID，AP\_MAC(AA)；   
STATION 端使用接收到的SSID，AP\_MAC和passphares使用同样算法产生PSK。

**c) 第二次握手**   
STATION 发送一个随机数SNonce，STATION\_MAC(SA)给AP；   
AP端接收到SNonce、STATION\_MAC(SA)后产生一个随机数ANonce，然后用 PMK、AP\_MAC(AA)、STATION\_MAC(SA)、SNonce、ANonce 用以下SHA1\_PRF算法产生PTK，提取这个 PTK 前16 个字节组成一个MIC KEY。   
**PTK=SHA1\_PRF(PMK, Len(PMK), “Pairwise key expansion”, MIN(AA, SA) || Max(AA, SA) || Min(ANonce, SNonce) || Max(ANonce, SNonce))**

**d) 第三次握手：**   
AP发送上面产生的ANonce给STATION   
STATION 端用接收到ANonce 和以前产生PMK、SNonce、AP\_MAC(AA)、STATION\_MAC(SA)用同样的算法产生PTK。提取这个PTK 前16 个字节组成一个MIC KEY使用以下算法产生MIC值用这个MIC KEY 和一个802.1X数据帧使用以下算法得到MIC值   
**MIC = HMAC\_MD5(MIC Key，16，802.1X data)**

**e) 第四次握手**：   
STATION 发送802.1X 数据帧，MIC给AP；STATION 端用上面那个准备好的802.1X 数据帧在最后填充上MIC值和两个字节的0（十六进制）然后发送这个数据帧到AP。   
AP端收到这个数据帧后提取这个MIC。并把这个数据帧的MIC部分都填上0（十六进制）这时用这个802.1X数据帧，和用上面AP产生的 MIC KEY 使用同样的算法得出MIC’。如果MIC’等于STATION 发送过来的MIC。那么第四次握手成功。若不等说明则AP 和 STATION 的密钥不相同，握手失败了。

**2) WPA—PSK破解原理**   
用我们字典中的Passphrase+SSID先生成PMK，然后结合握手包中的STA\_MAC、AP\_MAC、ANONCE、SNONCE计算PTK，再加上原始的报文数据算出MIC并与AP发送的MIC比较，如果一致，那么该PSK就是密钥。