一．选择题

1.解决无线局域网安全问题的基本方法不包括（B）。

A接入控制 B数字签名和源端检测 C加密 D完整性检测

2.关于WEP,以下哪一项描述是错误的?(D）  
A.用循环冗余码检测数据完整性  
B.伪随机数生成算法作为产生一次性密钥的单向函数  
C.采用流密码体制  
D.一次性密钥不会重复  
由于所有终端共享个一次性密钥,因此很容易导致一次性密钥重复使用。

3.以下哪项不属于频段开放性和空间开放性带来的安全问题（D）。

A重放攻击 B信道干扰 C嗅探和流量分析 D ARP欺骗攻击

1. 判断题
2. WPA2有企业模式和个人模式。这两种工作模式的加密和数据完整性检测机制相同,双向身份鉴别机制不同。 （√）
3. WEP是一种有着比802.11i更强安全功能的无线局域网安全协议。

（×）

3.802.1x用EAP作为鉴别协议，因此可以使用EAP协议的多种鉴别机制。 （×）

1. 名词解释

1.共享密钥鉴别机制  
在WEP安全机制下,一种通过判断终端能否计算出某个IV对应的有效一次性密钥判断终端是否拥有与AP相同的共享密钥的身份鉴别机制。

2.基于MAC地址鉴别机制  
一种厂家普遍使用的，只允许MAC地址是访问控制列表中的MAC地址的终端接人BSS的身份鉴别机制。

1. 一次性密钥字典  
   一种对应种IV组合,获取指定长度的个一次性密钥,并通过长度扩展,求出不同长度下种IV组合对应的个一次性密钥的方法。
2. 论述题

1.简述WEP的缺陷。  
一是由于密钥有效期间,所有终端共享个一次性密钥,因此很容易通过建立一次性密钥字典破译密文;二是一旦黑客获得密钥,即可破译经过无线局域网传输的所有密文;三是身份鉴别机制容易被黑客破解;四是完整性检测机制无法检测出精心设计的筛改。

2.简述TKIP和CCMP的差异。

一是计算消息鉴别码的算法。TKIP采用Michael算法,CCMP采用AES和加密分组链接模式。二是计算消息鉴别码时,TKIP除了净荷外,只包括源和目的终端地址,CCMP包含MAC帧首部中所有传输过程中不变的字段。三是一次性密钥计算方法。TKIP采用伪随机数生成函数,CCMP采用AES和计数器模式。四是TKIP使用不同的密钥计算消息鉴别码和一次性密钥,CCMP用同一个密钥计算消息鉴别码和一次性密钥。