7-01

答：

1. 威胁：截获，中断，篡改，伪造。
2. 区别：主动攻击是指攻击者对某个连接中通过的PDU进行各种处理。如有选择地更改、删除、延迟这些PDU。甚至还可将合成的或伪造的PDU送入到一个连接中去。被动攻击是指观察和分析某一个协议数据单元PDU而不干扰信息流。主要在于有无对PDU的更改。
3. 安全措施：对于主动：使用加密技术与适当的鉴别技术结合；对于被动：采用各种数据加密动技术

7-05

答：

无条件安全：无论密文敌手花费多少时间都无进行解密

在计算机上安全：破译所耗费的价值超出了密文信息本身的价值或破译所花费的时间超出了密文的有效生存周期

7-07

答：

对称密码体制特点：加密密钥与解密密钥相同。

优点：加密、解密处理速度快，具有很高的数据吞吐率，硬件加密实现可达到几百兆字节每秒，软件也可以达到兆字节每秒的吞吐率。密钥相对较短。

缺点：对称密钥算法的密钥分发过程十分复杂，所花代价高。多人通信时密钥组合数量会出现爆炸性膨胀，使密钥分发更加复杂化，N个人进行两两通信，总共需要的密钥数为，通信双方必须统一密钥，才能发送保密的信息。对称密码算法还存在数字签名困难问题

公钥密码体制特点：其原理是加密密钥与解密密钥不同，形成一个密钥对，用其中一个密钥加密结果，只能用配对的另一个密钥来解密。一个密钥可以公开，称为公钥；另一个只能被密钥持有人自己保管，称为私钥。

优点：网络中每一个用户只需要保护自己的私钥，N个用户仅需要产生N对密钥，密钥少，便于管理。密钥分配简单，不需要秘密的通道和复杂的协议来传送密钥。可以实现数字签名

缺点：与对称密码体制相比，非对称密码体制加密、解密处理速度较慢，同等安全强度下，非对称密码体制的密钥位数要求多一些。

7-11

答：

1. 使用报文鉴别是为了对付主动攻击中的篡改和伪造。当报文加密的时候就可以达到报文鉴别的目的，但是当传送不需要加密报文时，接收者应该能用简单的方法来鉴别报文的真伪。
2. 鉴别和保密并不相同。鉴别是要验证通信对方的确是自己所需通信的对象，而不是其他的冒充者。鉴别分为报文鉴别和实体鉴别。授权涉及到的问题是：所进行的过程是否被允许(如是否可以对某文件进行读或写)。
3. 报文鉴别和实体鉴别不同。报文鉴别是对每一个收到的报文都要鉴别报文的发送者，而实体鉴别是在系统接入的全部持续时间内对和自己通信的对方实体只需验证一次。