计算机等级考试三级网络复习纲要[16] PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/180/2021_2022__E8_AE_A1_E7_AE_97_E6_9C_BA_E7_c97_180250.htm 计算机等级考试训练软件《百宝箱》10）主动攻击和被动攻击：（被动攻击的特点是偷听或监视传送。其目的是获得正在传送的信息。被动攻击有：泄露信息内容和通信量分析等。主动攻击涉及修改数据流或创建错误的数据流，它包括假冒，重放，修改信息和拒绝服务等。假冒是一个实体假装成另一个实体。假冒攻击通常包括一种其他形式的主动攻击。重放涉及被动捕获数据单元以及后来的重新发送，以产生未经授权的效果。修改消息意味着改变了真实消息的部分内容，或将消息延迟或重新排序，导致未授权的操作。拒绝服务的禁止对通信工具的正常使用或管理。这种攻击拥有特定的目标。另一种拒绝服务的形式是整个网络的中断，这可以通过使网络失效而实现，或通过消息过载使网络性能降低。防止主动攻击的做法是对攻击进行检测，并从它引起的中断或延迟中恢复过来。从网络高层协议角度看，攻击方法可以概括为：服务攻击与非服务攻击。服务攻击是针对某种特定网络服务的攻击。非服务攻击不针对某项具体应用服务，而是基于网络层等低层协议进行的。非服务攻击利用协议或操作系统实现协议时的漏洞来达到攻击的目的，是一种更有效的攻击手段。）（11）安全策略的组成：威严的法律、先进的技术、严格的管理（12）安全管理原则：多人负责原则、任期有限原则、职责分离原则（13）安全管理的实现 P161 9、保密学（1）概念：是研究密码系统或通信安全的科学（2）分类：密码学和密

码分析学 （3）几个相关概念：需要隐藏的消息叫做明文。明文被变换成另一种隐藏形式被称为密文。这种变换叫做加密。加密的逆过程称为解密。对明文进行加密所采用的一组规则称为加密算法。对密文解密时采用的一组规则称为解密算法。加密算法和解密算法通常是在一组密钥控制下进行的，加密算法所采用的密钥成为加密密钥，解密算法所使用的密钥叫做解密密钥。 （4）密码系统分类：（各自特点 P162-163） 按将明文转化为密文的操作类型分为：置换密码和易位密码。 按明文的处理方法可分为：分组密码（块密码）和序列密码（流密码）。 按密钥的使用个数分为：对称密码体制和非对称密码体制。 （5）数据加密技术可以分为3类：对称型加密，不对称型加密和不可逆加密。对称加密使用单个密钥对数据进行加密或解密。 不对称加密算法其特点是有两个密钥，只有两者搭配使用才能完成加密和解密的全过程。不对称加密的另一用法称为“ 数字签名 ”。不可逆加密算法的特征是加密过程不需要密钥，并且经过加密的数据无法被解密，只有同样输入的输入数据经过同样的不可逆算法才能得到同样的加密数据。 （6）从通信网络的传输方面，数据加密技术可以分为3类：链路加密方式，节点到节点方式和端到端方式。链路加密方式是一般网络通信安全主要采用的方式。节点到节点加密方式是为了解决在节点中数据是明文的缺点，在中间节点里装有加，解密的保护装置，由这个装置来完成一个密钥向另一个密钥的变换。在端到端加密方式中，由发送方加密的数据在没有到达最终目的节点之前是不被解密的。（链路加密方式和端到端加密方式的区别请补充） （7）试图发现明文或密钥的过程叫做密码分析。