计算机等级考试三级网络复习纲要[17] 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_180252.htm 计算机等级考试训练软件《百宝箱》（8）加密方案是安全的两种情形：P165 （9）对称加密体制的模型的组成部分P166 （10）对称加密有两个安全要求：1需要强大的加密算法。2发送方和接受方必须用安全的方式来获得保密密钥的副本，必须保证密钥的安全。对称加密机制的安全性取决于密钥的保密性，而不是算法的保密性。对称加密算法有: DES. TDEA （或称3DES ）.RC-5. IDEA等。IDEA算法被认为是当今最好最安全的分组密码算法。 （11）公开密钥加密又叫做非对称加密。是建立在数学函数基础上的一种加密方法,而不是建立在位方式的操作上的。公钥加密算法的适用公钥密码体制有两个密钥：公钥和私钥。公钥密码体制有基本的模型，一种是加密模型，一种是认证模型。 常规加密使用的密钥叫做保密密钥。公钥加密使用的密钥对叫做公钥或私钥。私钥总是保密的。RSA体制被认为是现在理论上最为成熟完善的一种公钥密码体制。 （12）密钥的生存周期是指授权使用该密钥的周期。密钥的生存周期的经历的阶段 P170。 （13）密钥分发技术是将密钥发送到数据交换的两方，而其他人无法看到的地方。通常KDC技术用于保密密钥分发，CA用于公钥和保密密钥的分发 （14）证书权威机构（CA）是用户团体可信任的第三方。数字证书是一条数字签名的消息，它通常用与证明某个实体的公钥的有效性。数字证书是一个数字结构，具有一种公共的格式，它将某一个成员的识别符和一个公钥值绑定在一起

。（15）认证是防止主动攻击的重要技术，它对于开放环境中的各种信息系统的安全有重要作用。认证是验证一个最终用户或设备的声明身份的过程。认证主要目的为：验证信息的发送者是真正的，而不是冒充的，这称为信源识别。验证信息的完整性，保证信息在传送过程中未被窜改，重放或延迟等。认证过程通常涉及加密和密钥交换。帐户名和口令认证方式是最常用的一种认证方式。授权是把访问权授予某一个用户，用户组或指定系统的过程。访问控制是限制系统中的信息只能流到网络中的授权个人或系统。有关认证使用的技术主要有：消息认证，身份认证和数字签名。消息认证是意定的接收者能够检验收到的消息是否真实的方法。又称完整性校验。 消息认证的内容包括为：1 证实消息的信源和信宿。2 消息内容是或曾受到偶然或有意的篡改。3 消息的序号和时间性。消息认证的方法一般是利用安全单向散列函数生成消息摘要。安全单向散列函数必须具有以下属性：它必须一致，必须是随机的，必须唯一，必须是单向的，必须易于实现高速计算。常用的散列函数有:消息摘要4（MD4）算法.消息摘要5（MD5）算法.安全散列算法（SHA）.身份认证大致分为3类：1 个人知道的某种事物。2 个人持证3 个人特征。口令或个人识别码机制是被广泛研究和使用的一种身份验证方法，也是最实用的认证系统所依赖的一种机制。为了使口令更加安全，可以通过加密口令或修改加密方法来提供更强健的方法，这就是一次性口令方案，常见的有S/KEY和令牌口令认证方案。 持证为个人持有物。数字签名没有提供消息内容的机密性. 10、加密技术应用于网络安全通常有两种形式，既面向网络和面向应用程序服务。面向网络服务的加密技

术通常工作在网络层或传输层，使用经过加密的数据包传送，认证网络路由及其其他网络协议所需的信息，从而保证网络的连通性和可用性不受侵害。在网络层上实现的加密技术对于网络应用层的用户通常是透明的。面向网络应用程序服务的加密技术使用则是目前较为流行的加密技术的使用方法。 11、身份认证协议：S/KEY口令协议、PPP认证协议、Kerberos协议 12、电子邮件的安全：PGP、S/MIME 