安全第一:三种网络安全机制概述 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/142/2021_2022__E5_AE_89_E5_85_A8_E7_AC_AC_E4_c101_142474.htm 随着TCP/IP协议群在互联网上的广泛采用，信息技术与网络技术得到了飞速发展。随之而来的是安全风险问题的急剧增加。为了保护国家公众信息网以及企业内联网和外联网信息和数据的安全，要大力发展基于信息网络的安全技术。 信息与网络安全技术的目标 由于互联网的开放性、连通性和自由性，用户在享受各类共有信息资源的同事，也存在着自己的秘密信息可能被侵犯或被恶意破坏的危险。信息安全的目标就是保护有可能被侵犯或破坏的机密信息不被外界非法操作者的控制。具体要达到：保密性、完整性、可用性、可控性等目标。 网络安全体系结构 国际标准化组织（ISO）在开放系统互联参考模型（OSI/RM）的基础上，于1989年制定了在OSI环境下解决网络安全的规则：安全体系结构。它扩充了基本参考模型，加入了安全问题的各个方面，为开放系统的安全通信提供了一种概念性、功能性及一致性的途径。OSI安全体系包含七个层次：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。在各层次间进行的安全机制有： 1、加密机制 衡量一个加密技术的可靠性，主要取决于解密过程的难度，而这取决于密钥的长度和算法。 1）对称密钥加密体制对称密钥加密技术使用相同的密钥对数据进行加密和解密，发送者和接收者用相同的密钥。对称密钥加密技术的典型算法是DES（Data Encryption Standard数据加密标准）。DES的密钥长度为56bit，其加密算法是公开的，其保密性仅取决于对

密钥的保密。优点是：加密处理简单，加密解密速度快。缺点是：密钥管理困难。 2）非对称密钥加密体制非对称密钥加密系统，又称公钥和私钥系统。其特点是加密和解密使用不同的密钥。 （1）非对称加密系统的关键是寻找对应的公钥和私钥，并运用某种数学方法使得加密过程成为一个不可逆过程，即用公钥加密的信息只能用与该公钥配对的私钥才能解密；反之亦然。 （2）非对称密钥加密的典型算法是RSA。RSA算法的理论基础是数论的欧拉定律，其安全性是基于大数分解的困难性。 优点：（1）解决了密钥管理问题，通过特有的密钥发放体制，使得当用户数大幅度增加时，密钥也不会向外扩散；（2）由于密钥已事先分配，不需要在通信过程中传输密钥，安全性大大提高；（3）具有很高的加密强度。 缺点：加密、解密的速度较慢。 2、安全认证机制 在电子商务活动中，为保证商务、交易及支付活动的真实可靠，需要有一种机制来验证活动中各方的真实身份。安全认证是维持电子商务活动正常进行的保证，它涉及到安全管理、加密处理、PKI及认证管理等重要问题。目前已经有一套完整的技术解决方案可以应用。采用国际通用的PKI技术、X.509证书标准和X.500信息发布标准等技术标准可以安全发放证书，进行安全认证。当然，认证机制还需要法律法规支持。安全认证需要的法律问题包括信用立法、电子签名法、电子交易法、认证管理法律等。 1）数字摘要 数字摘要采用单向Hash函数对信息进行某种变换运算得到固定长度的摘要，并在传输信息时将之加入文件一同送给接收方；接收方收到文件后，用相同的方法进行变换运算得到另一个摘要；然后将自己运算得到的摘要与发送过来的摘要进行比较。这种方法可以

验证数据的完整性。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com