公钥基础设施技术基础电子商务师考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022__E5_85_AC_E9_92_A5_E5_9F_BA_E7_c40_645335.htm 一、前言 全球经济发展正在进入信息经济时代，知识经济初见端倪。作为二十一世纪的主要经济增长方式--电子商务，将给各国和世界经济带来巨大的变革，产生深远的影响。电子商务通过大幅度降低交易成本，增加贸易机会，简化贸易流程，提高贸易效率.电子商务提高生产力，改善物流系统，并推动企业和国民经济结构的改革。对电子商务的关注和投入可以发展新兴产业，创造就业机会，推动国家和全球经济的发展。电子商务是一个新兴市场，而且是一种替代传统商务活动的新形式。它有可能彻底改变贸易活动的本质，形成一套全新的贸易活动框架。但如何保证Internet网上信息传输的安全，是发展电子商务的重要环节。 为解决Internet的安全问题，世界各国对其进行了多年的研究，初步形成了一套完整的Internet安全解决方案，即目前被广泛采用的PKI技术(Public Key Infrastructure-公钥基础设施)，PKI(公钥基础设施)技术采用证书管理公钥，通过第三方的可信任机构--认证中心CA(Certificate Authority)，把用户的公钥和用户的其他标识信息(如名称、e-mail、身份证号等)捆绑在一起，在Internet网上验证用户的身份。目前，通用的办法是采用建立在PKI基础之上的数字证书，通过把要传输的数字信息进行加密和签名，保证信息传输的机密性、真实性、完整性和不可否认性，从而保证信息的安全传输。 二、PKI基础 PKI基础设施采用证书管理公钥，通过第三方的可信任机构--认证中心，把用户

的公钥和用户的其他标识信息捆绑在一起，在Internet网上验证用户的身份。PKI基础设施把公钥密码和对称密码结合起来，在Internet网上实现密钥的自动管理，保证网上数据的安全传输。 从广义上讲，所有提供公钥加密和数字签名服务的系统，都可叫做PKI系统，PKI的主要目的是通过自动管理密钥和证书，可以为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便的使用加密和数字签名技术，从而保证网上数据的机密性、完整性、有效性，数据的机密性是指数据在传输过程中，不能被非授权者偷看.数据的完整性是指数据在传输过程中不能被非法篡改.数据的有效性是指数据不能被否认。一个有效的PKI系统必须是安全的和透明的，用户在获得加密和数字签名服务时，不需要详细地了解PKI是怎样管理证书和密钥的，一个典型、完整、有效的PKI应用系统至少应具有以下部分： 公钥密码证书管理。 黑名单的发布和管理。 密钥的备份和恢复。 自动更新密钥。 自动管理历史密钥。 支持交叉认证。 由于PKI基础设施是目前比较成熟、完善的Internet网络安全解决方案，国外的一些大的网络安全公司纷纷推出一系列的基于PKI的网络安全产品，如美国的Verisign, IBM ,加拿大的Entrust、SUN等安全产品供应商为用户提供了一系列的客户端和服务器端的安全产品，为电子商务的发展以及政府办公网、EDI等提供了安全保证。简言之，PKI(Public Key Infrastructure)公钥基础设施就是提供公钥加密和数字签名服务的系统，目的是为了管理密钥和证书，保证网上数字信息传输的机密性、真实性、完整性和不可否认性。 1.单钥密码算法(加密) 单钥密码算法，又称对称密码算法：是指加密密钥和解密密钥为同一密钥的密码算法。因此

，信息的发送者和信息的接收者在进行信息的传输与处理时，必须共同持有该密码(称为对称密码)。在对称密钥密码算法中,加密运算与解密运算使用同样的密钥。通常,使用的加密算法比较简便高效,密钥简短,破译极其困难.由于系统的保密性主要取决于密钥的安全性,所以，在公开的计算机网络上安全地传送和保管密钥是一个严峻的问题。最典型的是DES(Data Encryption Standard)算法。 DES(Data Encryption Standard，数据加密标准)算法，它是一个分组加密算法，它以64 bit位(8 byte)为分组对数据加密，其中有8 bit奇偶校验，有效密钥长度为56 bit。64位一组的明文从算法的一端输入，64位的密文从另一端输出。DES是一个对称算法，加密和解密用的是同一算法。DES的安全性依赖于所用的密钥。 密钥的长度为56位。(密钥通常表示为64位的数，但每个第8位都用作奇偶校验，可以忽略。)密钥可以是任意的56位的数，且可以在任意的时候改变。其中极少量的数被认为是弱密钥，但能容易地避开它们。所有的保密性依赖于密钥。简单地说，算法只不过是加密的两个基本技术--混乱和扩散的组合。DES基本组建分组是这些技术的一个组合(先代替后置换)，它基于密钥作用于明文，这是众所周知的轮(round)。DES有16轮，这意味着要在明文分组上16次实施相同的组合技术。此算法只使用了标准的算术和逻辑运算，而其作用的数也最多只有64位。 DES对64位的明文分组进行操作，通过一个初始置换，将明文分组分成左半部分和右半部分，各32位长。然后进行16轮完全相同的运算，这些运算被称为函数f，在运算过程中数据与密钥结合。经过16轮后，左、右半部分合在一起经过一个末置换(初始置换的逆置换)，这样该算法就

完成了。在每一轮中，密钥位移位，然后再从密钥的56位中选出48位。通过一个扩展置换将数据的右半部分扩展成48位，并通过一个异或操作与48位密钥结合，通过8个s盒将这48位替代成新的32位数据，再将其置换一次。这四步运算构成了函数f。然后，通过另一个异或运算，函数f输出与左半部分结合，其结果即成为新的右半部分，原来的右半部分成为新的左半部分。将该操作重复16次，便实现了DES的16轮运算。假设Bi是第i次迭代的结果，Li和Ri是Bi的左半部分和右半部分，Ki是第i轮的48位密钥，且f是实现代替、置换及密钥异或等运算的函数，那么每一轮就是： 2.双钥密码算法(加密、签名) 双钥密码算法，又称公钥密码算法：是指加密密钥和解密密钥为两个不同密钥的密码算法。公钥密码算法不同于单钥密码算法，它使用了一对密钥：一个用于加密信息，另一个则用于解密信息，通信双方无需事先交换密钥就可进行保密 三.PKI组成 PKI是一种新的安全技术，它由公开密钥密码技术、数字证书、证书发放机构(CA)和关于公开密钥的安全策略等基本成分共同组成的。PKI是利用公钥技术实现电子商务安全的一种体系，是一种基础设施，网络通讯、网上交易是利用它来保证安全的。从某种意义上讲，PKI包含了安全认证系统，即安全认证系统-CA/RA系统是PKI不可缺的组成部分。PKI(Public Key Infrastructure)公钥基础设施是提供公钥加密和数字签名服务的系统或平台，目的是为了管理密钥和证书。一个机构通过采用PKI框架管理密钥和证书可以建立一个安全的网络环境。PKI主要包括四个部分：X.509格式的证书(X.509 V3)和证书废止列表CRL(X.509 V2).CA/RA操作协议.CA管理协议.CA政策制定。一个典型、完整、有效的PKI应用系统至

少应具有以下部分. 认证中心CA CA是PKI的核心，CA负责管理PKI结构下的所有用户(包括各种应用程序)的证书，把用户的公钥和用户的其他信息捆绑在一起，在网上验证用户的身份，CA还要负责用户证书的黑名单登记和黑名单发布，后面有CA的详细描述。 X.500目录服务器 X.500目录服务器用于发布用户的证书和黑名单信息，用户可通过标准的LDAP协议查询自己或其他人的证书和下载黑名单信息。来源：考试大 具有高强度密码算法(SSL)的安全WWW服务器 出口到中国的WWW服务器，如微软的IIS、Netscape的WWW服务器等，受出口限制，其RSA算法的模长最高为512位，对称算法为40位，不能满足对安全性要求很高的场合，为解决这一问题，采用了山东大学网络信息安全研究所开发的具有自主版权的SSL安全模块，在SSL安全模块中使用了自主开发的SJY系列密码设备，并且把SSL模块集成在Apache WWW服务器中，Apache WWW服务器在WWW服务器市场中占有百分之50以上的份额，其可移植性和稳定性很高。 Web(安全通信平台) Web有Web Client端和Web Server端两部分，分别安装在客户端和服务器端，通过具有高强度密码算法的SSL协议保证客户端和服务器端数据的机密性、完整性、身份验证。 自开发安全应用系统 自开发安全应用系统是指各行业自开发的各种具体应用系统，例如银行、证券的应用系统等。 完整的PKI包括认证政策的制定(包括遵循的技术标准、各CA之间的上下级或同级关系、安全策略、安全程度、服务对象、管理原则和框架等)、认证规则、运作制度的制定、所涉及的各方法律关系内容以及技术的实现。 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