2012版 权威·实用

紧扣大纲　直击要点　链接真题　一点就通

全国计算机等级考试6日达标

冲刺模拟+考点速记

全国计算机等级考试命题研究组◎编

三级 网络技术

考点全 真题多

多角度细致点评　讲解精髓　题目精选　针对性强

计算机等级考试

经过2年的研究与锤炼，从去年的7日达标延伸出来的更适合考生学习的这本6日达标终于付印成册。通过剖析考点、链接真题、达到精讲精练、使考生练一次就能上考场，赢高分。

链接多年真题

● 精选常考

练一次就能上考场

精选常考知识点、分类讲解、把握核心概念，做到事半功倍，考点中贯穿真题讲解，加深理解，短期内迅速提升。吃透重要考点，考试不再难。

直击常考点

精选常考知识点、分类讲解、把握核心概念，做到事半功倍，考点中贯穿真题讲解，加深理解，短期内迅速提升。吃透重要考点，考试不再难。

考点全面，针对性强。上考场前应知的考点通过提取常考知识点，抓住考试重点难点，分类讲解，便于考生专项攻克，迅速掌握命题规律与考试重点。

考点全 真题多

解、把握核心概中贯穿真题讲解，升。吃透重要考

高无难题

各类考试押题，全面覆盖所需考的知识点，通过反复练习考题，推敲解题方法，做到熟练掌握各种命题，巩固知识点，做到点面结合。

大学生最喜爱的等考品牌
北邮·等考

北京邮电大学出版社
www.buptpress.com

全国计算机等级考试6日达标

（冲刺模拟十考点速记）

——三级网络技术

全国计算机等级考试命题研究组　编

北京邮电大学出版社
·北京·

内容简介

本书由全国计算机等级考试一线命题研究人员联手多年从事考前培训与阅卷的专家一起为希望快速提高、过关的考生设计的一套高效应试方案。其内容包括：上考场前应知的考点、上考场前应练习的真题、上考场前应练习的题库三大部分。上考场前应知的考点通过提取常考知识点，抓住考试重点难点，分类讲解，贯穿真题、便于考生专项攻克；上考场前应练习的真题是选取最新几套考试真题、把握命题规律、便于考生了解最新考试动态。上考场前应练习的题库是根据最新版考试大纲的要求，由多年研究等级考试考纲、试题及相关政策的老师编写，覆盖所有考点。

此外，本书附赠超值软件，软件中包括10套笔试试卷和10套上机试卷。上机考试环境和操作界面与真题一致，并提供上机操作的视频演示。

本书精心设计应试板块，用最科学的方式引导考生在最短时间内获得最大收获，非常适合考前快速突破过关，也适合高等院校作为相关教学及培训辅导用书。

图书在版编目(CIP)数据

全国计算机等级考试6日达标：冲刺模拟＋考点速记. 三级网络技术/全国计算机等级考试命题研究组编. --北京：北京邮电大学出版社，2012.1

ISBN 978-7-5635-2805-9

Ⅰ.①全… Ⅱ.①全… Ⅲ.①电子计算机—水平考试—自学参考资料②计算机网络—水平考试—自学参考资料 Ⅳ.①TP3

中国版本图书馆CIP数据核字(2011)第217800号

书　　名：全国计算机等级考试6日达标(冲刺模拟＋考点速记)——三级网络技术
作　　者：全国计算机等级考试命题研究组
责任编辑：满志文　姚　顺
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路10号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京联兴华印刷厂
开　　本：880 mm×1 100 mm　1/16
印　　张：8.5
字　　数：336千字
版　　次：2012年1月第1版　2012年1月第1次印刷

ISBN 978-7-5635-2805-9　　定价：25.00元

前　言

计算机作为一种得到广泛应用的工具，其重要性与日俱增。越来越多的人开始学习计算机知识，很多单位已经把计算机应用能力作为考核、录用工作人员的重要条件之一。各种计算机水平考试也随之应运而生，其中最受欢迎和信赖的就是教育部考试中心所组织的“全国计算机等级考试”。

本书在上一版“7日达标”的基础上，整合考生的心理，深入分析，研究出更适合考生学习和掌握的方法。

本书特点如下：

➢ 精心设计，高效实用。本书由全国计算机等级考试一线命题研究人员联手多年从事考前培训与阅卷的专家一起为希望快速提高和过关的考生设计的一套高效应试方案。其主要内容包括：上考场前应知的考点、上考场前应练习的真题、上考场前应练习的题库三大部分。本书精心设计应试板块，用最科学的方式引导考生在最短的时间内获得最大收获，非常适合考前快速突破过关！

➢ 考点全面，针对性强。上考场前应知的考点通过提取常考知识点，抓住考试重点难点，分类讲解，便于考生专项攻克，迅速掌握命题规律与考试重点。

➢ 穿插真题，专项巩固。本书在每个考点讲解下穿插与考点相关的真题，逐个讲解，透彻分析，便于考生一一理解，专项巩固。

➢ 最新真题，详尽解析。选取最新几套考试真题，让考生亲临考场，将记忆中的考点分散到具体考题当中，更能把握出题思路，吃透真题，把握最新考试动态。

➢ 题库丰富，点面结合。精选各类考试押题，全面覆盖所需考的知识点，通过反复练习考题，推敲解题方法，做到熟练掌握各种命题，巩固知识点，做到点面结合。

➢ 注重上机。本书在提供笔试试题的同时，给予相应的上机试题。通过对上机考试时题库的深入研究，精选出最具有代表性的真题，方便考生过关练习，举一反三。

➢ 书盘结合，题量超大。盘中提供超大容量试卷库与答案解析，全真模拟环境，便于考生实战演练，适应上机考试。

➢ 作者实力强。作者团队是从事等级考试近10年的辅导、培训、命题、阅卷、及编写的经验，有较高的权威性，图书质量有保障。

本丛书由全国计算机等级考试命题研究组主编。参与本书编写与资料收集工作的有：秦海泉、陈忠贤、樊圣兰、俞翠兰、陈海霞、袁鸿鹏、陈斌、蔡季平、陈娟娟、刘卉、徐杨阳、白晖、李海磊、顾兴健、王连涛、陈海燕、赵海峰、李晓飞、吴松松、何光明。

由于水平有限，加上时间紧迫，书中难免有不足之处，恳请各位同仁和广大读者批评指正。如遇到疑难问题，可以通过以下方式与我们联系：bjbaba@263.net。微博地址：（北邮等考）http://weibo.com/u/2297589741。

全国计算机等级考试命题研究组

2012年1月

目　录

（工欲善其事，必先利其器；知已知彼，百战不殆）

第一部分

上考场前应知的考点

提取常考知识点，抓住考试重点难点，分类讲解，便于及时预习或复习，通过把握重要枝干来延伸细枝末节，在每个考点中插入链接到的相关真题，有助于更深入直观的理解考点，化抽象的概念为具体的题目，使考生在上考场前能够逐个理解掌握。

考点精讲一：因特网接入

评注：这类题型主要考查因特网的接入，普通 Modem 拨号接入方式等。考生要知道调制解调器的作用，计算机通过电话网接入因特网需要安装哪些设备。接入因特网需要向 ISP（因特网服务供应商）提出申请。将计算机输出的数字信息转换成普通电话线路能够传输的信号，叫做调制；将从电话线路接收的信号转化成计算机能够处理的数字信号，叫做解调。

历年真题链接

真题 1 如果用户计算机通过电话网接入因特网，那么用户端必须具有_____。（2008 年 9 月）

A）路由器　　B）交换机

C）集线器　　D）调制解调器

答案：D

解析：电话线路中传输的是模拟信号，而计算机处理的则是数字信号，要通过电话网上网必须有一设备进行数字信号与模拟信号的相互转换。这个设备就是调制解调器。

考点精讲二：宽带接入网技术

评注：这类题型主要考查电信网、有线电视网和计算机网三网的区别与融合，综合业务数字网及宽带综合业务数字网。考生应注意有线电视网采用的拓扑结构，B-ISDN 协议的组成，B-ISDN 的速率，B-ISDN的业务分类，综合业务数字网的设计目标。

B-ISDN 采用异步传输模式 ATM，实现高效的传输、交换和复用。B-ISDN 协议参考模型分为 3 面和 3 层的立体结构，考生需要记住下面三点：

（1）B-ISDN 的核心技术是采用异步传输模式 ATM。核心技术关键技术是满足各种各样的服务质量 QoS 要求。其目标是实现 4 个层次上的综合即综合接入、综合交换、综合传输、综合管理。速率在 155 Mbit/s 以上，而 N-ISDN 速率为144 kbit/s，采用 2B＋D 信道（B 信道64 kbit/s，D 信道 16 kbit/s）。

（2）B-ISDN 的业务分为两类：交互型业务（指在用户间或用户与主机之间提供双方信息交换的业务。包括会话性业务、消息性业务、检索性业务）和发布型业务（由网络中某点向其他多个位置传送单向信息流的业务）（补充实例）。

（3）B-ISDN 的协议参考模型：分为 3 面和 3 层，3 面分别称为用户面，控制面和管理面。每个面又分为 3 层：物理层，ATM 层和 ATM 适配层。

考点精讲三：SDH 技术

评注：这类题型主要考查 SDH 的特点，组网形式，SDH 的自愈环及其发展。

同步数字体系（SDH）主要特点：同步复用、标准的网络接口、强大的网络管理。SDH 的网络单元包含有终端复用器、分插复用器 ADM 和数字交叉连接设备 DXC 等。所谓自愈网就是无需人为干预，网络就能在极短的时间内从失效故障中自动恢复所承载的业务，使用户不会感到网络已经出故障。其基本原理就是使网络具备发现替代传输路由并重新确立通信的能力。

SDH 速率：SDH 信号最基本也是最重要的模块信号是 STM-1，其速率为 155.520 Mbit/s。更高等级的 STM-N 是将 STM-1 同步复用而成。STM-1 每秒的传输速率为 $9\times270\times8\times8000=155.52$ Mbit/s。（帧长度计算公式：$9\times270\times N$ 单位为：字节，帧传输速率计算公式：$9\times270\times N\times8\times8000$单位为：bit/s）。

考点精讲四：ATM 技术

评注：这类题型主要考查 ATM 技术的定义和特点，ATM 协议栈，ATM 信元结构。这类题目需要考生记住 ATM 技术的定义和特点，ATM 适配层，ATM 协议栈及 ATM 信元结构。

ATM 是一种分组交换和复用技术，它是一种未来多种业务设计的通用的面向连接的传输模式。ATM 是一种传输模式，这种模式是异步的。ATM 用固定长度的分组发送信息，每个信元在其头部包含一个虚信道标识符（VCI），VCI 提供一种方法，以创建多条逻辑信道，并在需要

时多路复用。因为信元长度固定,信元可能包含无用的比特。ATM技术的重要特征有:信元传输、面向连接、统计多路复用和服务质量。ATM协议本身可以分为3层:ATM适配层、ATM层和物理层。

ATM信元结构:ATM信元由53字节组成,前5个字节是信头,其余48字节是信息字段。

ATM实际上是一个非常简单的协议,它仅仅把数据从一个端点传送到另一个端点,它本身并不提供差错恢复。ATM作为B-ISDN的核心技术,特别适合高带宽和低时延应用。ATM的网络优点:非常适合标记交换、响应时间短、高速和高带宽、综合网络、从用户端综合接入、现有协议和传统LAN的互连。

历年真题链接

真题2 ATM采用的传输模式为_____。(2008年4月)

A) 同步并行通信

B) 同步串行通信

C) 异步并行通信

D) 异步串行通信

答案:B

解析:ATM是以信元为基础的一组分组和复用技术,是一种为了多种业务涉及的通用的面向连接的传输模式。在ATM的传输模式中,信息被组织成"信元",来自某用户信息的各个信元不需要周期性地出现。而实际上,信元中每个位常常是同步定时发送的,即通常所说的"同步串行通信"。

真题3 ATM的主要技术特征有:多路复用、面向连接、服务质量和_____传输。(2008年9月)

答案:信元传输

解析:ATM作为B-ISDN的核心技术,特别适合高带宽和低时延应用,ATM技术的重要特征有:信元传输、面向连接、统计多路复用和服务质量。ATM的基本传输单元是信元,数据都是被封装在信元中传输的。

考点精讲五:xDSL技术

评注:这类题型主要考查xDSL技术的特征及几种方式的比较。常考xDSL的特点及几种方式的比较。考生应记住哪些是对称传输的,哪些是非对称传输的。

xDSL是DSL的统称,意即数字用户线路,是以铜电话线为传输介质的点对点传输技术。DSL技术是利用在电话系统中没有被利用的高频信号传输数据。DSL利用了更加先进的调制技术。DSL技术主要分为对称和非对称两大类。xDSL技术按上行和下行的速率是否相同可分为对称型和非对称型两种。对称型的有:HDSL、SDSL、IDSL,非对称型的有ADSL、VDSL、RADSL。

ADSL是xDSL中的一种,称为非对称数字用户线。ADSL是基于ATM的一项物理层点对点数据传输技术,可支持多种网络协议。ADSL是一种上行和下行速率不对称的技术,上行速率为16 kbit/s~640 kbit/s,下行速率可以达到1.5 Mbit/s至8 Mbit/s。ADSL最大传输距离为5.5 km。Cabel Modem是一种专门为有线电视网络传输而设计的,连接用户计算机和有线电视同轴电缆,利用频分复用的方法,上行信道采用的载波频率范围在5~42 MHz,上行带宽在200 kbit/s~10 Mbit/s,下行信道采用的载波频率范围在450~750 MHz,信道带宽最高可达36 Mbit/s。

历年真题链接

真题4 关于xDSL技术的描述中,错误的是_____。(2008年4月)

A) VDSL是非对称传输

B) HDSL是对称传输

C) SDSL是非对称传输

D) ADSL是非对称传输

答案:C

解析:xDSL技术按上行和下行的速率是否相同可分为对称型和非对称型两种,对称型的有:HDSL、SDSL、IDSL,非对称型的有ADSL、VDSL、RADSL。

真题5 关于ADSL技术的描述中,错误的是_____。(2008年9月)

A) 上下行传输速率不同

B) 可传输数据、视频等信息

C) 可提供1 Mbit/s上行信道

D) 可在10 km距离提供8 Mbit/s下行信道

答案:D

解析:ADSL为非对称数字用户线,其非对称性表现在局端到用户端的下行速率和用户端到局端的上行速率不同。下行速率高,一般在1.5~8 Mbit/s之间,传送距离可达3.6 km,可向用户传输数据、视频、音频信息及控制、开销信号。上行速率低,一般在640 kbit/s~1 Mbit/s之间。

考点精讲六:HFC接入技术

评注:这类题型主要考查HFC的基本结构,电缆调制解调器,HFC的数据传输。HFC网是一种以模拟频分复用技术为基础,综合应用模拟和数字传输技术、光纤和同轴电缆技术、射频技术和调解技术的接入网络。HFC(Hybrid Fiber Coax),即光纤到同轴电缆混合网从拉入用户的角度来看是经过双向改造的有线电视网络,但从总体上来看它是以同轴电缆网络为最终接入部分的宽带网络系统。HFC电缆调制解调器的数据传输一般采用一种所谓的"幅载波调制式"方式进行,即利用一般有线电视的频带划分单位,然后将数据调制到某个电视频道中进行传输。

光纤结点将光纤干线和同轴分配线相互连接。光纤结点通过同轴电缆下引线可以为500~2 000个用户服务,这些用户共享同一根传输介质。除了实现高速上网外,还可以实现可视电话、电视会议、远程教学、IP电话、视频点播等数据传输服务。HFC的优势是频带宽、速度快。缺点是价格昂贵、回传信道干扰及多用户对有限资源的争用出现阻塞,可能会影响接入速率。

历年真题链接

真题6 HFC网络进行数据传输时采用的调制方式为_____调制。(2008年4月)

答案:幅载波

解析:HFC的数据传输一般采用所谓的"幅载波调制"方式进行的,即利用一般有线电视的频道作为频宽划分单位,然后将数据调制到某个电视频道中进行传输。

真题7 HFC网络依靠于复用技术,从本质上看其复用属于_____。(2008年9月)

A) 时分复用　　B) 频分复用

C) 码分复用　　D) 空分复用

答案:B

解析:HFC 网是一种以模拟频分复用技术为基础,综合应用模拟和数字传输技术、光纤和同轴电缆技术、射频技术和调解技术的接入网络。

真题 8　HFC 采用了以下哪个网络接入 Internet? _____。(2009 年 9 月)

A) 有线电视网　　B) 有线电话网

C) 无线局域网　　D) 移动电话网

答案:A

解析:HFC(Hybrid Fiber Coaxial)网是指光纤同轴电缆混合网,它是一种新型的宽带网络,采用光纤到服务区,而在进入用户的"最后 1 公里"采用同轴电缆,最常见的也就是有线电视网络,它比较合理有效地利用了当前的先进成熟技术,融数字与模拟传输为一体,集光电功能于一身,同时提供较高质量和较多频道的传统模拟广播电视节目、较好性能价格比的电话服务、高速数据传输服务和多种信息增值服务,还可以逐步开展交互式数字视频应用。

考点精讲七:无线接入技术

评注:这类题型主要考查无线接入技术的分类技术。考生需重点关注蓝牙技术,3G,GSM 接入技术和 802.11 技术。无线接入网可分为固定无线接入网和移动接入网两大类。主要分为 GSM 接入技术、CDMA 接入技术、GPRS 接入技术、蓝牙技术和 WCDMA 技术。国际电信联盟(ITU)在 2000 年 5 月确定 W-CDMA,CDMA2000 和 TD-SCDMA 为三大主流无线接口标准,而 GPRS(General Packet Radio System)是封包交换数据的标准技术。蓝牙技术是一种传输范围约为 10 m 左右的短距离无线通信标准,用于在便携式计算机、移动电话及其他的移动设备之间建立一种小型、经济、短距离的无线链路。

历年真题链接

真题 9　EDGE(数据速率增强型 GSM)技术可以达到的最高数据传输速率为_____。(2008 年 4 月)

A) 64 kbit/s　　B) 115 kbit/s

C) 384 kbit/s　　D) 512 kbit/s

答案:C

解析:EDGE(数据速率增强型 GSM)接入技术是一种提高 GPRS 信道编码效率的高速移动数据标准,数据传输速率最高达 384 kbit/s。

真题 10　802.11 技术和蓝牙技术可以共同使用的无线信道频点是_____。(2008 年 9 月)

A) 800 MHz　　B) 2.4 GHz

C) 5 GHz　　D) 10 GHz

答案:B

解析:2.4 GHz 频带在大部分国家免授权、免费使用,因此得到了广泛应用。802.11、802.11b、蓝牙、HomeRF 等标准都工作在 2.4 GHz 频带。

考点精讲八:QoS

评注:这类题型主要考查 QoS 协议的特点。考生应注意 QoS 中几种常用的协议。

QoS 是一个网络部件(如一个应用、一台主机或一个路由器)提供的一些保证稳定传输网络数据的质量级别。DiffServ、资源预留协议(RSVP)、多协议标识交换(MPLS)、支持 IP 组播都是为适应对媒体应用而改进传统网络的方法。对在 IP 协议中增加 IP 多播协议可以支持多媒体网络应用,这与 QoS 没什么联系。资源预留协议根据应用的需求在各个结点预留资源,保证数据传输通路中的数据流能满足 QoS 要求;区分服务 DiffServ 利用 IP 分组头对数据的服务级别进行标识,路由器根据标识建立一条能满足 QoS 的传输通道;多协议标识交换技术的核心是标记交换,标记是一个用于数据分组交换的、短的、固定长度的转发标识符。

历年真题链接

真题 11　关于 QoS 协议特点的描述中,错误的是_____。(2008 年 4 月)

A) RSVP 根据需求在各个交换结点预留资源

B) DiffServ 根据 IP 分组头的服务级别进行标识

C) MPLS 标记是一个用于数据分组交换的转发标识符

D) IP 协议中增加 CDMA 多播协议可以支持多媒体网络应用

答案:D

解析:区分服务 DiffServ、资源预留协议 RSVP、多协议标识交换 MPLS、支持 IP 组播都是为适应对媒体应用而改进传统网络的方法。对在 IP 协议中增加 IP 多播协议可以支持多媒体网络应用,这与 QoS 没什么联系。资源预留协议根据应用的需求在各个结点预留资源,保证数据传输通路中的数据流能满足 QoS 要求;区分服务 DiffServ 利用 IP 分组头对数据的服务级别进行标识,路由器根据标识建立一条能满足 QoS 的传输通道;多协议标识交换技术的核心是标记交换,标记是一个用于数据分组交换的、短的、固定长度的转发标识符。

考点精讲九:电子商务

评注:这类题型主要考查电子商务定义及分类。考生应知道什么是电子商务,电子商务主要实现哪些功能。

电子商务是以计算机与通信网络为基础平台,利用电子工具实现的在线商业交换和行政作业活动的全过程,涵盖了用户在公共信息网络和各种相对封闭的企业内部专用网上进行的各种商务活动。在线交易是电子商务的高级阶段和最终目的,它是指买卖双方以计算机网络为平台,进行在线的销售与购买。

电子商务的交易类型:企业与用户的交易 B to C 和企业之间的交易 B to B。

考点精讲十:电子商务系统结构

评注:这类题型主要考查电子商务系统结构。考生应掌握电子商务系统结构及其每个层次的特点,电子商务的系统结构可以分为网络基础平台、安全基础结构、支付体系和业务系统 4 个层次。电子商务安全基础结构层建立在网络基础上之上,包括 CA 安全认证体系和基本安全技术的。

电子商务的体系结构可以分为:网络基础平台、安全结构、支付体系、业务系统。电子商务是以计算机网络为基础的,计算机网络是电子商务的运行平台。电子商务活动分为支付型业务和非支付型业务。电子商务业务包括支付型业务和非支付型业务。支付型业务通常涉及资金的转移。支付型业务建立在支付体系之上,根据业务的需要使用相应的支付体系。而非支付型业务则直接建立在安全

基础结构之上,使用安全基础层提供的各种认证手段和安全技术保证安全的电子商务服务。电子商务的安全要求包括4个方面:数据传输的安全性、数据的完整性、身份安全、交易的不可抵赖性、通过数字签名技术和数字证书技术来实现。

电子商务应用系统:

(1) CA安全认证系统:通过CA安全认证系统发放的证书确认对方的身份是电子商务中最常用的方法之一。

安全是电子商务的命脉。电子商务的安全是通过加密手段来达到的。公用密钥加密技术是电子商务系统中使用的主要加密技术之一。证书按照用户和应用范围可以分为个人证书,企业证书,服务器证书和业务受理点证书等等。

(2) 支付网关系统:位于公共因特网与银行内部网络之间,主要完成通信,协议转换和数据加密解密功能和保护银行内部网络。

(3) 业务应用系统:每一个业务应用系统对应于一个特定的业务应用。支付型的业务应用系统必须配备具有支付服务功能的支付服务器,该服务器通过支付服务软件系统接入因特网,并通过支付网关系统与银行进行信息交换。

(4) 用户及终端系统:人们进行电子商务活动最常用的终端是计算机终端。

一个完整的电子商务系统需要CA安全认证中心,支付网关系统,业务应用系统及用户终端系统的配合与协作。

这其中有数字证书也会经常考核,考生应了解申请证书的目的是什么,数字证书的特征。证书是一个经证书授权中心签名的,它包括证书拥有者的基本信息和公用密钥。证书的作用归纳为两个方面:

① 证书是由CA安全认证中心发放的,具有权威机构的签名,所以它可以用来向系统中的其他实体证明自己的身份。

② 每份证书都携带着证书持有者的公用密钥,所以它可以向接收者证实某个实体对公用密钥的拥有,同时起着分发公用密钥的作用。

证书的有效性可以通过相关的信任签名来验证,证书包括版本、序号、签名算法、颁发者、有效期、主体、主体公钥信息等字段,不携带持有者的基本信息。

历年真题链接

真题12 关于数字证书的描述中,错误的是_____。(2008年4月)

A) 证书通常由CA安全认证中心发放

B) 证书携带持有者的公开密钥

C) 证书通常携带持有者的基本信息

D) 证书的有效性可以通过验证持有者的签名获知

答案:C

解析:证书是由CA安全认证中心发放的,具有权威机构的签名,所以它可以用来向系统中的其他实体证明自己的身份;每份证书都携带着证书持有者的公开密钥,所以可以向接收者证实某个实体对公开密钥的拥有,同时起着分发公开密钥的作用;证书的有效性可以通过相关的信任签名来验证,证书包括版本、序号、签名算法、颁发者、有效期、主体、主体公钥信息等字段,不携带持有者的基本信息。

真题13 电子商务应用系统由CA安全认证、支付网关、业务应用和_____等系统组成。(2008年4月)

答案:用户及终端

解析:电子商务应用系统由CA安全认证系统、支付网关系统、业务应用系统、用户及终端系统组成。电子商务用户包括企业用户、事业用户及个人用户等。用户使用的终端可以为计算机终端、智能终端、傻终端、电话终端等。

真题14 关于数字证书的描述中,正确的是_____。(2008年9月)

A) 包含证书拥有者的公钥信息

B) 包含证书拥有者的账号信息

C) 包含证书拥有者上级单位的公钥信息

D) 包含CA中心的私钥信息

答案:A

解析:数字证书是由CA安全认证中心发放的,具有权威机构的签名,携带证书持有者的公开密钥,用以向接收者证实某个实体对公开密钥的拥有,同时起着分发公开密钥的关系。CA安全认证中心为用户的公钥签发证书,以实现公钥的分发并证明其有效性。CA机构的数字签名使得攻击者不能伪造和篡改证书。

真题15 电子商务应用系统包括CA安全认证系统、_____系统、业务应用系统和用户及终端系统。(2008年9月)

答案:支付网关

解析:电子商务应用系统包括CA安全认证系统、支付网关系统、业务应用系统和用户及终端系统。所有这些子系统都需要连接在因特网上,它们之间相互通信,协同工作,构成完整的电子商务应用系统。

真题16 为了验证WWW服务器的真实性,防止假冒的WWW服务器欺骗,用户可以_____。(2009年9月)

A) 对下载的内容进行病毒扫描

B) 验证要访问的WWW服务器的CA证书

C) 将要访问的WWW服务器放入浏览器的可信站点区域

D) 严禁浏览器运行ActiveX控件

答案:B

解析:CA的英文全称是Certificate Authority,即证书授权中心,是数字证书的发行机构。CA提供的安全技术对网上的数据、信息发送方、接收方进行进行身份确认,以保证各方信息传递的安全性、完整性、可靠性和交易的不可抵赖性。

考点精讲十一:EDI

评注:这类题型主要考查EDI定义,EDI系统特点。电子数据交换EDI是按照协议对具有一定结构特征的标准信息,EDI可以实现两个或多个计算机应用系统之间的通信,其应用系统之间传输的信息要遵循一定的语法规则,EDI应用系统之间数据自动地投递和处理。

EDI系统的三个特点:

(1) EDI是两个或多个计算机应用系统之间的通信。所谓的计算机系统是与EDI通信网络系统相连接的电子数据处理系统EDP。

(2) 计算机之间传输的消息遵循一定

的语法规则与国际标准。

(3) 数据自动地投递和传输处理不需要人工介入,应用程序对它自动响应。总之,计算机通信网是 EDI 应用的基础,计算机系统应用是 EDI 的前提条件,而数据信息标准化是 EDI 的关键。

电子数据处理系统 EDP 是实现 EDI 的基础和必要条件。EDP 主要是企业内部自身业务的自动化。在 EDI 应用系统中,目前使用最多的是通过专门网络服务商提供的 EDI 网络平台,建立用户之间的数据交换关系。

历年真题链接

真题 17　关于 EDI 的描述中,错误的是_____。(2008 年 4 月)

A) EDI 的基础是 EDP

B) EDI 采用浏览器/服务器模式

C) EDI 称为无纸贸易

D) EDI 的数据自动投递和处理

答案:B

解析:电子数据交换 EDI,俗称无纸贸易,是从专用网络发展起来的,目前大部分 EDI 应用系统仍不是基于因特网的,因此一般不采用浏览器/服务器模式。由于 EDI 数据报文采用标准的报文格式,通过计算机数据通信网,数据可自动地投递和传输处理,应用程序自动对它响应,不需要人工介入。电子数据处理 EDP 是 EDI 的基础和必要条件,EDP 主要是企业内部自身业务的自动化,EDI 则是各企业之间交往的自动化,没有 EDP 就没有 EDI 的自动处理。

考点精讲十二:电子支付方式

评注:这类题型主要考查电子支付。考生应了解电子柜员机和电子钱包的概念,掌握电子现金的特点,电子支付的 3 种方式。电子支付就是网上进行买卖双方的金融交换,这种交换通常是由银行等金融机构中介完成的。电子支付工具包括电子现金、电子信用卡和电子支票等。电子商务活动中常涉及资金的转移和流动,其中,服务器端支付软件叫做电子柜员机,用户端支付软件叫做电子钱包。

历年真题链接

真题 18　有一种电子支付工具非常适合小额资金的支付,具有匿名性,无须与银行直接连接便可使用等特点,这种支付工具称为_____。(2008 年 4 月)

A) 电子信用卡　　B) 电子支票

C) 电子现金　　D) 电子柜员机

答案:C

解析:电子支付工具包括电子现金、电子信用卡和电子支票等。电子现金也称数字现金,具有用途广泛、使用灵活、匿名型、快捷简单、无须直接与银行连接便可使用等特点,既可以存储在智能 IC 卡上,也可以以数字形式存储在现金文件中。电子信用卡通过网络直接支付,具有快捷、方便的特点,在使用信用卡进行支付的过程中,也需要认证客户、商家一级信用卡发证机构的身份,防止抵赖行为的发生。

真题 19　关于电子现金的描述中,错误的是_____。(2008 年 9 月)

A) 匿名性

B) 适于小额支付

C) 使用时无须直接与银行连接

D) 依赖使用人的信用信息

答案:D

解析:电子现金也称数字现金,与普通现金一样具有用途广泛、使用灵活、匿名型、快捷简单、无须直接与银行连接便可使用等特点,既可以存储在智能 IC 卡上,也可以以数字形式存储在现金文件中。

考点精讲十三:安全电子交易

评注:这类题型主要考查安全电子交易。考生要知道什么是 SET 协议,题目一般是给出 SET 协议的相关描述,找出错误的或正确的选项。安全电子交易(SET)是由 VISA 和 MASTCARD 所开发的开放式支付规范,使用的安全技术协议是 SET 协议,SET 协议使用数据信封技术、数字签名技术、信息摘要技术,以及双重签名技术,SET 认证双方身份通过第三方 CA 安全认证中心,SET 协议涉及的证书包括持卡人证书、商家证书、支付网关证书、银行证书等。

历年真题链接

真题 20　SET 协议是针对以下哪种支付方式的网上交易而设计的?_____。(2008 年 9 月)

A) 支票支付　　B) 卡支付

C) 现金支付　　D) 手机支付

答案:B

解析:安全电子交易 SET 是由 VISA 和 MASTCARD 所开发的开放式支付规范,使为了保证信用卡在公共因特网网络上支付的安全而设立的。

考点精讲十四:站点内容和页面的策划与推广

评注:这类题型主要考查 Web 站点。考生只需记住利用 IIS 建立的 Web 站点的 4 级访问控制。限制用户访问站点资源的 4 种方法是 IP 地址限制、用户验证、Web 权限、NTFS 权限。

历年真题链接

真题 21　Web 站点可以限制用户访问 Web 服务器提供的资源,访问控制一般分为四个级别:硬盘分区权限、用户验证、Web 权限和_____限制。(2008 年 9 月)

答案: IP 地址

解析:Web 站点访问控制一般分为四个级别:IP 地址限制、用户验证、Web 权限和硬盘分区权限。其中,IP 地址限制是指:Web 服务器审核所访问的用户计算机的 IP 地址,以决定该用户能否访问 Web 站点的资源。

考点精讲十五:电子政务的基本概念

评注:这类题型主要考查电子政务的基本概念。题目主要考到电子政务的 3 种应用模式,电子政务的 3 个发展阶段及阶段特征。

电子政务建设中,网络是基础,安全是关键,应用是目的。电子政务的应用模式主要包括 3 种,它们是政府与政府间(G to G)应用模式、政府与企业间(G to B)的应用模式和政府与公民间(G to C)的应用模式。根据利用信息技术的目的和信息技术的处理能力来划分,电子政务的发展大致经历了面向数据处理、面向信息处理和面向知识处理 3 个阶段。

历年真题链接

真题 22　在电子政务发展过程中,有

一个阶段以政府内部的办公自动化和管理信息系统的建设为主要内容,这个阶段称为_____。(2008年4月)

A) 面向数据处理阶段

B) 面向信息处理阶段

C) 面向网络处理阶段

D) 面向知识处理阶段

答案:A

解析:电子政务的发展大致经历面向数据处理、面向信息处理和面向知识处理三个阶段,面向数据处理的电子政务主要集中在1995年以前,以政府办公网的办公自动化和管理系统的建设为主要特征。面向信息处理的电子政务一直延续到2001年,这一阶段以网络为中心建立通信基础平台,并以结构化数据的信息留为主要的存储和处理对象。面向知识处理阶段的主要目标是在政府信息支撑环境的基础上,利用知识管理技术提供政府的决策能力,建立基于网络的分布式政府结构。

真题23 电子政务的发展历程包括面向数据处理、面向信息处理和面向_____处理阶段。(2008年9月)

答案:知识

解析:根据利用信息技术的目的和信息处理技术的处理能力来划分,电子政务的发展大致经历了面向数据处理、面向信息处理和面向知识处理3个阶段。

考点精讲十六:电子政务的系统结构

评注:这类题型主要考查电子政务的系统结构。考生需牢记统一的安全电子政务平台包括哪3个统一的平台,电子政务的逻辑结构,网络基础设施有哪些,什么叫政府内网。

电子政务的逻辑结构自下而上分为3个层次:基础设施层、统一的安全电子政务平台层、电子政务应用层。其中基础设施层包括两个子层,即网络基础设施子网和信息安全基础设施子层,网络基础设施是为电子政务系统提供政务信息以及其他运行管理信息的传输和交换平台,它是整个电子政务系统的基础,位于整个分层体系结构的最底层。统一的安全电子政务平台包括统一的可信Web服务平台,统一的Web门户平台与统一的数据交换平台。

电子政务的网络基础设施主要包括因特网、公众服务业务网、非涉密政府办公网和涉密政府办公网几大部分。其中,公众服务业务网、非涉密政府办公网和涉密政府办公网3部分又称为政府内网。

历年真题链接

真题24 电子政务的公众服务业务网、非涉密政府办公网和涉密政府办公网称为_____。(2008年4月)

答案:政务内网

解析:电子政务的网络基础设施包括因特网、公众服务业务网、非涉密政府办公网和涉密政府办公网几大部分。其中公众服务业务网、非涉密政府办公网和涉密政府办公网又称为政务内网。所有的网络系统以统一的安全电子政务平台为核心,共同组成一个有机的整体。

真题25 可信时间戳服务位于电子政务分层逻辑模型中的_____。(2008年4月)

A) 网络基础设施子层

B) 信息安全基础设施子层

C) 统一的安全电子政务平台层

D) 电子政务应用层

答案:B

解析:电子政务分层逻辑模型包括基础设施层、统一的安全电子政务平台、电子政务应用平台。其中,基础设施层又包括网络基础设施子层和信息安全基础设施子层。信息安全基础设施子层以公钥基础设施(PKI)、授权管理基础设施(PMI)、可信时间戳服务系统和安全保密管理系统等为重点。

真题26 电子政务逻辑结构的三个层次是电子政务应用层、统一的安全电子政务平台层和_____。(2008年9月)

A) 接入层　　B) 汇聚层

C) 网络设施层　　D) 支付体系层

答案:C

解析:电子政务的逻辑结构自上而下分为三个层次:电子政务应用层、统一的安全电子政务平台层和网络设施层。

真题27 电子政务内网包括公众服务业务网、非涉密政府办公网和_____。(2008年9月)

A) 因特网

B) 内部网

C) 专用网

D) 涉密政府办公网

答案:D

解析:电子政务的网络基础设施主要包括因特网、公众服务业务网、非涉密政府办公网和涉密政府办公网,其中后三者又称政务内网。所有的网络系统以统一的安全电子政务平台为核心,共同组成一个有机的整体。

考点精讲十七:一站式电子政务应用系统

评注:这类题型主要考查一站式电子政务应用系统。考生应记住一站式电子政务应用的概念,一站式电子政务应用系统的实现流程的3个阶段。所谓"一站式"服务,简单来讲就是服务的提供者针对特定的用户群,通过网络提供一个有统一入口的服务平台,用户通过访问统一的门户即可得到全程服务。"一站式"电子政务应用系统的实现流程:身份认证、服务请求、服务调度及处理。

考点精讲十八:数字版权管理

评注:数字版权管理(Digital Rights Management,DRM)指的是出版者用来控制被保护对象的使用权的一些技术,这些技术保护的有数字化内容(例如:软件、音乐、电影)以及硬件,处理数字化产品的某个实例的使用限制。本术语容易和版权保护混淆。

数字版权管理可以防止视频内容的非法使用,主要采用数据加密、版权保护、数字水印和签名技术。数字水印技术是把代表著作人身份的特定信息、发行商的信息和使用条款等嵌入到数据中,它能给作品打上印记,防止非法传播。版权保护指的是应用在电子设备上的数字化媒体内容上的技术,版权保护技术使用以后可以控制和限制这些数字化媒体内容的使用权。

历年真题链接

真题28 数字版权管理主要采用数据加密、版权保护、数字签名和_____。(2009年3月)

A) 认证技术　　B) 数字水印技术

C) 访问控制技术　　D) 防篡改技术

答案：B

解析：数字版权管理可以防止视频内容的非法使用，主要采用数据加密、版权保护、数字水印和签名技术。数字水印技术是把代表著作人身份的特定信息、发行商的信息和使用条款等嵌入到数据中，它能给作品打上印记，防止非法传播。

真题 29　数字版权管理主要采用数据加密、版权保护、认证和_____。（2009 年 9 月）

A）防病毒技术　B）数字水印技术

C）访问控制技术　D）放篡改技术

答案：B

解析：数字版权管理，保护电影音乐不会被盗版，又称为 DRM，英文全称 Digital Rights Management 一般翻译为数字版权保护或数字版权管理。数字版权管理主要采用数据加密、版权保护、认证和数字水印技术。

考点精讲十九：信息安全技术概述

评注：这类题型主要考查信息安全的基本要求，信息安全的组成及系统设计原则。考生应记住信息安全主要包括这几个方面，信息系统安全管理需要遵守的原则，网络信息安全包括哪几个方面及信息安全的原则。

信息安全包括 5 个基本要素：机密性、完整性、可用性、可控性与可审查性，信息安全包括 3 个方面：物理安全、安全控制、安全服务。物理安全是指在物理媒介层次上对存储和传输的信息的安全保护。安全控制是指在操作系统和网络通信设备上对存储和传输信息的操作和进程进行控制和管理，主要是在信息处理层次上对信息进行初步的安全保护。安全服务是指在应用层对信息的保密性；完整性和来源真实性进行保护和鉴别，满足用户的安全需求，防止和抵御各种安全威胁和攻击。

网络信息系统的安全管理主要基于三个原则：多人负责原则、任期有限原则和职责分离原则。网络安全的目标是确保网络系统的信息安全，即保证信息的存储安全和信息的传输安全。

历年真题链接

真题 30　下面哪个不是网络信息系统安全管理需要遵守的原则？_____。（2008 年 9 月）

A）多人负责制

B）任期有限制

C）多级多目标管理原则

D）职责分离原则

答案：C

解析：网络信息系统的安全管理主要基于三个原则：多人负责原则、任期有限原则和职责分离原则。

真题 31　对网络系统而言，信息安全主要包括两个方面：存储安全和_____安全。（2009 年 9 月）

答案：传输

解析：确保网络系统的信息安全是网络安全的目标，信息安全包括两个方面：信息的存储安全和信息的传输安全。信息的存储安全是指信息在静态存放状态下的安全，如是否会被非授权调用等。信息的传输安全是指信息在动态传输过程中安全。

考点精讲二十：密钥管理

评注：这类题型主要考查密钥的生存周期，保密密钥的分发和公钥的分发。所有的密钥都有生存周期，密钥的生存周期是指授权使用该密钥的周期。

密码分析的目的就是千方百计地寻找密钥或明文。密钥分发技术是指将密钥发送到数据交换的双方，而其他人无法看到的方法。公钥是公开的，分发公钥不需要保密，目前主要采用数字证书来分发公钥，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。

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，它通常用于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。

历年真题链接

真题 32　在认证过程中，如果明文由 A 发送到 B，那么对明文进行签名的密钥是_____。（2008 年 4 月）

A）A 的公钥　B）A 的私钥

C）B 的公钥　D）B 的私钥

答案：B

解析：在认证过程中，发送者使用自己的私钥加密，接受者使用发送者的公钥解密。

真题 33　密钥分发技术主要有 CA 技术和_____技术。（2008 年 9 月）

答案：KDC

解析：通常使用的密钥分法技术有两种：KDC 技术和 CA 技术。KDC（密钥分发中心）技术可用于保密密钥的分发，CA（证书权威机构）技术可用于公钥和保密密钥的分发。

真题 34　进行唯密文攻击时，密码分析者已知的信息包括：要解密的密文和_____。（2009 年 9 月）

答案：密钥

解析：进行唯密文攻击时密码分析者有一些消息的密文，这些消息都用同一加密算法加密。密码分析者的任务是恢复尽可能多的明文，或者最好是能推算出加密消息的密钥来，以便可采用相同的密钥解出其他被加密的消息。

考点精讲二十一：对称加密技术

评注：这类题型主要考查对称加密技术。随着互联网的普及，网络安全技术越来越重要，考生要知道常用的几种对称加密算法，公钥体制的安全基础主要是数学中的难解问题，流行的两大类是什么。

对称加密采用了对称密码编码技术，它的特点是文件加密和解密使用相同的密钥，即加密密钥也可以用作解密密钥，这种方法在密码学中叫做对称加密算法，对称加密算法使用起来简单快捷，密钥较短，且破译困难。对称密码体制又称为常规密钥密码体制、单密钥密码体制、秘密密钥密码体制。

除了数据加密标准（DES），另一个对称密钥加密系统是国际数据加密算法（IDEA），它比 DES 的加密性好，而且对计算机功能要求也没有那么高。IDEA 加密标准由 PGP（Pretty Good Privacy）系统使用。数据加密技术可分为 3 类：对称型加密、不对称型加密和不可逆加密。对称加密有 DES 算法，对称密码体制的加密密钥和解密密钥是相同的，对称密码体制中算法不必是秘密的，而只需要对密钥进行保密即可。DES 是一种常用的对称加密

算法,一般的密钥长度为56位。对称加密又称为公开密钥加密,其密钥是公开的。

历年真题链接

真题35 凯撒密码是一种置换密码,对其破译的最多尝试次数是_____。(2008年4月)

A) 2次　　B) 13次

C) 25次　　D) 26次

答案:C

解析:凯撒密码是一种最古老的置换密码,这种密码算法对于明文中的每一个字母都用该字母后的第n个字母来替换,其中n就是密钥。由于凯撒密码的整个密码空间只有26个密钥,只要知道加密算法采用的是凯撒密码,破译者最多只需尝试25次就可以知道正确的密码。

真题36 关于RC5加密算法的描述中,正确的是_____。(2008年4月)

A) 分组长度固定

B) 密钥长度固定

C) 分组和密钥长度都固定

D) 分组和密钥长度都可变

答案:D

解析:RC5的分组和密钥长度都是可变的,可以在速度和安全性之间进行折中。

真题37 对称加密技术的安全性取决于_____。(2008年9月)

A) 密文的保密性

B) 解密算法的保密性

C) 密钥的保密性

D) 加密算法的保密性

答案:C

解析:对称机密技术中,通信双方对信息的加密和解密都使用相同的密钥,因此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。也可以讲对称加密技术的安全性取决于密钥的保密性,而不是算法的保密性。即使知道了密文和加密及解密的知识,解密消息也是不可能的。

真题38 下面哪种破译类型的破译难度最大?_____。(2008年9月)

A) 仅密文　　B) 已知明文

C) 选择明文　　D) 选择密文

答案:A

解析:加密消息的破译类型包括仅密文、已知明文、选择明文、选择密文、选择文本等。对于仅密文破译类型,密码分析人员仅拥有密文和加密算法,可用信息量很少,破译难度最大。

真题39 AES加密算法处理的分组长度是_____。(2009年3月)

A) 56位　　B) 64位

C) 128位　　D) 256位

答案:C

解析:高级加密标准AES的密钥长度为128、192或256位,分组长度为128位。

真题40 RC5加密算法没有采用的基本操作是_____。(2009年3月)

A) 异或　　B) 循环

C) 置换　　D) 加

答案:C

解析:RC5加密算法是一种对称加密算法,在该算法中使用了3种运算:异或、加和循环。

真题41 在DES加密算法中,不使用的基本运算是_____。(2009年9月)

A) 逻辑与　　B) 异或

C) 置换　　D) 移位

答案:A

解析:DES算法为密码体制中的对称密码体制,又被成为美国数据加密标准,是1972年美国IBM公司研制的对称密码体制加密算法。其密钥长度为56位,明文按64位进行分组,将分组后的明文组和56位的密钥按位替代或交换的方法形成密文组的加密方法。DES工作的基本原理是,其入口参数有三个:key、data、mode。key为加密解密使用的密钥,data为加密解密的数据,mode为其工作模式。在DES加密算法中,不使用的基本运算是逻辑与。

考点精讲二十二:公钥加密技术

评注:这类题型主要考查公钥密码体制的模型及常用的公钥体制。考生应知道公钥密码体制中用于加密的密钥,不公开的是哪个,公开的是哪个,常用的公钥体制有哪些,各自特点是什么。

公开密钥加密又称为不对称对称,方案包括6个组成部分:明文、加密算法、公共的密钥、私有的密钥、密文和解密算法。公开密钥的体制主要有两种公钥管理模式,一种是采用证书的方式,另一个是PGP采用的分布式密钥管理模式。

目前常用的公钥体制有:RSA公钥体制和El Gamal公钥体制。RSA体制被认为是现在理论上最为成熟完善的一种公钥密钥体制,RSA公钥体制的构造是基于Euler定理,经常用于数字签名、密钥管理和认证等方面。El Gamal公钥体制在原理上是基于离散对数的,即使加密相同的明文,得到的密文也是不同的,因此成为概率加密体制。

历年真题链接

真题42 公钥体制RSA是基于_____。(2008年4月)

A) 背包算法

B) 离散对数

C) 椭圆曲线算法

D) 大整数因子分解

答案:D

解析:RSA是迄今为止理论上最为成熟完善的一种公钥密码体制。该体制的构造基于Euler定理,它利用了如下的基本事实:寻找大素数相对容易,而分解两个大素数的积在计算上是不可行的。RSA算法的安全性就是建立在难以对大素数提取因子的基础上。

真题43 关于RSA密码体制特点的描述中,错误的是_____。(2008年9月)

A) 基于大整数因子分解问题

B) 是一种公钥密码体制

C) 加密速度很快

D) 常用与数字签名和认证

答案:C

解析:RSA体制被认为是迄今为止理论上最成熟完善的一种公钥密码体制。RSA算法的安全性建立在难以对大数提取因子的基础上。RSA的缺点是加密、解密速度太慢,因此很少用于数据加密,而多用于数字签名、密钥管理和认证等方面。

真题44 关于RSA密码体制的描述中,正确的是_____。(2009年3月)

A) 安全性基于椭圆曲线问题

B) 是一种对称密码体制

C) 加密速度很快

D) 常用于数字签名

答案：D

解析：RSA是一个公开密钥密码体制（非对称加密），该体制的构造基于Euler定理，算法的安全性建立在难以对大数提取因子的基础上。RSA加密、解密速度慢，很少用于数据加密，多用于数字签名、密钥管理和认证等方面。

真题45　用RSA算法加密时，已知公钥是（e=7，n=20），私钥是（d=30，n=20），用公钥对消息M=3加密，得到的密文是_____。（2009年3月）

A）19　　B）13

C）12　　D）7

答案：D

解析：密文为 $M^e \bmod n = 3^7 \bmod 20 = 2187 \bmod 20 = 7$。

真题46　下面不属于公钥加密算法的是_____。（2009年9月）

A）RSA　　B）AES

C）EIGamal　　D）背包加密算法

答案：B

解析：AES是对称加密算法，其他的属于公钥加密算法。

考点精讲二十三：分组密码的特点

评注：这类题型主要考查分组密码的特点。考生要分清可逆加密和不可逆加密的算法各有哪些，了解分组密码的优缺点。

分组密码的加密方式首先将明文序列以固定长度进行分组，每一组明文用相同的密钥和加密函数进行运算，分组密码算法实际上就是密钥控制下，通过某个置换来实现对明文分组的加密变换。为了保证密码算法的安全强度，对密码算法的要求如下。

（1）分组长度足够大。当分组长度较小时，分组密码类似于古典的代替密码，它仍然保留了明文的统计信息，这种统计信息将给攻击者留下可乘之机，攻击者可以有效地穷举明文空间，得到密码变换本身。

（2）密钥量足够大。分组密码的密钥所确定密码变换只是所有置换中极小一部分。如果这一部分足够小，攻击者可以有效地穷举明文空间确定所有的置换。这时，攻击者就可以对密文进行解密，以得到有意义的明文。

（3）密码变换足够复杂。使攻击者除了穷举法以外，找不到其他快捷的破译方法。

其优点是明文信息良好的扩散性；对插入的敏感性；不需要密钥同步；较强的适用性，适合作为加密标准。不可逆加密有MD5算法和SHA算法。分组密码的缺点是：加密速度慢，错误扩散和传播。

历年真题链接

真题47　Blowfish加密算法处理的分组长度是_____。（2009年9月）

A）56位　　B）64位

C）128位　　D）256位

答案：B

解析：BlowFish算法用来加密64 bit长度的字符串。BlowFish算法使用两个“盒”：ungigned long pbox[18]和unsigned long sbox[4,256]。BlowFish算法中，有一个核心加密函数：BF_En（后文详细介绍）。该函数输入64位信息，运算后，以64位密文的形式输出。用BlowFish算法加密信息，需要两个过程：（1）密钥预处理；（2）信息加密。

考点精讲二十四：认证技术

评注：这类题型主要考查认证技术中的消息认证。考生应熟记常用的认证方式及最常用的认证方式，了解认证技术的基本概念，常用的摘要算法，消息认证技术的特点、身份认证的分类和协议。

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。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。

1. 消息认证

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）消息内容是否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）。MD5是一种常用的摘要算法，它产生的消息摘要长度是128位。

2. 身份认证

身份认证大致可分为3类：一是个人知道的某种事物，如口令、账号、个人识别码等；二是个人持证，如图章、标志、钥匙、护照磁卡和智能卡等；三是个人特征，如指纹、声纹、手形、视网膜、血型、基因、笔迹和习惯性签字等。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。身份认证的两种方法：（1）本地控制；（2）可信任的第三方提供确认。主要考查常用身份认证协议（S/Key口令协议、令牌口令协议、PPP认证协议）。考生应了解几种常用的身份认证协议，重点掌握S/Key口令协议。

S/Key口令是一种一次性口令生成方案，它可以对付重放攻击。S/Key协议运行于客户机/服务器环境中。客户机发送初始化包启动S/Key协议，服务器以明文形式发送一个启动值给客户机。

PPP认证协议是最常用的建立电话线或ISDN拨号连接的协议，PPP可使用口令认证协议、挑战握手协议和可扩张协议这三种标准认证机制中的任何一种。

Kerberos协议是一种对称密码网络认证协议，广泛使用于校园网环境。考生应知道Kerberos协议的加密算法。Kerberos基于对称密钥体制，一般采用DES，但也可以采用其他算法。在Kerberos模型中，有一个存有所有用户秘密密钥的数据库，对于每个用户来讲，秘密密钥是一个加密口令。Kerberos还能提供会话密钥，该密钥用来加密双方间的通信信息，通信完毕，即销毁会话密钥。

3. 数字签名

对于认证技术中的数字签名。考生应了解什么是数字签名，有什么特点，有什么作用。数字签名是指以用户私钥作

为加密密钥,以公钥为解密密钥,实现由一个用户加密的信息能够被多个用户解读,且发送方无法否认自己所发送的信息。数字签名是用于确认发送者身份和消息完整性的一个加密的消息摘要,是0和1的数字串。数字签名主要的功能是:保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。数字签名可以利用公钥密码、对称密码体制或公证系统来实现。数字签名没有提供消息内容的机密性。因为许多时候证明消息的来源要比隐藏消息的内容更加重要,可能需要消息的认证和完整性,而不需要保密性。

历年真题链接

真题48 关于数字签名的描述中,错误的是_____。(2008年4月)

A) 可以利用公钥密码体制

B) 可以利用对称密码体制

C) 可以保证信息内容的机密性

D) 可以进行验证

答案:C

解析:数字签名可以利用公钥密码、对称密码体制或公证系统来实现。数字签名没有提供消息内容的机密性。因为许多时候证明消息的来源要比隐藏消息的内容更加重要,可能需要消息的认证和完整性,而不需要保密性。

真题49 Kerberos是一种常用的身份认证协议,它采用的加密算法是_____。(2008年9月)

A) El Gamal　　B) DES

C) MDS　　D) RSA

答案:B

解析:Kerberos是一种对称密码认证协议,采用DES加密算法进行加密和认证,广泛用于校园网环境。

真题50 SHA是一种常用的摘要算法,它产生的消息摘要长度是_____。(2008年9月)

A) 64位　　B) 128位

C) 160位　　D) 256位

答案:C

解析:SHA是当今安全产品中最常用的散列函数之一,它是建立在MD4的基础之上,按512 bit/s块处理其输入,并产生一个160位的消息摘要,要消耗更多的处理器时间,运行慢一些。

真题51 数字签名是用于确认发送者身份和消息完整性的一个加密消息_____。(2008年9月)

答案:摘要

解析:数字签名是用于确认发送者身份和消息完整性的一个加密的消息摘要。数字签名与手写签名类似,只不过数字签名是0和1的数字串,因消息而异。

真题52 关于消息认证的描述中,错误的是_____。(2009年3月)

A) 消息认证称为完整性校验

B) 用于识别信息源的真伪

C) 消息认证都是实时的

D) 消息认证可通过认证码实现

答案:C

解析:消息认证又称完整性校验,使接收者能够识别信息源、信息内容的真伪、时间性和意定的信宿。但认证不一定是实时的,如电子邮件系统。消息的完整性认证有两条基本途径:消息认证码和篡改检测码。

真题53 关于Kerberos认证系统的描述中,错误的是_____。(2009年3月)

A) 有一个包含所有用户密钥的数据库

B) 用户密钥是一个加密口令

C) 加密算法必须使用DES

D) Kerberos提供会话密钥

答案:C

解析:Kerberos基于对称密钥体制,一般采用DES,但也可以采用其他算法。在Kerberos模型中,有一个存有所有用户秘密密钥的数据库,对于每个用户来讲,秘密密钥是一个加密口令。Kerberos还能提供会话密钥,该密钥用来加密双方间的通信信息,通信完毕,即销毁会话密钥。

真题54 数字签名是笔迹签名的模拟,用于确认发送者身份,是一个_____的消息摘要。(2009年3月)

答案:加密

解析:利用公钥密码体制,数字签名是一个加密的消息摘要,附加在消息的后面。

真题55 关于数字签名的描述中,错误的是_____。(2009年9月)

A) 通常能证实签名的时间

B) 通常能对内容进行鉴别

C) 必须采用DSS标准

D) 必须能被第三方验证

答案:C

解析:数字签名的简单实例是直接利用RSA算法和发送方的秘密密钥,对被签名的数据进行加密,当接收方收取本块密文时,使用发送方的公开密钥进行解密,如果能够还原明文,则根据公开密钥体制的特点(公开密钥加密的密文只能用秘密密钥解密,秘密密钥加密的密文只能用公开密钥解密),可以认为该数据确实来自于希望的发送方,通常能证实签名的时间以及对内容进行鉴别,必须能被第三方验证。

考点精讲二十五:Web安全

评注:这类题型主要考查IPSec提供的服务。考生重点掌握IPSec提供的服务,安全套接层SSL技术。

所有信息要想交换,必须在网络上进行传输,那么传输的过程就是Web安全至关重要的一个环节。Web浏览器和Web服务器之间的信息交换也是通过数据包的网络传输来实现的,所以,Web数据传输过程的安全性直接影响着Web的安全。加强Web通信安全的方案有SSL、IPSec等。

IPSec可以提供访问控制、无连接完整性、数据源鉴别、载荷机密性和有限流量机密等安全服务,弥补由于TCP/IP协议体系自身带来的安全漏洞。IPSec不是一种协议而是由IKE(Internet Key Exchange,互联网密钥交换)、AH(Authentication Header,鉴定包头)和ESP(Encapsulation Security Payload,负载安全封装)等组件组成。

SSL(Security Socket Layer)的中文全称是"加密套接字协议层",是由Netscape公司推出的一种安全通信协议,它位于HTTP协议层和TCP协议层之间,能够对信用卡和个人信息提供较强的保护。SSL在客户和服务器之间建立一条加密通道,确保所传输的数据不被非法窃取,SSL安全加密机制功能是依靠使用数字证书来实现的。

历年真题链接

真题56 为了防止第三方偷看或篡改用户与Web服务器交互的信息,可以采

用_____。(2008年4月)

A) 在客户端加载数字证书

B) 将服务器的IP地址放入可信站点区

C) SSL技术

D) 将服务器的IP地址放入受限站点区

答案：C

解析：在使用因特网进行电子商务活动中，通常可以使用安全通道访问Web站点，以避免第三方偷看或篡改。而安全通道使用安全套接层SSL技术。

真题57　为了避免第三方偷看WWW浏览器与服务器交互的敏感信息，通常需要_____。(2008年9月)

A) 采用SSL技术

B) 在浏览器中加载数字证书

C) 采用数字签名技术

D) 将服务器放入可信站点区

答案：A

解析：在使用因特网进行电子商务活动中，通常可以使用安全通道访问Web站点，以避免第三方偷看或篡改。而安全通道使用安全套接层SSL技术。

真题58　关于安全套接层协议的描述中，错误的是_____。(2008年9月)

A) 可保护传输层的安全

B) 可提供数据加密服务

C) 可提供消息完整性服务

D) 可提供数据源认证服务

答案：D

解析：安全套接层SSL是Netscape设计的一种用户保护传输层安全的开放协议，它在应用层协议和低层的TCP/IP之间提供数据安全，为TCP/IP连接提供数据加密、服务器认证、消息完整性和可选的客户机认证。IPSec协议提供数据源认证服务。

真题59　关于IPSec的描述中，错误的是_____。(2009年9月)

A) Kerberos是为Novell网络设计的

B) 用户须拥有数字证书

C) 加密算法使用RSA

D) Kerberos提供会话密钥

答案：D

解析："Internet协议安全性(IPSec)"是一种开放标准的框架结构，通过使用加密的安全服务以确保在Internet协议(IP)网络上进行保密而安全的通信。IPSec协议不是一个单独的协议，它给出了应用于IP层上网络数据安全的一整套体系结构，包括网络认证协议、封装安全载荷协议、密钥管理协议和用于网络认证及加密的一些算法等，但是Kerberos并没有提供会话密钥。

真题60　关于IPSec的描述中，错误的是_____。(2009年9月)

A) 主要协议是AH协议与ESP协议

B) AH协议保证数据完整性

C) 只使用TCP作为传输层协议

D) 将互联成改造为有逻辑连接的层

答案：C

解析："Internet协议安全性(IPSec)"是一种开放标准的框架结构，通过使用加密的安全服务以确保在Internet协议(IP)网络上进行保密而安全的通信。IPSec协议不是一个单独的协议，它给出了应用于IP层上网络数据安全的一整套体系结构，包括网络认证协议、封装安全载荷协议、密钥管理协议和用于网络认证及加密的一些算法等。ESP报头的位置在IP报头之后，TCP、UDP，或者ICMP等传输层协议报头之前，所以C不对。

考点精讲二十六：组播路由技术

评注：这类题型主要考查组播协议和组播路由。考生需知道组播路由协议分为哪两种，密集组播路由协议有哪些。

组播是一种数据包传输方式，当有多台主机同时成为一个数据包的接收者时，出于对带宽和CPU负担的考虑，组播成了一种最佳选择。组播路由协议分为域内组播路由协议和域间组播路由协议两类。域内组播路由协议包括PIM－SM(Protocol Independent Multicast-Sparse Mode)、PIM-DM(Protocol Independent Multicast-Dense Mode)、DVMRP(Distance Vector Multicast Routing Protocol)等协议，域间组播路由协议包括MBGP(Multiprotocol BGP)、MSDP(Multicast Source Discovery Protocol)等协议。

同时为了有效抑制组播数据在链路层的扩散，引入了IGMP Snooping、CGMP等二层组播协议。IGMP建立并且维护路由器直联网段的成员关系信息。域内组播路由协议根据IGMP维护的这些组播成员关系信息，运用一定的组播路由算法构造组播分发树进行组播数据包转发。域间组播路由协议在各自治域间发布具有组播能力的路由信息以及组播源信息，以使组播数据在域间进行转发。

历年真题链接

真题61　下面哪个不是密集组播路由协议？_____。(2009年9月)

A) DVMRP　　B) MOSPF

C) PIM-DM　　D) CBT

答案：D

解析：PIM由IDMR(域间组播路由)工作组设计，PIM不依赖于某一特定单播路由协议，PIM定义了两种模式：密集模式(Dense-Mode)和稀疏模式(Sparse-Mode)，PIM-D与DVMRP很相似，都属于密集模式协议，密集模式——DVMRP、MOSPF、PIM-DM。

考点精讲二十七：P2P网络拓扑

评注：这类题型主要考查P2P网络，考生需要注意P2P网络的4种结构及结构代表。

分布式非结构化P2P网络的代表有Gnutella、Shareaza、Lime Wire和Bear-Share。Maze属于集中式拓扑结构的P2P网络。P2P网络存在四种主要的结构类型，即以Napster为代表的集中目录式结构，分布式非结构化P2P网络结构，分布式结构化P2P网络和混合式P2P网络结构。

历年真题链接

真题62　以下P2P应用软件中不属于文件共享类应用的是_____。(2009年3月)

A) Skype　　B) Gnutella

C) Napster　　D) BitTorrent

答案：A

解析：P2P应用可以分为多类。Skepe、MSN、QQ等都属于即时通信软件，典型的文件共享软件包括Napster、Gnutella和BitTorrent。

真题63　下面哪种P2P网络拓扑不是分布式非结构化的_____。(2009年3月)