

图书基本信息

书名：<<网络工程师考试考点分析与例题精解>>

13位ISBN编号：9787560620336

10位ISBN编号：7560620337

出版时间：2008-8

出版时间：张友生、唐平 西安电子科技大学出版社 (2008-08出版)

作者：唐平，张友生 编

页数：484

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## 前言

计算机技术与软件专业技术资格（水平）考试（以下简称计算机软件资格考试）是国家人力资源和社会保障部、工业和信息化部对全国计算机与软件专业技术人员进行的职业资格和专业技术资格认定（国人部发（2003）39号文件）。

参加这种考试并取得相应级别的资格证书，是各用人单位聘任计算机技术与软件专业工程师系列职务的前提。

计算机软件资格考试与会计、经济师、税务师、律师、建筑师等资格考试一样，属于国家专业技术资格考试，并被纳入了全国专业技术人员职业资格证书制度的统一规划。

计算机软件资格考试在全国范围内已经实施了十多年，累计参加考试的人数超过200万人次。

该考试由于其权威性和严肃性，得到了社会各界的广泛认同，被称为中国专业技术职务任职资格和考试的第一品牌。

我国软件考试已与部分国家签定了相互认证的备忘录，正逐步走向世界。

本书紧扣考试大纲，采用表格统计法、饼状图分析法、走势图分析法，科学地研究每个知识点的命题情况，准确把握每个出题点的深浅；同时基于每个章节知识点分布统计分析的结果，科学地编写了相应的同步训练试题；全真模拟试题紧扣大纲，结构科学，重点突出，针对性强。

## 内容概要

《网络工程师考试考点分析与例题精解》由希赛IT教育研发中心组织编写，紧扣全国计算机技术与软件专业技术资格（水平）考试——网络工程师考试大纲，通过对历年试题进行科学分析、研究、总结、提炼后编写而成。

《网络工程师考试考点分析与例题精解》的主要内容包括应试指南、考点分析与同步训练、全真模拟试题及解析。

基于历年试题，利用统计分析的方法，科学地得出结论并预测以后的出题动向，是《网络工程师考试考点分析与例题精解》的一大特色。

《网络工程师考试考点分析与例题精解》力求保证既不漏掉考试必需的知识点，又不加重考生的备考负担，使考生轻松、愉快地掌握知识点并领悟网络工程师考试的真谛。

《网络工程师考试考点分析与例题精解》可作为参加全国计算机技术与软件专业技术资格（水平）考试——网络工程师考试的复习用书，也可作为网络工程技术人员的参考用书。

## 书籍目录

第1章网络工程师应试指南1.1考试简介1.2上午试题模块的知识架构与答题技巧1.3下午模块题型与答题技巧第2章计算机硬件知识2.1计算机体系结构2.2存储系统2.3输入 / 输出系统2.4其他知识点2.5本章小结2.6同步训练第3章操作系统基础3.1操作系统的基本概念3.2处理机管理3.3存储管理3.4设备管理3.5文件管理与作业管理3.6本章小结3.7同步训练第4章系统开发、运行与性能评价4.1软件工程与项目管理基础4.2需求分析与设计4.3软件测试与管理4.4系统运行、维护与配置管理4.5本章小结4.6同步训练第5章标准化与知识产权知识5.1标准化知识5.2知识产权基础5.3本章小结5.4同步训练第6章网络体系结构6.1体系结构基础知识6.2OSI参考模型6.3OSI协议集6.4本章小结6.5同步训练第7章数据编码与传输7.1数据通信基础7.2数据调制与编码7.3数据传输与交换技术7.4本章小结7.5同步训练第8章局域网与城域网技术8.1局域网技术8.2城域网技术8.3本章小结8.4同步训练第9章广域网与接入网技术9.1广域网技术9.2接入网技术9.3本章小结9.4同步训练第10章网络互联与因特网应用10.1网络互联基础10.2TCP / IP协议族10.3因特网应用10.4信息化与信息系统10.5本章小结10.6同步训练第11章网络服务器配置技术11.1Windows服务配置11.2Linux服务配置11.3本章小结11.4同步训练第12章网络设备配置技术12.1交换机的配置12.2路由器的配置12.3广域网接入的配置12.4防火墙的配置12.5本章小结12.6同步训练第13章系统及网络安全基础13.1信息安全基础13.2加解密技术13.3常用网络安全技术13.4本章小结13.5同步训练第14章网络管理、维护与评价14.1网络管理基础14.2网络操作系统管理14.3网络管理工具与命令14.4网络运行维护与评价14.5本章小结14.6同步训练第15章全真模拟试题全国计算机技术与软件专业技术资格（水平）考试《网络工程师模拟试题》上午试卷全国计算机技术与软件专业技术资格（水平）考试《网络工程师模拟试题》下午试卷上午试题答案及解析下午试题答案

## 章节摘录

13.3.1【考点】数字签名与数字证书简单地说,所谓数字签名,就是附加在数据单元上的一些数据,或是对数据单元所做的密码变换。

这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性并保护数据,防止被人(例如接收者)进行伪造。

数字签名是对电子形式的消息进行签名的一种方法,一个签名消息能在一个通信网络中传输。

基于公钥密码体制和私钥密码体制都可以获得数字签名,目前主要是基于公钥密码体制的数字签名。

数字签名包括普通数字签名和特殊数字签名。

普通数字签名算法有RSA、E1Gamal、Fiat-Shamir、Des / DSA、椭圆曲线数字签名算法和有限自动机数字签名算法等。

特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等,它与具体应用环境密切相关。

显然,数字签名的应用涉及法律问题。

美国联邦政府基于有限域上的离散对数问题制定了自己的数字签名标准(DSS)。

数字签名必须保证以下三点:(1)接收者能够核实发送者对报文的签名。

(2)发送者事后不能抵赖对报文的签名。

(3)接收者不能伪造对报文的签名。

数字签名的主要功能是:保证信息传输的完整性,进行发送者的身份认证,防止交易中的抵赖发生。

Hash签名是最主要的数字签名方法,也称之为数字摘要法(DigitalDigest)或数字指纹法(DigitalFingerPrint)。

与RSA数字签名是单独的签名不同,该数字签名方法是将数字签名与要发送的信息紧密联系在一起,它更适合于电子商务活动。

将一个商务合同的个体内容与签名结合在一起,比合同和签名分开传递增加了可信度和安全性。

数字摘要(DigitalDigest)加密方法亦称安全Hash编码法(SHA)或MD5。

该编码法采用单向Hash函数将需加密的明文"摘要"成一串128bit的密文,这一串密文亦称为数字指纹(FingerPrint),它有固定的长度,且不同的明文摘要必定一致。

这样,这串摘要就成为验证明文是否为"真身"的"指纹"了。

数字证书又称为数字标识(DigitalCertificate或DigitalID),是由证书签证机关(CA)签发的对用户的公钥的认证。

因此,证书的内容应包括CA的信息、用户信息、用户公钥、CA签发时间及有效期等内容。

目前国际上对证书的格式及认证方法遵从X.509体系标准。

- 数字证书实际上是一份电子文档。

- 数字证书是一段包含用户身份信息、用户公钥信息以及身份验证机构数字签名的数据。

身份验证机构的数字签名可以确保证书信息的真实性。

证书格式及证书内容.....

编辑推荐

《网络工程师考试考点分析与例题精解》可作为参加全国计算机技术与软件专业技术资格（水平）考试——网络工程师考试的复习用书，也可作为网络工程技术人员的参考用书。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>