<<计算机网络技术项目化教程>>

图书基本信息

书名：<<计算机网络技术项目化教程>>

13位ISBN编号：9787302304791

10位ISBN编号：7302304793

出版时间：2013-1

出版时间：清华大学出版社

作者：任雪莲　等主编

页数：238

字数：371000

<<计算机网络技术项目化教程>>

内容概要

《计算机网络技术项目化教程》系统地介绍了计算机网络的基础知识、相关技术和实际应用。全书共分10
章，主要内容包括：计算机网络基础知识、服务器操作系统的安装、局域网及其技术、局域网的结构化布线技术、路由器和交换机的配置、无线局域网、网络服务、计算机网络安全等，另外为了方便读者实践学习，还介绍了vmware
workstation 8的使用教程。

《计算机网络技术项目化教程》侧重对实际动手能力的培养，强调在掌握计算机网络基础知识的同时，通过对书中各种实际项目的理解，提高学习者分析问题、解决问题的能力。

《计算机网络技术项目化教程》适合作为高等职业院校、高等专科学校、成人高校、本科院校等二级职业技术学院的教材，也可作为示范性软件职业技术学院、继续教育学院、技能型紧缺人才培养的培训教材，还可作为本科院校、计算机专业人员和爱好者的参考用书。

书籍目录

章节摘录

版权页： 插图： 在1998年11月18日，美国商务部出口管理局修改了上述对加密技术出口的限制规定。
现在除古巴、伊朗、伊拉克、利比亚、朝鲜人民共和国、苏丹和叙利亚外，对其他国家出口加密技术产品，对DES及类似的批量加密技术（RC2、RC4、RC5及CAST）密钥长度允许达到56位，对非对称密钥RSA的密钥长度允许达到1024位。
此外，任何美国公司只要未在上述国家开设分支机构，均可自由使用不限长的加密密钥。
（2）常用对称加密原理 ①DES 数据加密标准（DES）是最常用的批量加密技术。
它最初是IBM于1977年开发出来的，能够抵抗对其密钥的进攻。
DES将要加密的明文按64位大小划块，并使用56位的密钥经过一系列的数学运算进行加密转换，最终得到密文。
在标准的DES的基础上，各厂商也陆续开发了不少DES变种，如密码块链接及三级DES等。
密码块链接技术将明文的数据块在加密前与前一数据块进行异或（XOR，一种逻辑运算）处理，大大加强了保密性。
三级DES则是将数据进行三次DES加密运算得到密文，借以提高加密强度。
②RC2／4 RC2和RC4这两个相关的加密技术是由美国的RSA Data Security，Inc.开发的。
RC2是与DES相似的批量加密算法，而RC4则是对数据流进行加密的算法。
它们均采用128位的密钥，但支持密钥掩码技术。
这意味着部分密钥是公开的，而剩余的部分密钥用于加密，总的密钥长度仍维持128位。
在设计用于出口的40位加密软件产品时，采用支持密钥掩码技术的算法就有相当的优势。
③IDEA 国际数据加密法则（IDEA）是另一种批量加密算法。
IDEA的模式与DES类似，它以64位大小划分数据块，使用128位长的密钥。
IDEA也是我们常见的PGP使用的加密技术。
2.公开密钥加密 在我们上述介绍的简单例子中，即便是数学天分不高的人也很容易理解对称密钥加密的工作原理。
相比而言，公钥加密的机制反而是一般人较少接触到的。
事实上，公钥加密技术与其说是一种技术，倒不如说更像是变魔术一样。
公钥加密的关键特点在于：（1）与对称加密机制的使用的单一密钥不同，公钥加密是使用一对相关的密钥（即密钥对）进行加密。
（2）任何使用密钥对中的一个密钥进行加密的消息只能用该密钥对中另一个密钥来解密。
例如，我们假设张三与李四两人希望使用公钥加密机制来交换数据。

编辑推荐

《高等职业教育"十二五"规划教材:计算机网络技术项目化教程》适合作为高等职业院校、高等专科学校、成人高校、本科院校等二级职业技术学院的教材，也可作为示范性软件职业技术学院、继续教育学院、技能型紧缺人才培养的培训教材，还可作为本科院校、计算机专业人员和爱好者的参考用书。

版权说明