<<密码学与网络安全>>

图书基本信息

书名：<<密码学与网络安全>>

13位ISBN编号：9787302185840

10位ISBN编号：7302185840

出版时间：2009-1

出版时间：清华大学出版社

作者：福罗赞

页数：658

前言

互联网作为一个世界范围的通信网络，已经在许多方面改变了我们的日常生活。
一个最新的商业上的例子就是每个人都可以在线购物。
万维网（WWW）还可以让我们分享信息。
电子邮件的技术把世界各个角落的人联系在了一起。
这种必然的发展也形成了对互联网的依赖。
互联网作为一个开放的论坛，已经产生了一些安全方面的问题。
互联网需要有机密性、完整性和可信性。
人们需要确保网络通信是机密的。
当我们在线购物时，我们需要确保出售方是真实的。
当我们把交易请求发送给银行时，我们还要保证信息的完整性不被破坏。

<<密码学与网络安全>>

内容概要

《密码学与网络安全》延续了Forouzan先生一贯的风格，以通俗易懂的方式全面阐述了密码学与计算机网络安全问题所涉及的各方面内容，从全局角度介绍了计算机网络安全的概念、体系结构和模式。

《密码学与网络安全》以因特网为框架，以形象直观的描述手法，详细地介绍了密码学、数据通信和网络领域的基础知识、基本概念、基本原理和实践方法，堪称密码学与网络安全方面的经典著作。

作者简介

Behrouz A. Forouzan 先生毕业于加州大学艾尔温分校，现在是迪安那大学教授，从事计算机信息系统方面的研究工作。
此外，他还是多家公司的系统开发咨询顾问。
除本书外，Forouzan还著有多部成功的编程与网络方面的书籍，有的已经成为该领域的权威性著作，例如《TCP/IP协议族（第3版）》和《密码学与网络安全》等。

<<密码学与网络安全>>

书籍目录

章节摘录

第1章　导言　　目标　　本章的几个目标是：　　·明确三种安全目标　　·明确威胁安全目标的几种攻击　　·明确安全服务的内容及其和三种安全目标的联系　　·介绍两种实现安全机制的技术：密码术和密写术　　我们生活在信息时代，在生活的各方面都需要保持信息畅通。
换句话说，信息是一种资产，它和其他任何资产一样具有价值，需要被保护以避免攻击。
为了安全，信息要被隐藏起来以避免未经授权的访问（机密性），被保护起来以避免未经授权的更改（完整性），还要保证对授权实体随时可用（可用性）。
直到几十年前，信息才被组织在一起并保存在物理文档中。
访问人被限制在该组织内已被授权并可信赖的少数几个人中，这样就实现了文档的机密性。
随着计算机的出现，信息储存被电子化。
信息并不是存储于物理介质之中，而是存于计算机中。
然而三种安全要求却并未因此而改变。
存储于计算机中的信息要求具有机密性、完整性和有效性，然而实现这三种要求的方法各不相同并具有挑战性。
过去的20年中，计算机网络在信息应用上掀起了一场革命。
信息是分散的，利用计算机网络，一个被授权的人可以从很远的地方发送或接收信息。
上述三种要求（机密性、完整性和可用性）不但并未改变，而且具有了新的含义。
不仅在信息被保存在计算机当中时要确保其机密性，而且应当有一种方法，能使信息在由一台计算机被发送到另一台计算机的过程中，也能保证其机密性。
在本章中，我们首先讨论信息安全的三个主要目标，然后再来了解一下什么样的攻击才能对这三个目标构成威胁，并且进一步讨论与这三种安全目标有关的安全服务。
最后，我们详细论述提供安全服务的机制，同时介绍用来实现安全机制的技术。

<<密码学与网络安全>>

编辑推荐

《密码学与网络安全》作者Behrouz A Forouzan运用一种易于理解的写作风格和直观的表述方法，为我们全面介绍了密码学与网络安全方面的概念。
他把难于理解的教学概念穿插在了中间的章节中，这样既为后面章节的学习打下必要的数学基础，又紧密结合密码学，使枯燥的数学概念变得妙趣横生。
概念阐释直观、易懂稗序可用性强，便于学生实践最新的网络安全技术，贴近实际。
《密码学与网络安全》（包括其中文导读英文版）可作为大学本科通信相关专业的教科书，也可作为对密码学与网络安全有兴趣的读者的自学用书。

<<密码学与网络安全>>

版权说明