<<计算机安全基础>>

图书基本信息

书名：<<计算机安全基础>>

13位ISBN编号：9787508440750

10位ISBN编号：7508440757

出版时间：2006-10

出版时间：中国水利水电出版社

作者：帕布鲁兹

页数：453

字数：729000

<<计算机安全基础>>

内容概要

本书重点介绍了密码学、计算机与网络安全的基本概念，为读者提供了完整而全面的理论和技术支持。
本书的主要内容包括：密码学基础、私钥密码系统、公钥密码系统、伪随机数、散列法、数字签名、认证、秘密共享、零知识证明系统、群体密码学、密钥建立协议、身份识别、入侵检测、电子投票和数字货币、数据库保护与安全、访问控制以及网络安全等。
　　全书内容广博权威，讲解由浅入深，且重要的章节都附有习题，可以帮助读者进一步掌握本章的内容。
本书适用于计算机专业或相关专业本科生专业课、研究生课程教材，也可作为专业人员的参考书。

<<计算机安全基础>>

作者简介

作者：(德)帕布鲁兹 译者：孙茂竹 范歆 等

<<计算机安全基础>>

书籍目录

前言第1章　绪论　1.1　引言　1.2　术语　1.3　历史透视　1.4　现代密码学第2章　基础理论　2.1　数论基本原理　2.2　计算技术中的代数结构　2.3　计算复杂性　2.4　信息论基本原理　2.5　习题第3章　私钥密码系统　3.1　传统密码　3.2　DES系列　3.3　现代私钥加密算法　3.4　差分密码分析　3.5　线性密码分析　3.6　S盒理论　3.7　习题第4章　公钥密码系统　4.1　公钥密码的概念　4.2　RSA密码系统　4.3　Merkle-Hellman密码系统　4.4　McEliece密码系统　4.5　EIGamal密码系统　4.6　椭圆曲线密码系统　4.7　概率加密　4.8　公钥加密范例　4.9　习题第5章　伪随机性第6章　散列法第7章　数字签名第8章　认证第9章　私密共享第10章　群体密码学第11章　密钥建立协议第12章　零知识证明系统第13章　身份识别第14章　入侵检测第15章　电子选举和数字货币第16章　数据库保护和安全第17章　访问控制第18章　网络安全参考资料

<<计算机安全基础>>

编辑推荐

计算机安全以前成为世人所瞩目的一件大事。
本书的主要目的是论述计算机与网络安全的基本概念。
本书的初稿源自作者在澳大利亚武龙岗(wollonggong)大学教授本科课程《计算机安全》时使用的讲稿。
本书共有18章，作为一本书，它所包含的知识已经较为完备了。

<<计算机安全基础>>

版权说明