第一图书网, tushu007.com

<<信息安全原理与技术>>

图书基本信息

书名：<<信息安全原理与技术>>

13位ISBN编号：9787302177654

10位ISBN编号：7302177651

出版时间：1970-1

出版时间：清华大学出版社

作者：郭亚军，宋建华，李莉 著

页数：246

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

第一图书网, tushu007.com

前言

信息安全涉及的知识面很广，本书的目标是力图向读者系统地介绍信息安全的基本原理与技术。
全书主要由下面几个部分组成。
第一部分：信息安全的数学基础。
这一部分介绍了信息安全所需要的数学知识，包括数论、代数基础、计算复杂性理论和单向函数等。
第二部分：信息安全的基本理论与技术。
包括密码技术、认证、数字签名和访问控制等。
第三部分：信息安全技术在网络安全上的应用。
这一部分重点介绍了PKI技术、网络安全协议。
第四部分：系统安全技术这一部分简单介绍了保障系统安全的防火墙技术和入侵检测技术。
信息安全涉及许多复杂的概念和技术。
为了处理这种复杂性，本书从两个方面让读者“看透”信息安全基本技术。
一是从整体上让读者了解其外貌，从全局的角度向读者揭示信息安全研究的基本内容和基本技术，本书的章节安排体现了这一点；二是在局部方面向读者展示每一章应该学些什么以及它们的作用等（如导读部分）。
本书作者多年从事信息安全课程的教学和研究，了解学生的需要，因此本书始终从读者的角度进行编写的。
每一章的导读部分介绍了本章的知识要点、作用以及它们之间的联系。
在正文中用大量的事例来帮助读者理解重点知识和难点知识。
为了方便教师授课，我们还专门整理了本书的课件以及本书习题的全部答案。
本书由郭亚军整体规划和统稿，郭亚军编写了第1、2、3、4章，宋建华编写了第6、7、9、10章，李莉编写了第5、8章。
本书在编写过程中参考了国内外许多文献和书籍，在此，编者对原作者表示真诚的感谢！
本书的出版得到了中国博士后基金（20070410953）和华中师范大学教学研究项目（2007004）的资助。
在本书的编写过程中得到了许多同行的热情帮助和支持，得到了清华大学出版社编辑们的关心和帮助，在此一并表示衷心的谢意。
由于作者水平有限，书中难免有不足之处，敬请读者提出宝贵意见。

第一图书网, tushu007.com

<<信息安全原理与技术>>

内容概要

《高等学校信息安全专业规划教材：信息安全原理与技术》系统地介绍了信息安全的基本原理和基本技术。
全书共10章，包括信息安全的数学基础、对称加密技术、公钥加密技术、消息认证与数字签名、身份认证与访问控制、网络安全协议、公钥基础设施、防火墙和入侵检测等内容。

本书体现以读者为中心的思想。
为了让读者充分理解每一章节内容以及它们之间的联系，每一章附有本章导读，并用大量的事例帮助读者理解重点知识和难点知识。

本书可作为计算机、信息安全、通信等专业的本科生以及低年级的研究生的教材，也可供从事信息安全相关专业的教学、科研和工程技术人员参考。

第一图书网, tushu007.com

<<信息安全原理与技术>>

书籍目录

第一图书网, tushu007.com

章节摘录

3．5 数据加密标准1949年Shannon的论文《保密系统的通信理论》，标志着密码学作为一门独立的学科的形成。
从此，信息论成为密码学的重要的理论基础之一。
Shannon建议采用扩散（Diffusion）、混淆（Confusion）和乘积迭代的方法设计密码。
所谓扩散就是将每一位明文和密钥的影响扩散到尽可能多的密文数字中。
这样使得密钥和明文以及密文之间的依赖关系相当复杂，以至于这种依赖性对密码分析者来说无法利用。
产生扩散的最简单的方法是置换。
混淆用于掩盖明文和密文之间的关系。
使得密钥的每一个位影响密文的许多位，以防止对密钥进行逐段破译，并且明文的每一个位也应影响密文的许多位，以便隐蔽明文的统计特性。
用代换方法可以实现混淆。
混淆就是使密文和密钥之间的关系复杂化。
密文和密钥之间的关系越复杂，则密文和明文之间、密文和密钥之间的统计相关性就越小，从而使统计分析不能奏效。
设计一个复杂的密码一般比较困难，而设计一个简单的密码相对比较容易，因此利用乘积迭代的方法对简单密码进行组合迭代，可以得到理想的扩散和混淆，从而得到安全的密码。
近代各种成功的分组密码（如DES、AES等），都在一定程度上采用和体现了Shannon的这些设计思想。
为了适应社会对计算机数据安全保密越来越高的需求，美国国家标准局（NBS），即现在的国家标准和技术研究所（NIST）于1973年5月向社会公开征集标准加密算法，并公布了它的设计要求。
（1）算法必须提供高度的安全性。
（2）算法必须有详细的说明，并易于理解。
（3）算法的安全性取决于密钥，不依赖于算法。
（4）算法适用于所有用户。
（5）算法适用于不同应用场合。
（6）算法必须高效、经济。
（7）算法必须能被证实有效。
1974年8月27日，NBS开始第二次征集，IBM提交了算法LUCIFER，该算法由Feistel领导的团队研究开发，采用64位分组以及128位密钥。
IBM用改版的Lucifer算法参加竞争，最后获胜，成为数据加密标准（DataEncryptionStandard，DES）。
1976年11月23日，采纳为联邦标准，批准用于非军事场合的各种政府机构。
1977年1月15日，数据加密标准，即FIPSPUB46正式发布。
DES是分组密码的典型代表，也是第一个被公布出来的加密标准算法。
现代大多数对称分组密码也是基于Feistel密码结构。

第一图书网, tushu007.com

编辑推荐

第一图书网, tushu007.com

<<信息安全原理与技术>>

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