<<密码学基础>>

图书基本信息

书名：<<密码学基础>>

13位ISBN编号：9787560620848

10位ISBN编号：7560620841

出版时间：2008-8

出版时间：西安电子科技大学出版社

作者：范九伦 等 著

页数：174

<<密码学基础>>

前言

密码学有着悠久而神秘的历史，最早的密码技术可以追溯到古罗马时代。
1949年，Claude Shannon在Bell System Technical Journal上发表的论文“The Communication Theory of Secrecy Systems”，标志着密码学研究进入了崭新的时代。
20世纪70年代以来，分组密码和公钥密码技术得到了迅速发展，取得了丰富的研究成果，也被广泛应用于信息安全的各个领域。
随着互联网技术和计算机技术的发展和普及，越来越多的人认识到密码学的重要性。
为了能为在校本科生学习密码学提供内容较新、论述较系统的教材，也能为相关领域的科研人员提供一本内容充实、具有一定实用性的参考书，我们编写了《密码学基础》这本教材。

本书系统介绍了密码学的基本原理，在此基础上详细介绍了密码学中的基本算法及其应用，详细介绍了当前广泛应用的密码算法及其理论基础，并对其安全性进行了相应的分析。
本书内容以当前广泛应用的密码技术为主，重点放在密码学研究的核心问题上，既突出了广泛性，又注重对主要知识内容的深入讨论。
本书的每一章后都附有相应的习题，便于读者对书中的内容进行总结和应用，同时也对思维和智力进行相应的锻炼。
作为示例，本书给出了常用的基本加密算法——DES和RSA算法的C语言程序。

本书主要供信息安全、网络工程、计算机科学与技术、通信工程等本科专业的高年级学生使用。
学习该课程的学生需要具备高等数学和线性代数的基础知识，同时应该掌握基本的编程技术和数据结构的基本知识。
通过对本课程的学习，学生可以掌握基本的密码学算法原理，对加／解密技术具备一定的实际应用能力。
为了便于学生学习和理解本课程，我们以结论性的方式在附录A中给出了学习密码学需要具备的数论基础知识。
对于已经具备相关数论知识的学生，这一部分内容可以作为了解内容；对于不具备相关数论基础知识的学生，这一部分内容可以作为自学内容。
本书计划课时为48～64学时，其中对密码学基础知识的介绍大约需要48学时，具有扩展性的知识用*号给出了标记。
在讲授本书的过程中，建议根据课时量和授课对象来选择和组织相关内容。

<<密码学基础>>

内容概要

本书系统地介绍了密码学的基本原理、基本算法，并对算法的安全性进行了相应的分析。主要内容包括古典密码、分组密码、序列密码、Hash函数、公钥密码、数字签名、密钥管理和计算复杂性等。

本书主要供信息安全、网络工程、计算机科学与技术、通信工程等本科专业的 高年级学生使用，也可供相关专业的教学、科研和工程技术人员参考。

<<密码学基础>>

书籍目录

<<密码学基础>>

章节摘录

第1章　古典密码　　古典密码（Classical Cipher)是现代密码的基础。
本章在简要介绍密码学基本概念的基础上，介绍一些典型和古典密码体制，通过对古典密码学进行分析，给出密码分析学的基本概念和原理。
1.1　密码学的基本概念　　密码学有着悠久而神秘的历史，人们很难对密码学的起始时间给出准确的定义。
一般认为人类对密码学的研究与应用已经有几千年的历史，该学科一直广泛应用于军事领域。
密码学正式一门科学的理论基础应该首推1949年美国科学家Shannon的一篇文章《保密通信的信息理论》，他在研究保密机的基础上，蝗出了将密码建立在解某个已知数学难题基础上的观点。
20世纪70年代，以公钥密码体制的提出和数据加密标准DES的问世为标志，现代密码学开始蓬勃发展。
随着计算机技术和网络技术的发展，互联网的普及和网上业务的大量开展，人们更加关注密码学，更加依赖密码技术。
保密是密码学的核心。
密码学的基本目的是面对攻击者Oscar,在被称为Alice和Bob的通信双方之间应用不安全的信道进行通信时，设法保证通信安全。
密码学研究对通信双方要传输的信息进行何种保密变换以防止未被授权的第三方对信息的窃取。
此外，密码技术还可以用来进行信算鉴别、数据完整性检验、数字签名等。
在通信过程中，Alice和Bob也分别被称为信息的发送方和接收方。
Alice要发送给Bob的信息称为明文（Plaintext）。

版权说明