

<<密码学与通信安全基础>>

图书基本信息

书名：<<密码学与通信安全基础>>

13位ISBN编号：9787560945682

10位ISBN编号：7560945686

出版时间：2008-11

出版时间：华中科技大学出版社

作者：祝跃飞，王磊 编著

页数：152

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>

## &lt;&lt;密码学与通信安全基础&gt;&gt;

## 前言

鉴于安全机制和通信系统早已紧密结合甚至融合，通信专业的硕士研究生学习必要的密码理论和技术已经成为现实的需要。

本书正是专门针对这一需要而编写的。

当前，密码学的内容非常丰富，通信专业的研究生应该掌握哪些基本的密码理论和技术是编写本书首先需要考虑的问题。

基于通信专业研究生学习密码学的目的和一般所具备的知识基础考虑，我们在下述思想指导下进行了内容的选取和体系设计。

第一，通信专业研究生学习密码学的主要目的是理解和掌握基本的密码技术，进而理解其在通信系统中应用的基本思想和方法。

因此，本书的重点在于应用密码学和掌握典型密码算法，而未包括难度较大的密码安全性理论和密码分析方面的内容。

第二，考虑到读者学习过大学工科数学和信息论与编码课程，书中就不再涉及相关的数学原理。由于目前国内信息安全数学基础课程已经成熟，因此教材中没有包含相关数学基础的详细内容，仅在附录中给出主要的概念和结论。

另外，考虑到一般通信专业学生没有系统学习计算复杂性理论，在附录中简要介绍了相关的基本知识供读者参考。

第三，读者学习密码学的最终目的是在理解和掌握现有的核心密码技术及其应用的基础上，深入理解密码学的思想和应用方法，从而能够较好地适应密码学和通信安全技术快速发展的需要，因此本书建立了一个密码学的体系结构，重点揭示了密码设计思想及密码应用模式和方法。

第四，在密码应用方面，选取因特网应用作为重点介绍，既取决于目前通信现实，更利于系统地理解密码技术的应用思想，同时介绍各种无线通信网的安全体系，从而使读者较为全面地了解目前密码学在通信中的应用。

在这些内容的介绍中，采用了先阐述原理再展开对细节做必要介绍的模式，而不是以技术手册的方式进行全面细节介绍，这样更符合教材的特点。

第五，为了适应读者不同层次学习的需求，本书分为4个层次。

第1个层次为1 - 4章，其内容为应用密码学基础，其中，第1章概要介绍密码学学科体系，第2 - 4章分别介绍加密体制、认证系统和基本密码协议。

第2个层次包括第5 - 9章，内容为应用密码学，较为系统地介绍了密码技术在因特网中的综合应用，同时简单介绍了各种无线通信网和密码相关的安全机制。

第3个层次包括第10 - 12章，内容为密码算法，重点介绍各种典型算法的细节和数学原理，供需要深入了解算法进而实现算法的读者学习。

最后1个层次是第13章，介绍了密码学的其他典型内容，供读者全面地了解密码学。

前2个层次为基本内容，而后2个层次为深入学习的内容。

这种分层次的体系结构非常便于读者由浅入深的学习。

由于本书定位于通信安全的密码学基础，对密码学的介绍还是比较基本的，如果需要进一步深入学习，请参考有关的专业书籍（如参考文献[2]、[5]等）。

感谢国家自然科学基金项目和国家“863”项目的支持。

作者 2008年2月

## <<密码学与通信安全基础>>

### 内容概要

本书主要面向通信专业的硕士研究生，是基于这类读者的一般知识基础和学习密码学的目的而专门设计编写的。

本书内容按照4个层次编写：第1层次为应用密码学基础，在概要中介绍密码学学科体系，介绍各种基本密码技术；第2层次为应用密码学，较为系统地介绍密码技术在因特网中的应用，同时简单地介绍密码技术在各种无线通信网中的应用；第3层次为密码算法，重点介绍各种典型算法及其数学原理；第4层次简单介绍现代密码学的一些其他问题。

另外，在附录中简要给出必要的数学基础和计算复杂性的理论基础知识。

本书的分层体系便于读者由浅入深逐步学习密码学，因内容不包括层次较深的密码安全理论和密码分析内容，故可供以应用为主而非研究为目的学习密码学的读者作为参考书籍。

## 书籍目录

第1章 密码学概要 1.1 密码学的简要历史 1.2 密码学的体系结构 1.2.1 安全问题 1.2.2 基本密码技术 1.2.3 安全性 1.2.4 有效性 1.2.5 密码分析 习题第2章 加密体制 2.1 古典密码 2.1.1 算法基本模式 2.1.2 代换密码举例 2.2 Shannon理论概要 2.2.1 伪密钥与唯一解距离 2.2.2 完善保密性 2.2.3 实际保密性 2.3 加密体制的安全性 2.4 序列密码 2.4.1 工作模式与研究问题 2.4.2 线性反馈移位寄存器 2.4.3 典型算法 2.5 分组密码 2.5.1 基本参数与模式 2.5.2 主要算法 2.5.3 使用模式 2.6 公钥加密体制 2.6.1 产生背景和理论模型 2.6.2 安全性 2.6.3 典型算法 2.6.4 混合加密和密钥封装—数据封装模式 习题第3章 认证系统 3.1 杂凑函数 3.1.1 安全性 3.1.2 典型算法 3.2 消息认证码 3.2.1 安全性 3.2.2 典型算法 3.3 数字签名 3.3.1 应用背景与形式定义 3.3.2 安全性 3.3.3 典型算法 习题第4章 基本密码协议 4.1 身份认证协议 4.2 数字证书与公钥基础设施 4.3 密钥建立协议 4.3.1 密钥分配 4.3.2 密钥协商 4.4 零知识证明协议 4.5 身份识别协议 4.6 应用协议举例 4.6.1 电话抛币协议简例 4.6.2 秘密共享简例 习题第5章 因特网安全协议基础 5.1 公钥基础设施 5.1.1 体系结构 5.1.2 X.509 5.2 网络认证 5.2.1 X.509认证 5.2.2 Kerberos简介 习题第6章 PGP 6.1 公钥系统的密钥管理 6.2 整体操作 6.3 消息格式和处理过程 6.4 信任管理 习题第7章 传输层安全协议 7.1 基本原理 7.2 握手协议 7.3 密钥系统 7.4 数据安全 7.5 协议体系 习题第8章 网络层安全协议 8.1 基本原理 8.2 SPD和SAD 8.3 认证头协议 8.3.1 认证头的格式 8.3.2 认证及其作用域 8.4 封装安全载荷 8.4.1 ESP的数据包格式 8.4.2 ESP的作用域 8.5 安全关联和密钥管理协议 8.5.1 基本原理 8.5.2 ISAKMP头格式 8.5.3 ISAKMP载荷类型 8.5.4 ISAKMP交换类型 8.6 IKE协议 8.6.1 IKEv1交换模式 8.6.2 密钥建立 8.6.3 IKEv2 8.7 虚拟专用网简介 习题第9章 无线通信安全简介 9.1 移动通信安全 9.1.1 移动通信系统概要 9.1.2 GSM安全体系 9.1.3 GPRS和3G系统的安全体系简介 9.2 无线局域网安全 9.2.1 WLAN安全技术 9.2.2 安全缺陷及改进 9.3 WAP 9.3.1 WAP简介 9.3.2 WAP安全体系 9.3.3 WAP安全实现 9.4 无线传感器网络安全简介 9.4.1 无线传感器网络简介 9.4.2 WSN的安全特点 9.4.3 WSN的安全需求 9.4.4 WSN安全机制的两种思路 9.4.5 WSN常用的安全协议 9.4.6 WSN的密钥管理第10章 对称加密算法 10.1 序列密码 10.1.1 RC4 10.1.2 基于模算术的生成器 10.2 分组密码设计原理 10.3 DES 10.3.1 加密整体结构 10.3.2 密钥扩展 10.3.3 f函数 10.3.4 解密 10.4 AES 10.4.1 数学基础 10.4.2 输入、输出和中间状态 10.4.3 整体加密和解密 10.4.4 加密、解密中的变换 10.4.5 密钥扩展 习题第11章 公钥加密算法 11.1 RSA的实现问题 11.1.1 素数分布的相关结果 11.1.2 模 $n$ 求逆算法 11.1.3 快速模幂算法 11.2 概率素性判别 11.2.1 Solovay—Strassen素性测试法 11.2.2 Miller—Rabin素性测试法 11.3 RSA-OAEP 11.4 椭圆曲线的数学理论简介 11.4.1 实数域上的椭圆曲线 11.4.2 有限域上的椭圆曲线 11.4.3 与椭圆曲线密码有关的计算问题 11.5 基于离散对数的典型加密方案 11.5.1 Cramer—Shoup体制简介 11.5.2 基于DLP的KEM 习题第12章 签名、杂凑与协议算法 12.1 RSA-PSS 12.1.1 编码 12.1.2 解码 12.1.3 RSA-PSS 12.2 基于离散对数签名 12.2.1 Schnorr签名 12.2.2 数字签名标准算法DSA 12.2.3 椭圆曲线DSA 12.2.4 基于离散对数的一般签名 12.3 杂凑函数 12.3.1 算法设计原理 12.3.2 SHA-1 12.4 零知识证明 12.5 Shamir门限秘密共享 习题第13章 其他密码问题 13.1 密钥规模的选取 13.2 特殊签名 13.2.1 典型扩展签名 13.2.2 不可否认签名 13.3 基于身份公钥密码简介 13.4 理论密码学简介 13.4.1 现有体系和基本结论 13.4.2 核心概念 13.5 分布式密码简介附录 相关知识 附录A 数学基础 A.1 初等数论 A.1.1 算术基本定理 A.1.2 同余 A.1.3 二次剩余 A.2 群 A.3 环与域 A.4 有限域 附录B 计算复杂性理论 B.1 问题与算法 B.2 算法的复杂度 B.3 问题复杂度 B.4 Turing归约与NPC问题 B.5 概率算法与有效算法含义参考文献

## <<密码学与通信安全基础>>

### 章节摘录

历史上，密码在军事、外交上的许多重大事件中起过重要甚至决定性的作用，事例不胜枚举。

第二次世界大战的历史更是集中体现了密码的意义：“月光之夜”的故事可谓密码价值的经典事例。

德国制订了代号为“月光之夜”的行动计划，计划夜间毁灭性地空袭英国工业重镇考文垂，英国通过破译德军密码及时获悉了这一计划，但如果采取措施来减轻对其重要工业基地的损失，将暴露已破译德军密码，进而导致德军很快更换密码，为了通过已破译密码获得更有价值的情报，英国首相丘吉尔艰难地选择了牺牲考文垂。

中途岛海战是太平洋战场的转折点，美国胜利的根本原因在于及时破译了日本偷袭中途岛的情报，从而设伏使日本海军遭到致命的打击。

由于行动计划被完全破译，日本战争核心人物山本五十六大将在视察途中被美国空军拦截击落座机而亡。

有专家估计，盟军密码专家的破译工作，至少使第二次世界大战缩短了8年。

由于密码的特殊作用，世界大多数国家的军政部门始终都有庞大的、秘密的密码研究机构。

当今，世界范围内的政治、军事、外交、经济等斗争更加尖锐与复杂，特别是社会信息化导致了国家安全战略的变化，各国都在不断加强对密码学研究。

## <<密码学与通信安全基础>>

### 编辑推荐

本书主要讲述应用密码学基础、应用密码学、密码算法、现代密码学的一些其他问题。本书可供各类以密码学应用为主而非研究为目的的学习的读者作为参考书籍。

<<密码学与通信安全基础>>

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>