

<<密码学基础>>

图书基本信息

书名：<<密码学基础>>

13位ISBN编号：9787030212641

10位ISBN编号：7030212649

出版时间：2008-5

出版时间：科学出版社

作者：陈少真

页数：303

字数：371000

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>

## <<密码学基础>>

### 内容概要

本书全面讲解密码学的基本知识，在阐述密码理论的同时，还介绍了大量的算法和标准，特别在序列密码体制、分组密码体制和公开密钥密码体制的章节中，不仅介绍了经典的密码体制和算法，而且阐述了部分算法的安全性分析以及相关领域的最新研究成果，为使读者更好地掌握密码学知识，本书讲授必要的数学背景，并在附录中提供相关参考资料，以便读者进行相关研究，本书表达清晰、论证严谨、习题丰富。

本书可作为高等院校应用数学、通信和计算机等专业密码学、通信安全和网络安全等课程的教材或参考书，也可供信息安全系统设计开发人员、密码学和信息安全爱好者参考。

## &lt;&lt;密码学基础&gt;&gt;

## 书籍目录

前言第1章 引论 1.1 密码学与信息安全概述 1.2 密码体制与密码分析 1.3 密码体制的安全性 1.4 香农理论简介 1.5 计算复杂性理论简介 1.6 小结与注释 习题1第2章 古典密码学 2.1 语言的统计特性 2.2 单表代替密码 2.3 单表代替密码的分析 2.4 多表代替密码 2.5 多表代替密码的分析 2.6 转轮密码与M-209 2.7 M-209的已知明文攻击 2.8 小结与注释 习题2第3章 布尔函数 3.1 布尔函数的表示方法 3.2 布尔函数的重量与概率计算 3.3 布尔函数的非线性度 3.4 布尔函数的相关免疫性 3.5 相关免疫函数的构造 3.6 严格雪崩准则和扩散准则 3.7 小结与注释 习题3第4章 序列密码 4.1 引言 4.2 线性反馈移位寄存器序列 4.3 基于LFSR的序列密码体制 4.4 带进位的反馈移位寄存器序列 4.5 小结与注释 习题4第5章 分组密码与数据加密标准 5.1 概述 5.2 分组密码的基本概念 5.3 数据加密标准DES 5.4 RC6算法 5.5 高级数据加密标准(AES) 5.6 差分密码分析原理 5.7 线性密码分析原理 5.8 分组密码的工作模式和设计理论 5.9 小结与注释 习题5第6章 公开密钥密码体制 6.1 公钥密码概述 6.2 RSA公钥体制 6.3 素性检测 6.4 RSA的安全性 6.5 Rabin公钥体制 6.6 基于离散对数问题的公钥密码体制 6.7 其他几种公钥密码体制 6.8 小结与注释 习题6第7章 Hash函数与数字签名体制 7.1 Hash函数概述 7.2 Hash函数的安全性 7.3 安全Hash算法(SHA-1) 7.4 数字签名体制概述 7.5 签名体制的安全需求 7.6 几种著名数字签名体制 7.7 群签名及其应用 7.8 盲签名及其应用 7.9 小结与注释 习题7第8章 密钥建立及管理技术 8.1 密钥概述 8.2 密钥分配 8.3 密钥协商 8.4 秘密共享 8.5 密钥保护 8.6 小结与注释 习题8第9章 身份认证和零知识证明 9.1 身份认证概述 9.2 零知识证明的基本概念 9.3 识别个人身份的零知识证明 9.4 Feige—Fiat—Shamir身份识别体制 9.5 Guillou—Quisqualter身份识别体制 9.6 Schnorr身份识别体制 9.7 Okamoto身份识别体制 9.8 身份识别体制向数字签名体制转化 9.9 小结与注释 习题9参考文献附录 附录A 数论基础 附录B 代数学基础 附录C 有限域基础

## &lt;&lt;密码学基础&gt;&gt;

## 章节摘录

第1章 引论 本章主要对密码学中的基本概念进行简要介绍，并对密码学中常用的一些符号和密码分析的类型加以说明，同时对密码学相关的信息论和计算复杂性基础知识加以阐述。

1.1 密码学与信息安全概述 研究信息的保密和复原保密信息以获取其真实内容的学科称为密码学（cryptology）。

它包括：密码编码学（cryptography）：研究对信息进行编码，实现隐蔽信息的一门学科。

密码分析学（cryptanalytics）：研究复原保密信息或求解加密算法与密钥的学科。

在邮政系统和信息的电气化传输发展以前，通信主要由秘密信使来完成。

然而信使有被抓获和叛变的可能，所以人们希望他们的通信不能为那些没有获得他们所提供的特殊的解密信息的人们所理解。

完成这一目的的技术就构成了密码编码学。

因此，密码编码学是一门使传递的信息只为预定的接收者所理解而不向他人泄漏的学科。

这里所说的信息包括文字、语音、图像和数据等一切可用于人们进行思想交流的工具。

密码的出现迫使人们使用这样或那样的方法去揭示使用了密码技术的保密通信的秘密。

当然，这一过程是在缺乏隐蔽此消息的密码技术的任何细节知识的情况下进行的。

完成这一目的的过程就构成了密码分析学，有时也称为破译或攻击。

因此，密码分析学是研究如何获得使用了密码技术的保密通信的真实内容的一门学科。

密码方法的使用和研究起源颇早。

四千多年以前，人类创造的象形文字就是原始的密码方法。

我国周朝姜太公为军队制定的阴符（阴书）就是最初的密码通信方式。

19世纪末，无线电的发明使密码学进入一个开始发展的时期。

这一时期密码的主要标志是以手工操作或机械操作实现的，通常称之为初等密码。

这类密码的编码思想是：要么错乱明文的顺序，要么用一个字母去替换另一个明文字母，要么用一组字母去替换另一组明文字母，要么对明文信息进行多次代替和置换，以达到文字加密的目的。

这一阶段始于20世纪之初，一直延续到20。

<<密码学基础>>

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>