

<<密码学>>

图书基本信息

书名：<<密码学>>

13位ISBN编号：9787508435909

10位ISBN编号：7508435907

出版时间：2006-3

出版时间：第1版 (2006年3月1日)

作者：邓安文

页数：217

字数：348000

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&gt;&gt;

## 内容概要

密码学的研究与应用已有几千年的历史，但作为一门科学是20世纪50年代才开始的。

不可否认，互联网的广泛应用大大推动了密码学的研究与发展。

大多数国家和地区都成立了密码学学会，这些学会定期召开学术会议进行学术交流，促进了密码学的研究与应用。

国内外已出版了大量有关密码学的书籍，其理论研究也相对比较成熟，很多观点已达成共识。

本书具有以下几个方面特点：表述清晰、论证严谨、内容新颖、选材精良、内容丰富翔实。

本书共12章，包括：古典密码、基础数论、信息理论，对称密钥密码系统、RSA密码、非对称密钥密码系统与离散对数、数字签名、质数与大整数算术、椭圆曲线密码、公开钥基础建设、量子密码。

写一本密码学方面著作的最大困难，就是确定应包含多少数学背景知识。

密码学是一个涉及广泛的学科，它需要多个数学领域的知识，包括数论、群论、环论、域论、线性代数、概率论以及信息论。

同样地，熟悉计算复杂性、算法和NP完全性理论也是很有用的。

在笔者看来，正是因为需要广泛的数学背景知识，所以导致学生们在开始学习密码学时感到很困难。

笔者试图不使用太多的数学理论，在大多数情况下，只有需要时才引入相应的数学工具。

当然，如果读者熟悉基本线性代数和模算术是会很有帮助的。

另一方面，对于更专业的主题，例如信息论中熵的概念，仅给出白描似的介绍。

本书理论阐述严格完备，实例丰富，包含有大量的算法程序以及形象的图形图表，适合于读者自学，也可作为学习密码学的参考书。

## 书籍目录

序前言第1章 绪论 1.1 通信安全 1.2 公开密钥密码系统与对称密钥密码系统第2章 古典密码 2.1 凯撒挪移码 2.2 仿射密码 2.3 单套字母替代法以及频率分析 2.4 福尔摩斯密码 2.5 Vigen6re密码 2.6 Hill密码 2.7 单次密码本 2.8 Enigma密码机 2.9 破译Enigma与对称群第3章 基础数论 3.1 模运算与辗转相除法 3.2 中国余式子定理(Chinese Remainder Theorem) 3.3 Lagrange定理与费马小定理 3.4 原根 3.5 二次剩余(Quadratic.Residue) 3.6 Galois域 3.7 质数理论 3.8 连分数 3.9 密码安全伪随机数生成器第4章 信息理论 4.1 概率 4.2 完美秘密 4.3 熵第5章 对称密钥密码系统 5.1 19ES与Feistel密码 5.2 Triple DES挑战DES 5.3 AES 5.4 IDEA 5.5 区块密码加密模式第6章 RSA密码 6.1 公开密钥密码系统 6.2 RSA算法 6.3 RSA的数论背景 6.4 RSA数字签名 6.5 同时进行RSA加密和RSA数字签名 6.6 RSA.129挑战与因数分解 6.7 二次筛法Pollard的 $p-1$ 法 6.7.1 二次筛法 6.7.2 Pollard的 $p-1$ 法 6.8 利用RSA私钥因数分解 6.9 RSA密码系统使用的注意事项 6.10 Wiener低幂次 $d$ 攻击 6.11 Rabin密码第7章 非对称密钥密码系统与离散对数 7.1 Pohlig-Hellman密码与离散对数 7.2 Diffie-Hellman密钥交换 7.3 ElGamal密码 7.4 Pohlig-Hellman算法 7.5 Index Calculus第8章 数字签名 8.1 数字签名方案 8.2 RSA盲签名 8.3 Hash函数简介 8.4 生日攻击 8.5 ElGamal数字签名 8.6 DSA数字签名 8.7 Schnorr数字签名 8.8 Nyberg-Rueppel数字签名 8.9 MD5 Hash函数 8.10 SHA—1 Hash函数 8.11 信息校验码MAC第9章 质数与大整数算术 9.1 大整数的加减乘法 9.2 大整数的除法 9.3 Montgomery算术 9.4 Miller-Rabin质数测试 9.5 Agrawal-Kayal-Saxena算法 9.6 公开密钥密码的质数 9.6.1 强质数 9.6.2 DSA质数 9.7 Java的BigInteger Class 9.8 大整数算术与数论套件及软件第10章 椭圆曲线密码 10.1 椭圆曲线 10.2 椭圆曲线(mod  $p$ ) 10.3 加权投影坐标 10.4 定义在Galois域 $F_m$ 的椭圆曲线 10.5 密码安全曲线 10.6 将信息转化为椭圆曲线代码 10.7 椭圆曲线公开密钥密码算法 10.8 椭圆曲线因数分解 10.9 ECCP-109挑战 10.10 并行Pollard Rho法第11章 公开密钥基础建设 11.1 认证机构CA 11.2 X.509 11.3 认证机构CA第12章 量子密码 12.1 量子实验 12.2 量子密钥分配 12.3 浅谈Shor之量子算法参考文献

#### 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>