

# 《现代密码学趣味之旅》

## 书籍信息

版次：1

页数：

字数：

印刷时间：2015年07月01日

开本：16开

纸张：纯质纸

包装：精装

是否套装：否

国际标准书号ISBN：9787515512174

## 编辑推荐

本书为我国首部现代密码技术及应用的科普读物，旨在用简单风趣的语言，深入浅出地介绍现代密码学发展历程及技术应用。

编辑推荐1.作为密码科普图书，本书语言风趣，通俗易懂

本书通过创设应用场景，采用简单风趣的语言，深入浅出地描述了现代密码学发展历程和技术应用，相比同类教材，本书深奥难懂的密码学变得通俗易懂。

编辑推荐2.密码技术爱好者的入门书籍

作为一本入门读物，无论你是信息安全专业的学生，还是业余爱好者，都可以从本书中理解到一点密码学原理，掌握到一点现代密码技术，了解到一点现代密码技术的应用。

## 内容简介

彭长根老师编写的《现代密码学趣味之旅》，为我国首部现代密码技术及应用的科普读物，旨在用简单风趣的语言，深入浅出地介绍现代密码学发展历程及技术应用，如密码学的数学技术、加密、认证、秘密共享、密钥管理、未来密码技术等，使读者既能掌握现代密码学基础知识和技术，了解实际信息安全问题的解决办法，又能激发对密码学的浓厚兴趣，非常适合高中生和非信息安全专业的大学生，以及从事相关工作的机关企事业单位人员阅读。

## 作者简介

彭长根，教授，博士，博士生导师。中国密码学会理事兼教育委员会委员、贵州省计算机学会常务副理事长兼秘书长、贵州省数学学会理事；公安部《信息安全》杂志编委；国家自然科学基金评审专家、贵州省科技计划项目评审专家、贵州省统计局专家库专家、贵州省综合评标专家、贵阳市科技局项目评审专家、贵阳市保密局信息安全专家组专家。

以第一完成人获贵州省科技进步二等奖1项、贵州省教学成果二等奖1项。主持国家自然科学基金3项、省部级科研项目5项。以第一作者或通讯作者发表学术论文近50篇，其中SCI或EI收录近20篇，主编或参编教材3部。担任过十余门基础和专业课教学。获得各种荣誉称号多项。

## 目录

## 第1章 漫步密码学的发展之路

### 1.1 追溯古代信息保密之术

### 1.2 惊叹军事领域中的密码较量

#### 1.2.1 荧屏故事中的密码学

#### 1.2.2 古战场上的另类较量

#### 1.2.3 国家安全的制高点

### 1.3 欣赏艺术视觉下的古典密码

#### 1.3.1 替换与换位造就的密码艺术

#### 1.3.2 古典密码实现的基本技巧

#### 1.3.3 古典密码的局限性

### 1.4 初识应运而生的现代密码学

#### 1.4.1 古典密码面临计算机的挑战

#### 1.4.2 从艺术到科学——现代密码学的产生

#### 1.1 追溯古代信息保密之术 1.2 惊叹军事领域中的密码较量 1.2.1 荧屏故事中的密码学 1.2.2

#### 古战场上的另类较量 1.2.3 国家安全的制高点 1.3 欣赏艺术视觉下的古典密码 1.3.1

#### 替换与换位造就的密码艺术 1.3.2 古典密码实现的基本技巧 1.3.3 古典密码的局限性 1.4

#### 初识应运而生的现代密码学 1.4.1 古典密码面临计算机的挑战 1.4.2

#### 从艺术到科学——现代密码学的产生 1.4.3 打开密码之门的咒语——密钥 1.4.4

#### 密码技术支撑下的信息安全 1.4.5 我国自己的商用密码标准

## 第2章 探寻现代密码学的数学之源

### 2.1 品味数论之美 2.1.1 数论之趣 2.1.2 由时钟想到的——模余运算 2.1.3 大素数判定的苦恼

### 2.1.4 欧拉函数和欧拉定理 2.1.5 中国古代数学的骄傲——孙子定理 2.2

### 领会从小学数学抽象出来的近世代数 2.2.1 抽象的"加法"与群论 2.2.2 由除法引出的有限域

### 2.2.3 域的"种子"——本原元 2.3 捉摸漂浮不定的随机数 2.3.1 砂锅炒板栗的故事 2.3.2

### 随机数生成算法 2.3.3 国家标准——《随机性检测规范》 2.4 见识计算机也难解的数学问题

### 2.4.1 计算机求解的"难"与"易" 2.4.2 计算机也"害怕"的数学问题 2.4.3

### 难解问题假设下的密码学 2.5 领略密码学领域中的数学家风采 2.5.1

### 信息论创始人与现代密码学的创立 2.5.2 计算机之父与密码破译 2.5.3 密码战背后的数学家

## 第3章 穿行对称密码系统之林

### 3.1 概貌略影 3.1.1 共享密钥的密码方案 3.1.2 信息的"搅拌" 3.1.3 分组密码 3.2

### 深入数据加密标准 DES 3.2.1 概览算法框架 3.2.2 领会核心结构与技术细节 3.2.3 DES

### 为什么被攻破 3.2.4 功不可没的商用标准 3.2.5 DES 还能用吗? 3.3 剖析高级加密标准 AES

### 3.3.1 AES 走向前台 3.3.2 算法结构与技术细节 3.3.3 AES 加密举例 3.3.4 AES vs DES 3.4

### 研读我国的对称密码标准 SM4 3.4.1 国标 SM4 的诞生 3.4.2 算法细节浏览 3.4.3

### 应用举例与分析 3.4.4 无线通信安全的福音 3.5 认识轻量级对称密码 3.5.1

### 步步紧逼的应用需求 3.5.2 "瘦身"的密码算法 3.5.3 几个轻量级密码体制概览 3.5.4

### 应用普及还有多远

## 第4章 攀登公钥密码系统之崖

### 4.1 入门之引 4.1.1 无需共享密钥的密码方案 4.1.2 公钥密码的精髓——有陷门的单向函数

### 4.1.3 公钥密码能为我们做什么 4.2 赏析 Diffie-Hellman 密钥交换 4.2.1 密钥交换的苦恼 4.2.2

### 整数上的对数——离散对数 4.2.3 巧妙的 Diffie-Hellman 密钥协商 4.2.4 中间人攻击 4.3

探究整数分解引出的密码系统 RSA4.3.1 RSA 设计之巧4.3.2 RSA 加密举例4.3.3 RSA 就在我们身边4.3.4 RSA 面临的挑战4.3.5 Rivest、Shamir 和 Adleman 其人其事4.4 摸索椭圆曲线上的密码系统 ECC4.4.1 椭圆曲线方程4.4.2 浅说椭圆曲线密码离散对数问题4.4.3 椭圆曲线密码举例4.4.4 被看好的公钥密码方案4.4.5 ECC 走向应用的及时雨——国家标准 SM2

第 5 章 鉴赏信息安全认证技术之宝

5.1 感触网上交易的担忧5.2 惊异信息伪造识别之术——Hash 算法5.2.1 信息也可以有"指纹"5.2.2 单向 Hash 函数的构造5.2.3 几个国际标准5.2.4 生日悖论与生日攻击5.2.5 让世界关注的国内成果5.2.6 我国的杂凑算法标准 SM35.3 赞赏身份识别技术5.4 欣慰拥有数字签名之利器5.4.1 从手写签名想到的5.4.2 数字签名设计浅说5.4.3 电子商务中的数字签名技术5.4.4 需求催生的各种数字签名方案5.4.5 保护数字版权的数字水印技术

第 6 章 踏入密钥管理技术之洲

6.1 困惑密钥管理之瓶颈6.2 知晓密钥的类型6.3 关注密钥管理的内容6.3.1 密钥生成6.3.2 密钥分发6.3.3 密钥存储6.4 浏览公钥密码基础设施 PKI 平台6.4.1 PKI 在我们身边6.4.2 细谈 PKI 技术与应用

第 7 章 走进多方密码体制之园

7.1 初见多方密码体制之基石7.1.1 买股票看承诺方案7.1.2 从阿里巴巴的咒语看零知识证明7.1.3 从扑克牌游戏看不经意传输协议7.2 初探秘密共享7.2.1 从绝密信息的分拆保存谈起7.2.2 秘密共享设计方法7.3 初解安全多方计算7.3.1 百万富翁炫富引出安全多方计算7.3.2 安全多方计算如何实现7.3.3 安全多方计算能做什么

第 8 章 开启密码系统安全之门

8.1 明晰密码方案的安全含义8.1.1 理论安全性8.1.2 实际安全性8.1.3 密码方案中的假设8.2 了然密码方案的安全目标8.2.1 网络攻击类型和攻击手段8.2.2 加密方案的安全要求8.2.3 数字签名方案的安全要求8.3 见证学术界关注的研究——可证明安全8.4 见闻密码方案的攻击案例

第 9 章 畅游密码学应用之地

9.1 贴近密码技术应用规范9.2 追寻网上办公系统中的密码技术9.3 体验电子邮件的加密与认证9.4 关注网上购物安全保障技术9.5 探求网上支付的安全防护9.6 尝试 QQ 聊天隐私保护9.7 关切手机信息安全9.8 瞭望云计算中的密码技术9.9 呼唤大数据时代的信息安全

第 10 章 登上密码学未来之舟

10.1 忧虑当前密码技术的局限性10.2 惊奇混沌现象衍生的密码技术10.3 遥望量子密码的身影

结束语参考文献

[显示全部信息](#)

在线试读部分章节

序言

密码有着数千年的悠久历史，经历了从手工、机械、电子到计算机作业的发展过程，从一种技巧演变成一门科学，特别是近年来，随着我国自主密码技术的迅速发展，密码已广泛应用到军事、外交、政府、能源、金融、交通等关键部门和重要领域，在保障我国网络和信息安全中发挥了重要作用，取得了很好的社会效益和经济效益。密码技术作为保障网络和信息安全的核心技术和基础支撑，在身份识别、安全隔离、信息保密、完整性保护和抗抵赖性等方面发挥着其他技术手段不可替代的重要作用，在当今云计算、物联网和大数据兴起的时代，亟须引起人们更多的关注。

彭长根老师编写的《现代密码学趣味之旅》，通过创设应用场景，采用简单风趣的语言，深入浅出地描述了现代密码学发展历程和技术应用，让带有深深数学烙印且深奥难懂的密码学书籍，变得通俗易懂，非常适合高中生和非信息安全专业的大学生，以及从事相关工作的机关企事业单位人员阅读。

密码科普在我国还处在起步阶段，广大密码工作者有责任和义务花更多的时间来开展这方面的工作，多出一些浅显易懂、可读性强、面向社会公众的书籍，帮助人们更多地了解密码、用好密码，引领有志于密码研究的年轻人进入这个领域，提升我国密码技术自主创新能力，在保障我国网络和信息安全中发挥更大的作用。

前言

作为中国密码学会理事兼教育工作委员会委员，一直想着为密码学的科普做点事情，这正是撰写此书的最初动机。不曾想在这过程中，渐渐喜欢上了写科普的感觉，科普工作居然出乎预料的如此有魅力。跟着这种感觉，2013年我做了一个《Diffie-Hellman 密钥交换》的科普视频课，参加了全国高校微课教学比赛，更

序言

密码有着数千年的悠久历史，经历了从手工、机械、电子到计算机作业的发展过程，从一种技巧演变成一门科学，特别是近年来，随着我国自主密码技术的迅速发展，密码已广泛应用到军事、外交、政府、能源、金融、交通等关键部门和重要领域，在保障我国网络和信息安全中发挥了重要作用，取得了很好的社会效益和经济效益。密码技术作为保障网络和信息安全的核心技术和基础支撑，在身份识别、安全隔离、信息保密、完整性保护和抗抵赖性等方面发挥着其他技术手段不可替代的重要作用，在当今云计算、物联网和大数据兴起的时代，亟须引起人们更多的关注。彭长根老师编写的《现代密码学趣味之旅》，通过创设应用场景，采用简单风趣的语言，深入浅出地描述了现代密码学发展历程和技术应用，让带有深深数学烙印且深奥难懂的密码学书籍，变得通俗易懂，非常适合高中生和非信息安全专业的大学生，以及从事相关工作的机关企事业单位人员阅读。

密码科普在我国还处在起步阶段，广大密码工作者有责任和义务花更多的时间来开展这方面的工作，多出一些浅显易懂、可读性强、面向社会公众的书籍，帮助人们更多地了解密码、用好密码，引领有志于密码研究的年轻人进入这个领域，提升我国密码技术自主创新能力，在保障我国网络和信息安全中发挥更大的作用。

前言

作为中国密码学会理事兼教育工作委员会委员，一直想着为密码学的科普做点事情，这正是撰写此书的最初动机。不曾想在这过程中，渐渐喜欢上了写科普的感觉，科普工作

居然出乎预料的如此有魅力。跟着这种感觉，2013年我做了一个《Diffie-Hellman 密钥交换》的科普视频课，参加了全国高校微课教学比赛，更进一步意识到科普工作的价值，此书的撰写正是在这种感受的驱动下所做的一点事情。曾几何时，“密码”一词不断地出现在影视作品中，密码技术也徐徐走进了大众视野。影视剧中扣人心弦的情节，惊心动魄的密码对抗，神乎其神的破译技术，总是能给人们带来无限的好奇和遐想，也激起了越来越多爱好者的探究欲望。荧屏上的密码技术自然是做了艺术化处理的，但有一个不争的事实是：军事战争驱动了密码学的发展，密码学从艺术到科学，自古就与战争联系在一起，从古代战场到现代战争，始终未离开过密码技术的较量。从姜子牙的“阴符？阴书”保密之术，到古希腊的“石蜡密信”，从二战的恩尼格玛机，到现代信息战，无不彰显着密码技术的重要作用，甚至可以说，战争催生了密码技术，密码是没有硝烟的战场，是军事领域中的另类较量。其实，密码技术也正在走进我们的生活，不管你是否意识到，它就在我们身边默默地保障着我们的信息安全。随着信息网络的飞速发展，现实中的业务将不断向网络空间延伸，从电子邮件到现在的电子商务和电子政务，无不依靠着密码技术的护航；我们所熟悉的网络银行、支付宝、证券交易背后都有坚固的密码技术做后盾。信息网络在给人类社会带来巨大方便的同时，也在深刻地改变着人们的安全观念，网络信息空间的安全已被各国提升到国家安全的战略高度。2014年，我国成立了“中央网络安全和信息化领导小组”，中共中央总书记、国家主席、中央军委主席习近平亲自担任组长，李克强、刘云山任副组长，领导小组规格之高、力度之大，可谓是前所未有。由此可见，网络空间的安全已不可小视。密码技术是信息安全的核心技术基础，它解决了信息的保密性和认证性，信息网络中防火墙、安全路由、虚拟专用网、身份认证、访问控制等，依靠的正是密码学中的保密算法和认证算法。然而有密码编码，就会有密码攻击，密码学正是以密码编码和密码分析两大分支为研究的学科，密码编码和密码攻击总是在不断的博弈之中，可谓是“道高一尺、魔高一丈”。近年来的病毒、木马、黑客、蠕虫、后门等网络攻击的日益剧增，也在悄然促进着密码技术的发展。扣人心弦的密码剧情节，眼花缭乱的网络攻击手段，常让我们跃跃欲试，渴望有朝一日自己也变成一个密码高手，成为信息安全的保护神。可是，每当我们拿起密码书籍来读，才发现那里原来全是一些索然无味的抽象数学符号，顿时让我们的兴趣荡然无存。面对渴望轻松了解密码技术及其应用的读者，面对日益严的网络攻击，作为密码学研究人员，是到了该做点什么的时候，科普不失为一种不错的选择。近年来，国内外也陆续出版了几本密码学的科普书籍，但大多是介绍古典密码技术，或是战争中的密码故事，未曾见介绍现代密码技术及其应用的作品，这正是萌生撰写本书的初衷。本书是一本现代密码技术与应用的科普书籍，旨在用最通俗的语言、生动的方式和趣味的故事介绍现代密码学方法、技术与应用，如密码学的数学技术、加密、认证、秘密共享、安全多方计算、密钥管理、PKI/CA、轻量级密码和未来密码技术等及其应用场合。主要特色是突出“现代”、“通俗”、“趣味”，通过故事、采访和新闻报道等形式，以主角艾丽和柏彬在学习、生活和工作中遇到的信息安全问题为主线，介绍现代密码学的基础知识和技术，力求文字浅显、通俗、趣味，使读者既能了解实际信息安全问题的解决办法，又能激发对密码学的浓厚兴趣。本书的读者对象定位为高中生、非信息安全专业大学生、信息技术及数学爱好者、关注信息安全的各行业工作人员和具有中等文化程度的广大民众等。作为一本入门读物，希望能透过浅显的介绍，让读者理解到一点密码学原理，掌握到一点现代密码技术，了解到一点现代密码技术的应用。云计算的风起云涌，大数据的悄然而至，又会有新的安全问题摆在我们面前，云端数据的安全存储亟待解决，大数据的隐私保护不可避

免。面对不断涌现的信息技术，此书可作为抛砖引玉之尝试。

贵州大学李祥教授作为国内老一辈计算机科学研究学者，于20世纪80年代初在贵州大学开辟了可计算性理论和计算复杂性理论研究，并形成一定的优势，基于此基础，李祥教授于20世纪90年代初期开辟了密码学研究方向，在密码算法与密码协议、模型检测方面取得了不少的研究成果，在国内形成了一定的影响。自从被恩师李祥教授引领进入密码学研究的大门，我未敢放松对密码学研究的关注，尽管身处欠发达地区工作，但仍希望能贡献一点绵薄之力，本书若能为老一辈人创建的平台增加点色彩，我将欣慰之至。本书得以完成，我首先要感谢亲如家人的研究生们，在中科院信息工程研究所做博士后的田有亮博士，为本书答辩和出版手续做了不厌其烦的工作。朝夕相处的周洲、杨玉龙、刘海（小）、任祉静、丁红发、杨震、徐志聘、张豹、吕桢、刘海（大）、王伟茹、原志龙、刘荣飞、张铎等研究生为本书的资料收集和整理做了大量的工作；更要感谢国家密码管理局和中科院信息工程研究所的支持，你们的支持是本书得以出版的重要基础；与此同时，我怀着深深的敬意感谢沈昌祥院士，您对本书的肯定是我撰写的动力。最后，衷心感谢为本书评审和提出宝贵建议的专家、学者和领导，本书包含了你们的智慧。彭长根2015年2月

伴随着信息网络的发展，病毒、木马、黑客、蠕虫、后门等术语逐步为大众所知，“棱镜门”、“心脏出血”、银行账号和隐私泄露等网络攻击事件不断发生，使网络安全渐成焦点，网络攻击威胁的日益严峻，让人们网络安全产生

了深深的忧虑。在这样的信息网络时代里，我们每个人都再也无法绕行于信息安全之外，信息安全关乎国家安全，同时也在影响着寻常百姓的工作和生活。信息安全需要法律和技术的双重保障，密码技术作为信息安全保障的核心基础，很有必要在大众中普及。网络攻击形式的日益复杂，势必需要更牢固的现代密码技术对信息保驾护航。其实，现代密码技术已悄然走到我们身边，网上购物、网络银行、第三方支付、基金证券交易等电子商务活动的不断掀起，让我们逐渐感受到密码技术的用场，但日益严峻的信息安全威胁又让人们网络安全产生了信任危机，甚

至对网络应用感到无所适从。本书力图从“应用”、“通俗”、“趣味”等目标出发，以信息网络时代为背景，通过塑造艾丽、柏彬和庞老师等人物，用通俗的方式叙述他们在学习、生活和工作中对信息安全问题的困惑及探究之旅，力图让读者了解和体会现代密码技术在信息安全中的应用，以激发读者对现代密码学的浓厚兴趣。本书涵盖了现代密码学的基本内容，包括现代密码学起源、密码的数学基础、加密、认证、秘密共享、安全多方计算、密钥管理、PKI/CA、轻量级密码和未来密码技术等。本书的第一个期望是能够引领广大读者走进现代密码技术之门，领会到现代密码学的原理及应用场景，通过典型案例的引入来提高读者对网络攻击的警觉

；另一个期望是帮助有兴趣的读者在美妙的密码世界里享受最聪明科学家们的智慧，体验数学的应用之美，不再抱怨密码算法的抽象，更好更快地带领他们走进现代密码学之门。在写本书之时，深深地体会到科普的困难，要将枯燥无味的密码算法深入浅出地展现给读者，实属难事，说实话，在这点上作者虽绞尽脑汁，但由于水平有限，未尽如人意，下一步当继续探求浅显之法，同时也渴望读者给予帮助。同时，由于时间仓促，本书肯定还有许多不当之处或错误，恳请读者朋友批评指正。

密码技术的历史起源很难追溯，戴维·卡恩（David Kahn）在《破译者》一书中就曾说道：“人类使用密码的历史几乎与使用文字的时间一样长。”一天，艾丽去另一所学校看望

同学，被同学带到该校的文化书院参观，艾丽随手从书架上拿出一本战国时期的《六韬》翻阅，居然发现第三卷的《六韬？

龙韬》是一本中国古代兵书，它通过武王和姜子牙的对话，阐述了用兵作战的原则。该卷还记载了采用"阴书"方法来传递军情，其中有一句话为"敌虽圣智，莫之能识"，正是一种秘密传递军情的方法。阴书这种保密之术可以看作是密码学的萌芽，也标志着中国古代的秘密通信方法已具有了密码学的雏形。密码学就是一种将公开信息转化为秘密信息的技术或者方法，简单地说，密码学是研究密码设计和密码破译的科学。加密是密码学中最重要技术方法之一，它是从古至今的一种保密通信的技术手段。作为四大文明古国之一的中国，在古代就已发明出种种加密手段，内容丰富，形形色色，多种多样，《六韬？龙韬》正是我国古代密码技术应用的佐证。有了上次文化书院的经历，艾丽对古代中国保密之术的兴趣油然而生。有时间她就上网浏览，发现宋代的兵书《武经总要》中也记载了一些军事保密方法，宋代的军事活动有请刀、请弓、请马、请甲、请牛车、请添兵、请进军、请固守、贼多、贼少等四十多项。为了传递军事情报的安全，宋代军队常用一首共有40个字的诗传递情报，用其中不同的字代替不同的军事活动，也就是说，用"字验"的方式实现军事的秘密通信。杜甫的《春望》就是其中的一首，在杜甫的《春望》中，诗句"家书抵万金"的"金"字表示"贼多"，那么当指挥官在传递情报时，就可以在"金"字上做一个记号，收到军事情报的人，根据"字验"的方法获得敌人秘密的军情。

[显示全部信息](#)



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www.tushupdf.com](http://www.tushupdf.com)