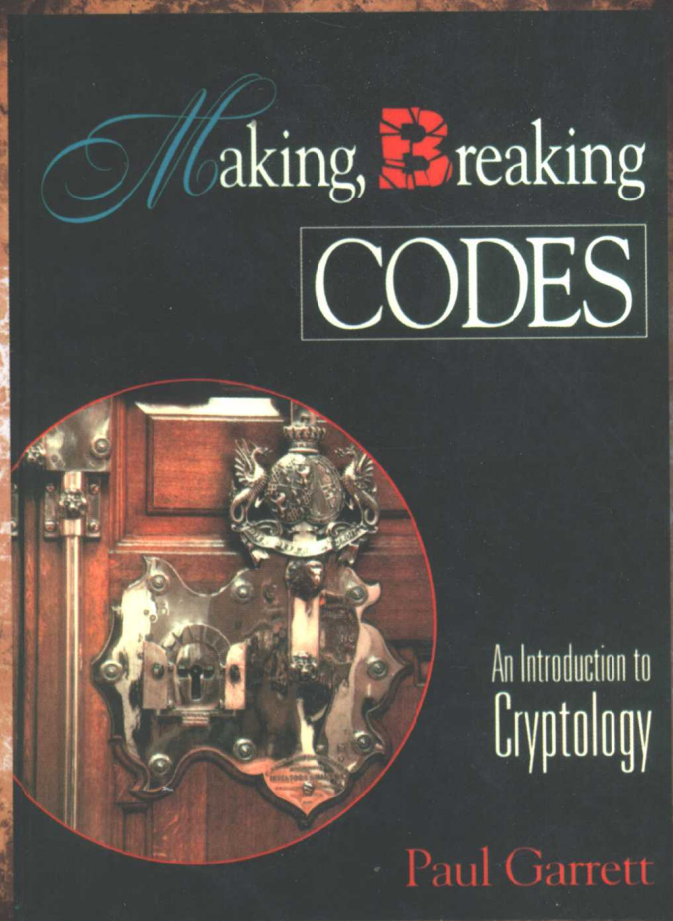
PEARSON Prentice Hall

计 算 机 科 学 丛 书

密码学导引

(美) Paul Garrett 明尼苏达大学 著 吴世忠 宋晓龙 郭涛 等译



Making, Breaking Codes
An Introduction to Cryptology

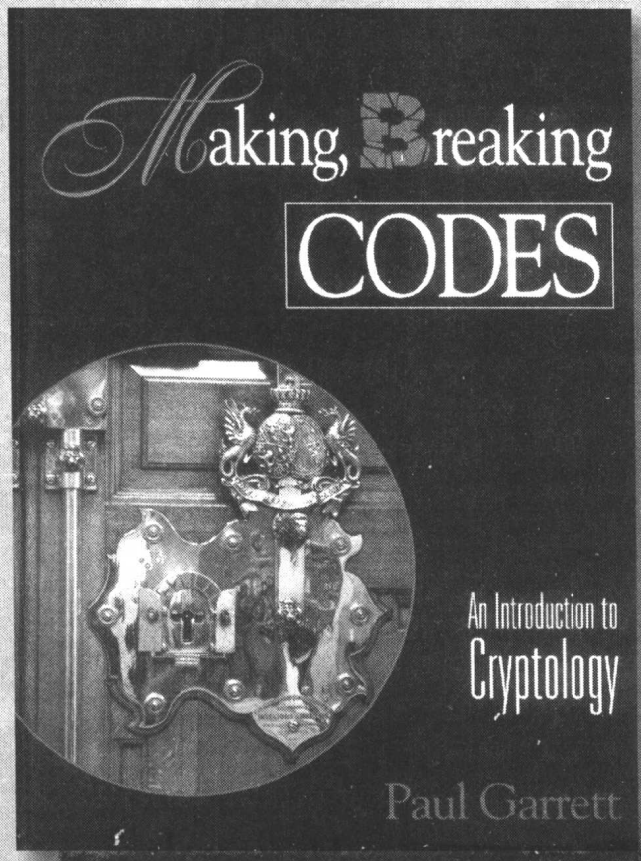
机械工业出版社
China Machine Press

Pearson Education

计 算 机 科 学 丛 书

密码学导引

(美) Paul Garrett 明尼苏达大学 著 吴世忠 郭涛 宋晓龙 等译



Making, Breaking Codes
An Introduction to Cryptology

机械工业出版社
China Machine Press

本书着重介绍现代密码学的加密思想及其实现方法，内容涉及数论、概率论、抽象代数、加密算法的思想及复杂度理论。本书介绍了密码学的历史沿革，剖析了古典的加密算法为何会被现代的加密算法所取代，展望了密码编码领域的发展，为古典和现代密码体系提供了数学理论基础，还给出了一些针对各种加密算法的密码分析方法。

本书适合作为高校计算机安全与信息安全专业密码学导论的简明教材，也可供对密码学、数论和计算机数论有兴趣的技术人员参考。

本书版权登记号：图字：01-2001-3870

图书在版编目（CIP）数据

密码学导引 /（美）加内特（Garrett,P.）著；吴世忠等译. —北京：机械工业出版社，2003.8
（计算机科学丛书）
书名原文：Making, Breaking Codes: An Introduction to Cryptology
ISBN 7-111-12478-2

Ⅰ.密… Ⅱ.①加… ②吴… Ⅲ.密码—理论 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字（2003）第 050100 号

机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码　100037）
责任编辑：[illegible]
北京瑞德印刷有限公司印刷·新华书店北京发行所发行
2003 年 8 月第 1 版第 1 次印刷
787mm×1092mm 1/16 • 27.75 印张
印数：0 001-5000 册
定价：39.00 元

出版者的话

文艺复兴以降，源远流长的科学精神和逐步形成的学术规范，使西方国家在自然科学的各个领域取得了垄断性的优势；也正是这样的传统，使美国在信息技术发展的六十多年间名家辈出、独领风骚。在商业化的进程中，美国的产业界与教育界越来越紧密地结合，计算机学科中的许多泰山北斗同时身处科研和教学的最前线，由此而产生的经典科学著作，不仅擘划了研究的范畴，还揭橥了学术的源变，既遵循学术规范，又自有学者个性，其价值并不会因年月的流逝而减退。

近年，在全球信息化大潮的推动下，我国的计算机产业发展迅猛，对专业人才的需求日益迫切。这对计算机教育界和出版界都既是机遇，也是挑战；而专业教材的建设在教育战略上显得举足轻重。在我国信息技术发展时间较短、从业人员较少的现状下，美国等发达国家在其计算机科学发展的几十年间积淀的经典教材仍有许多值得借鉴之处。因此，引进一批国外优秀计算机教材将对我国计算机教育事业的发展起积极的推动作用，也是与世界接轨、建设真正的世界一流大学的必由之路。

机械工业出版社华章图文信息有限公司较早意识到“出版要为教育服务”。自1998年开始，华章公司就将工作重点放在了遴选、移译国外优秀教材上。经过几年的不懈努力，我们与Prentice Hall，Addison-Wesley，McGraw-Hill，Morgan Kaufmann等世界著名出版公司建立了良好的合作关系，从它们现有的数百种教材中甄选出Tanenbaum，Stroustrup，Kernighan，Jim Gray等大师名家的一批经典作品，以“计算机科学丛书”为总称出版，供读者学习、研究及庋藏。大理石纹理的封面，也正体现了这套丛书的品位和格调。

“计算机科学丛书”的出版工作得到了国内外学者的鼎力襄助，国内的专家不仅提供了中肯的选题指导，还不辞劳苦地担任了翻译和审校的工作；而原书的作者也相当关注其作品在中国的传播，有的还专诚为其书的中译本作序。迄今，“计算机科学丛书”已经出版了近百个品种，这些书籍在读者中树立了良好的口碑，并被许多高校采用为正式教材和参考书籍，为进一步推广与发展打下了坚实的基础。

随着学科建设的初步完善和教材改革的逐渐深化，教育界对国外计算机教材的需求和应用都步入一个新的阶段。为此，华章公司将加大引进教材的力度，在“华章教育”的总规划之下出版三个系列的计算机教材：除“计算机科学丛书”之外，对影印版的教材，则单独开辟出“经典原版书库”；同时，引进全美通行的教学辅导书“Schaum's Outlines”系列组成“全美经典学习指导系列”。为了保证这三套丛书的权威性，同时也为了更好地为学校和老师们服务，华章公司聘请了中国科学院、北京大学、清华大学、国防科技大学、复旦大学、上海交通大学、南京大学、浙江大学、中国科技大学、哈尔滨工业大学、西安交通大学、中国人民大学、北京航空航天大学、北京邮电大学、中山大学、解放军理工大学、郑州大学、湖北工学院、中国国家信息安全测评认证中心等国内重点大学和科研机构在计算机的各个领域的著名学者组成“专家指导委员会”，为我们提供选题意见和出版监督。

这三套丛书是响应教育部提出的使用外版教材的号召，为国内高校的计算机及相关专业

的教学度身订造的。其中许多教材均已为M. I. T.，Stanford，U.C. Berkeley，C. M. U. 等世界名牌大学所采用。不仅涵盖了程序设计、数据结构、操作系统、计算机体系结构、数据库、编译原理、软件工程、图形学、通信与网络、离散数学等国内大学计算机专业普遍开设的核心课程，而且各具特色——有的出自语言设计者之手、有的历经三十年而不衰、有的已被全世界的几百所高校采用。在这些圆熟通博的名师大作的指引之下，读者必将在计算机科学的宫殿中由登堂而入室。

权威的作者、经典的教材、一流的译者、严格的审校、精细的编辑，这些因素使我们的图书有了质量的保证，但我们的目标是尽善尽美，而反馈的意见正是我们达到这一终极目标的重要帮助。教材的出版只是我们的后续服务的起点。华章公司欢迎老师和读者对我们的工作提出建议或给予指正，我们的联系方法如下：

电子邮件：hzedu@hzbook.com
联系电话：（010）68995264
联系地址：北京市西城区百万庄南街1号
邮政编码：100037

专家指导委员会

（按姓氏笔画顺序）

尤晋元	王　珊	冯博琴	史忠植	史美林
石教英	吕　建	孙玉芳	吴世忠	吴时霖
张立昂	李伟琴	李师贤	李建中	杨冬青
邵维忠	陆丽娜	陆鑫达	陈向群	周伯生
周克定	周傲英	孟小峰	岳丽华	范　明
郑国梁	施伯乐	钟玉琢	唐世渭	袁崇义
高传善	梅　宏	程　旭	程时端	谢希仁
裘宗燕	戴　葵			

译 者 简 介

吴世忠：博士、研究员，中国信息安全产品测评认证中心主任。现为全国信息安全标准化技术委员会副主任，中国信息产业商会信息安全产业分会理事长，《信息安全与通信保密》杂志主编。已公开出版文章百余篇，著有《信息系统的互连与互通》、《C3I系统的安全与保密》、《关贸总协定：中国准备好了吗？》、《首都信息化标准指南·信息安全与保密标准化体系》等专著五部和《应用密码学》、《网络信息安全的真相》、《密码学的理论和实践》、《中文 Windows 2000 的安全性》等译著五部，同时还主持起草了防火墙、应用网关安全技术要求以及信息技术安全性评估准则等 7 项国家标准，并主笔撰写了与信息安全战略技术发展有关的多篇专题报告。

宋晓龙：男，1970 年 9 月出生。2000 年 5 月毕业于中国人民解放军信息工程大学，获理学硕士学位；主要研究兴趣为密码算法与理论、密码分析和密码产品测试技术；曾在《通信学报》、《信息安全与通信保密》等刊物发表论文多篇，译著有《密码编码和密码分析：原理与方法》。

郭涛：男，1974 年 9 月出生，湖北宜昌人。毕业于华中科技大学计算机学院，2003 年 10 月将获得工学博士学位；主要研究方向为安全电子支付、信息安全、密码学；曾在《通信学报》、《高技术通讯》等刊物发表论文十几篇。

译 者 序

自从 20 世纪末以来，信息安全成为了人们密切关注的热点问题，而作为信息安全理论基石的密码学更是成为学术界炙手可热的研究方向。市场上关于密码学的译著已经不下几十本，当然也包括我们翻译的《应用密码学》、《密码编码和密码分析》（中译本由机械工业出版社引进出版）等书。而明尼苏达州大学数学系的 Paul Garrett 教授所著的这本书以其深入浅出、条理清晰的风格而在诸多密码学专著中独具特色，它弥补了其他密码学专著忽略密码学相关数学知识的不足，介绍了与密码学相关的几乎所有数学知识。通过阅读本书，读者可以对密码学涉及到的所有数学知识有一个比较全面的了解，有助于加深读者对密码学的理解。

本书并没有深入阐述密码理论和具体的密码算法，而是就密码学相关的数学知识做详细介绍。如果跳过数学知识部分，本书可以作为一本密码学导论。但本书更是一本数论教程，一本以密码学为主线、包含抽象代数的广义数论教程。因此，本书不仅适合于广大数学、密码学专业的学生阅读，也适合于密码学和网络安全专业人士参考。我们希望所有读者阅读之后都能有所收益。

本书的翻译工作受到国家自然科学基金重大项目（90104033）的资助。

本书由吴世忠、郭涛、宋晓龙主持翻译，其他参与翻译校对工作的人员还有杨玉斌、付敏、彭建芬等，在此一并表示感谢。

由于水平所限，翻译不妥或错误之处在所难免，敬请广大读者批评指正。

吴世忠

2002 年 9 月

于中国信息安全产品测评认证中心

前　言

本书主要介绍现代密码学的加密思想及其实现方法，涉及数论、概率论、抽象代数。此外，还有一些是加密算法思想的描述及复杂度理论。我们在讨论安全通信及其理论时，有三个专业术语的含义有些许差异，它们是*密码编码*（cryptography）、*密码分析*（cryptanalysis）和*密码学*（cryptology）。其中，密码编码指的是用各种不同的加密算法对信息进行加密，以保证其安全性；密码分析是相对于密码编码而言的，它包含有密码攻击、发现漏洞和系统安全性证明的内容。密码学则是一个比较综合的概念，它涵盖了密码编码和密码分析两个概念，这也是使用最频繁的一个词。

在介绍了密码编码、密码分析和密码学的概念之后，下面我们介绍一下本书的主要内容：

1) 介绍密码学的历史沿革，特别是给出一些古典的加密算法，并且分析这些算法为什么被现代的加密算法所取代。
2) 密码编码领域的展望（在实际应用领域，加密并不仅仅用于数据的安全和保密）。
3) 介绍古典和现代密码体系的同时，给出这些密码体系的数学理论基础。
4) 给出一些针对各种加密算法的密码分析方法。
5) 阐明密钥管理和执行是基础。

阅读本书要求读者具备跟微积分相关的复杂数学和一些基本的线性代数知识。

首先我们将有选择性地介绍*古典密码学*，这主要是指 20 世纪 40 年代之前的密码编码和密码分析技术。特别是在 1935 年到 1940 年期间，一些通过机械的和初级的电子设备自动实现加密和解密的设备大量出现，这些设备工作速度很慢，而且非常的笨重。这主要是由于加密和解密的过程基本上是用机械和电子方法实现的，并不是通过软件实现的。

按照现代的标准来衡量，那些古典密码（德国的恩格码之前的密码）看来是很失败的。这主要归功于现代的计算机远比 20 世纪 40 年代那些用真空电子管的机器要好得多，而且现在的加密算法远比以前的复杂，主要是为了防止一些在以前看来是不可思议的攻击。

虽说古典的密码分析和现代的密码分析有很大的区别，但它们有一个共同的地方：都使用了数学中的*统计算法*（stochastic algorithm）或者*概率算法*（probabilistic algorithm）。这相对于初等数学中非常传统而且较常用的*确定性算法*（deterministic algorithm）形成了鲜明的对比。对于许多应用目的而言，这样的算法运行速度非常快但成功率却达不到 100%，或者说通常运算速度较快，但不总对。这似乎就像现实生活，而非人为的特意忽略。

在这里需要说明的一点就是，计算机的普及对密码学理论产生了很大的影响，极大地改变了密码学，例如：

1) 加、解密的工作可以自动完成，大规模的加、解密的运算变得很容易完成，设计更为精巧的系统成为可能。
2) 计算机网络中数据的存储、传输和数据处理的激增，对有效的加密及相关技术提出了新的要求。
3) 当然，这也使密码分析攻击变得很容易。所以，可能以前只有小孩或者间谍才感兴趣的问题，而现在却有很多人感兴趣。

这是一门应用数学的学科，在以往我们所接触的数学绝大部分都是由应用来推动的。在这里，我们将要接触的有：数论、线性代数、抽象代数、概率论、复杂度理论和其他一些数学知识。当然，我们在本书中不可能把所有的理论一一细述，但会介绍一些和本书相关的知识。

当然，在本书中我们也没有足够的篇幅把有关密码学的历史演变和现在的发展完整地讲述一遍。我们只会给出一些具有代表性而且在密码学发展历史上比较重要的例子，并描述一下密码学发展的其他分支。

我们也不可能全面模拟现实生活中的各种有关加密的问题并进行讨论，密码分析尤其是更不可能。因为我没有实际接触过那些机器，而且，在现实生活中，无论是加密还是密码分析的模拟，都可能需要几个小时甚至几天的时间，此外还需要大量的存储空间。普通的计算机处理加密和（授权的）解密很快，而现实生活中对密码系统的攻击可能需要花费数天甚至数月的时间。

因此，我们会首先讨论一些古典的加密系统，以及这些加密系统中所使用的数学知识，甚至用来理解或者破译这些加密系统的数学知识，这是一种好的热身方式。然后我们会讨论一种现在正在使用的对称加密系统——DES(数据加密标准，Data Encryption Standard)。DES 加密算法比那些古典的加密算法要复杂得多。当然，也正是由于它的成功，目前还没出现一种好的攻击方法。DES 早在 20 世纪 70 年代中期就已经成为美国的一套加密标准(对称密码)。而且，DES 标准除了在美国以外的其他国家也得到了广泛的应用。从 DES 标准被采用至今，经过 20 多年来的密码分析考验，还没有发现它有什么致命的弱点。但现在计算机的运算速度已是远非 1976 年那时候的计算机所能比拟的，通过穷举法进行攻击已经成为可能。事实上，在 1998 年中期，美国的 EFF（Electronic Frontier Foundation）花费了 100 000 美元，用一般商用元件构造了一个 DES 破解器，这个破解器可以在两天内获得一个 DES 密钥。好在还可用 DES 做三次加密，即所谓的 3-DES 加密算法，这种算法被认为是一种比较安全的算法。然而，美国国家标准协会（National Institute of Standard）正在征集一种新的 128 位对称加密算法。迄今为止，征集还没有结束，最终被采纳的加密算法将被命名为高级加密标准(Advanced Encryption Standard，AES)[⊖]。

本书中还将讨论另外一类密码算法——非对称加密算法，又称公钥密码算法。我们将主要讨论两种公钥密码算法：一种是 RSA 算法，另外一种是 ElGamal 算法及其应用。RSA 加密算法比较简单而且也很流行，但 ElGamal 算法更适用于椭圆曲线密码。RSA 加密算法的安全性基于数学中的一个难题：大整数因式分解。ElGamal 加密算法的安全性则是基于这样一个难题：有限域中的离散对数计算（这在后面会给出具体的含义）。这两种密码体制中的任何一种加密算法都需要生成大量且很大的素数，其实这本身就是一个有趣的问题。在介绍完这两个加密算法后，我们将进一步介绍 NTRU 密码，这是一种新的密码，从数学理论上它显得更为成熟。与对称密码体制相比，非对称密码体制由于它更加依赖于数学理论的本质，似乎看上去更容易受到攻击。在这部分我们将介绍一些重要而且精妙的数学问题。

在介绍完经典问题以后，我们会专门给出一些数论的知识，这些知识和现代加密系统有

⊖ 2000 年 10 月，美国国家标准技术局选定由比利时人 Vincent Rijmen 和 Joan Daemen 设计的 Rijndael 加密算法为 AES 的惟一候选算法。2001 年已确定为美国联邦信息处理标准 FIPS190。——译者注

着很大的关系，在公钥加密体制（如 RSA 加密系统和 ElGamal 加密系统）中尤其如此。这部分将包括下面这样一些内容：

1) 公钥（非对称）密码
2) 伪随机数发生器（pRNG）
3) 协议

必要的数学知识将包括：

1) 一些数论和抽象代数的结论
2) 素性检验、因式分解及相关算法
3) 复杂度理论

我们不会过多地讨论复杂度理论，在书中我们只简单地介绍一下复杂度理论的有关指标，并且判断一些问题的复杂程度。

在这里，素数检验和整数分解是所有问题的根本，许多实际的加密算法都可以通过这些基本问题来描述。尽管有时候要解释一个完整的算法，往往还需要很多其他的知识。但是不用解释算法的实质，我们也有可能通过实验对算法的性能和准确性有一个直观的认识。

首要的基本问题就是整数模 n 的结构以及它的一般化问题，记为 $\mathbf{Z}/n$。我们需要明白，对于 n 为合数和 n 为素数时，得到的这个 $\mathbf{Z}/n$ 存在本质上的区别。

在好多高效的算法中，还有一个很重要的随机化问题。在数学中，我们可能已经习惯了每个问题都会有一个肯定的结果，即确定性。随机化可能看上去不是那么容易理解，但在许多情况下，这又恰恰是很多加密算法的重要的理论基础。那么我们直接面临的问题就是去考虑概率意义上的素性检验，比如索洛维-斯特拉森方法和米勒-罗宾方法，并证明它们真正可行。

本书中所包含的内容，可能已经超过了一学期的课程，目前书中的内容都是经过我精心筛选的。如果给一年的时间来学习这门课，可能就会比较轻松一点。

本教程在实际教学中已经使用了多次，并且都是基于这么一个前提，学生对数论、抽象代数、概率甚至密码编码都没有什么了解。密码应用总是离不开数学问题，本书则使得注重实用的人和注重理论的人都可在书中得到各自感兴趣的信息。在编写此书的过程中，我已经尽量使各章节内容相互独立，以便读者可以跳过自己不喜欢的章节，而不影响对其他章节的理解。因此，在某些章节，可能会重复出现某些知识。从教与学的观点看，适当的内容重复是一件好事。

如果把此书作为一学期的数论教材，可以跳过密码编码和计算部分，但可把这部分作为选读资料。当然，在本书中，还有很多抽象代数的知识，这些知识已经远远超过了传统的数论教程。在我为本科生讲授数论课程的时候，我总是考虑一个问题，那就是，在讲授数论的时候是将抽象代数的知识作为独立的预备知识，还是由数论的知识来引出抽象代数的知识。最后我往往会选择后者，就是在讲述数论知识的同时，我一般会附带上抽象代数，但很少会有一本教材能够符合这个要求。本书的一部分内容是我为本科生所写的讲义，在那个讲义中我将数论和抽象代数都纳入其中，并将数论作为引入抽象代数的一个具体入口，而反过来数论的一些基本结论又来源于抽象代数。在选择把此书作为数论的教程时，应该跳过前面六章的内容（前六章主要讲的是加解密的问题）。此外，还要跳过“希尔密码”这一章。有关公开密钥加密系统的章节也可以跳过，但这却是数学在通信中的主要应用之一。

此外，可以将此书作为密码学知识的简短介绍性教程（略过有关数学的知识）。为了使本书更容易理解，书中在涉及到数学知识的时候，一般只提到一些必须需要了解的知识，而且都是一些基本知识。我在编写时也力图使这些数学知识无论是从初级的观点，还是高级的观点都是容易理解的。一般来说，在遇到需要证明的时候，我们往往都对特殊情况给出初等证明，而对一般情况给出较高层次的证明。我认为在教学中，这是一种比较好的教学方法，而且我也没有在这方面吝惜时间和篇幅。另外。一些比较严格的密码学教材都有一个通病，即相关的数学知识受到了冷遇。还有一个普遍的局限就是它们总是假定读者已经具备了相当的数学功底。相比较而言，在本书中不仅为希望了解数学在密码学中如何应用的学生提供了充足的数学资源，而且还尽可能降低对数学知识的要求。因此，本书完全可以作为一本密码学导论的简明教材。从某种意义上说，这也是写作本书的初衷。

如果要把此书作为计算数论的教材，我建议读者应该把注意力集中在算法上，减少对密码学以及更多的理论数学部分的关注。在我教授这门课的过程中，我没有假定学生能够或者愿意做任何的计算机的工作，毕竟这需要 CPU 的时间。在本书中，我详细地给出了算法的描述，目的就是使其清晰易懂，但并没有给出具体的算法的伪代码或者算法的某种语言实现。我之所以这么做，很重要的一个原因就是，我希望学生至少明白算法是如何工作的，而不是简单地去执行它。我没有用专用语言写出算法的另一个原因，是因为我无意认可某种语言及其所需要的全部东西。尽管我坚决支持学生去学习如何编写程序，但不鼓励他们去研究软件包。但是，界面友好的软件包的确很容易上手。

在授课的过程中，若有些学生已经学习过概率论或者数论的知识，就可以跳过其中一些相关的章节。在本书的编写工作中，我将大量的数学知识放到了各章各节中去讲解，而不像有的教程将所有的知识放到最后的附录中。我是基于这么一种考虑，那就是，已经学过这些知识的学生可以跳过相关章节不看，而不了解这些知识的学生可以直接按着顺序阅读，无需为了看一些相关知识而前后翻个不停。这样组织也是为了各章保持独立性。

最后，我要感谢我的朋友们，他们给我的初稿提出了好多宝贵的意见，在此我特别感谢：美国艾奥瓦州立大学的 Irvin Roy Hentzel 教授、艾奥瓦大学的 Yangbo Ye、圣母玛利亚大学的 Joachim Rosenthal、密苏里大学的 Daniel Lieman、密歇根州立大学的 Jonathan Hall 等人。在我写书的这么多年中，我的学生们一直都在使用这些初稿，我要感谢这些学生，他们给我提出了很多好的建议，而且也指出了初稿中的若干问题，使本书的质量有了较大的提升。

Paul Garrett
于明尼阿波利斯，明尼苏达大学
garrett@math.umn.edu
paul.garrett@acm.org
http://www.math.umn.edu/~garrett/

引　言

密码技术的应用：以前，密码技术的最直接的目的其实就是保密。通常，保密的意思就是用加密算法将有用的消息加密，使得即便敌人窃听、截获那些加密后的消息，也很难知道原先的内容是什么。而对于那些既定的或授权的用户，获得加密消息后，可以很容易地解密出原始消息。

目前密码学的一个新应用是消息认证，而不论这个消息是否需要保密。认证的意思是，消息的接收者需要通过一种方法来确认这是合法的发送者发来的信息，或者合法的发送者发来的消息是不是已经被修改了。验证消息在中途是不是已经被修改了非常重要，这一问题也称作数据的完整性。在传输信息的过程中，如果只考虑环境中有噪声影响，而不考虑有人在窃听，则一个相对简单的校验和就足够了。但如果同时考虑到有人破坏，则要实现此功能就会比较复杂，因为设备还要检测是否存在欺骗。

此外，目前还有一种比较流行的应用，那就是签名，以前的签名都是用钢笔来签，这一般称作物理签名，而在网络通信中，这种非物理的签名叫做数字签名。

密码技术另一个不太明显的应用就是非否认问题，尽管这是签名的一个方面：必须让数字签名的签署者事后否认对此签过名成为不可能。这就引起了一个识别欺骗的问题，我们能否使欺骗变得不可能，或者使欺骗可以被检测到？后者可能更容易实现，尽管在一些场合这是不可接受的。

不经意传输：不经意传输指的是如果 Alice 传输一个秘密给 Bob，此后，Alice 就不知道 Bob 是否接收到了这个秘密（但 Bob 知道他是不是收到了）。或者还有一种可能就是，Alice 卖给 Bob 几个秘密中的一个，使得 Alice 不知道 Bob 到底买的是哪一个秘密。

例如在政治条件下，Bob 承认忽略了某些秘密是件尴尬的事情。在这种环境下，信任裁判的简单方案是不可行的。

零知识证明：零知识证明指的是这么一种协议标准，Alice 可以证明给 Bob 看，她知道一个秘密，并且不会泄漏这个秘密。一般来说，当 Alice 证明她知道秘密时，最小泄露证明将使 Alice 告知的信息极小化。欺骗应当是困难的：如果 Alice 根本就不知道秘密，那么她能够使 Bob 错误地相信她的概率应当可以忽略，并且 Bob 不能从 Alice 的证明中获得更多的信息。特别地，Bob 应当不能够（失败）向任何人证明他知道秘密。（最小泄露证明是可能的，数学或其他技术课程的学生可以联想到，他们十分确信讲课者确实知道如何证明一个定理，即便授课者没有给出更多的信息。）

术语：**密码体制或密码**指的是一个完整的过程，通过这个过程的处理，可以使得一些明文信息，对于授权用户来说，很容易理解，而对于未授权的用户，就显得很难理解。由发送者执行的**加密处理**，指的是发送者将一些明文信息通过加密算法，加密成一些对于未授权用户不可理解的信息。由合法的既定接收者执行的**解密处理**，指的是通过解密算法和密钥，把难解的信息（**密文**）恢复成原始信息（**明文**）。注：对于没有授权的用户，想通过密文而获得明文会非常的困难。在对称加密系统中，应该只有发送者和接收者**共享一个秘密**，称为**密钥**。不让窃听者知道密钥，一般来说可以很有效地阻止他们破解密文。

你现在或许会认为使所有的加密和解密处理都保密，就可以很好地保证加密系统的安全性。然而，事实并非如此，你是不是会觉得不可思议？但事实就是如此，从现在加密安全的观点来看，加密和解密算法都可以公开，只要保证加密密钥保密。这个观点有时被称为Kerckhoff **原则**，对这个原则有几个不同的看法。其中最引人注目的一个看法很简单，就是不必担心别人知道加密过程，而且设计出符合这个要求的密码体制是可能的，那么不满足这一要求的任何体制都将是不能接受的。

一种与 Kerckhoff 原则一致的看法认为，算法的标准化使得实现大规模的通信变得更加容易。我们可以这么认为，这个加密系统的工作过程对大家来说是公开的。这并不意味着就没有什么需要保密的，唯一的**秘密**就是**密钥**。因为，**密钥分配**和**密钥管理**就成为了一个很重要的问题。

尽管在通俗英语中，“code”（代码，编码）和“cipher”（密码）是同义词，但我们对它们的使用却是不同的。**代码**是利用某个字典，将英语中的词或短语变换为另一种词或短语，从而隐藏消息内容的一种方法。这种变换通常在某种程度上依赖于消息的语法和含义：比如名词和动词被识别并被转换为名词和动词。相比而言，**密码**则把消息当作**字符**流，（一个字符可能是一个字母、数字、空格或者标点符号）不去参照其任何可能的含义。还有一个类似的词，“encode”（**编码**），它指的是非隐藏目的的变换，但却是为了后来的处理更加方便。比如，在对英文加密处理之前，先要将 26 个字母 a~z 编码为数字 0~25。

古典密码学：这指的是在电子计算机出现以前已经得到应用或者已经发明的密码学理论。在二次大战中，有很多恩格码和其他机器用于实现这些加密算法。其实在那时候，那些加密系统及其加密算法已经有了很大的改变，它们的性能已经得到了很大的提高。所以，这里说的“古典”的意思，在很大程度上指的是那些相对于现代系统来说不是很好的系统（用现在的标准衡量）。

对称加密系统：这指的是在加密系统中，加密密钥中含有解密密钥的信息，或者更极端的是在系统中，加密密钥和解密密钥完全一样。这样，信息的发送者和接收者共享同一个密钥，所有的古典加密系统都是这种对称加密系统。事实上，1975 年以前，一直都只有这种加密的方法。但在 1975~1978 年的时候，Merkle 和 Hellman 提出了一种新的加密系统：**非对称密码**，在这种加密系统中，加密密钥含有很少的解密密钥的信息，反之亦然。虽然这种加密系统看上去不太可靠，但实际上它是在许多数学难题的理论基础上建立起来的，所以它的安全性可以由数学知识加以证明。而对称密码则不像非对称密码那样神秘（最近已经知道，在 Merkle 和 Hellman 提出非对称密码思想的 10 年前，英国秘密机构的研究人员已经提出了公钥密码的思想）。

对密码系统的**攻击**：指的是在不知道密钥的情况下，对一个加密系统进行攻击，以获取明文信息。一般有四种基本攻击类型：

1) **唯密文的攻击**：在这种情况下，密码分析者得到了密文片断，但是不知道任何明文，也不知道密钥。这种攻击一般又分为两种情况：一是只解密某个特殊的消息；另一种情况是，获得了密钥，然后进一步破解所有后面的加密消息。
2) **已知明文攻击**：在这种情况下，密码分析者得到了全部或部分明文，以及这些明文所对应的密文，目的是通过这些信息来判断密钥。大多数的古典加密系统最容易被这种攻击方法攻破。

3) **选择明文攻击**：在这种情况下，密码分析者可以选择一定数量的明文，并分析对应的加密，攻击目的是获得密钥。大多数的古典加密系统也很容易被这种攻击方法攻破。

4) **对加密密钥的攻击**：这是对那些由加密密钥的信息容易得到解密密钥信息的非对称加密系统而言的。目的是可以预先处理，在截获任何密文前得到解密密钥。

对攻击方法的分类并不能像其字面意思那样明确。通常，攻击者不知道整个明文，但由于特定环境的原因，攻击者可以肯定某些特定的词会在明文中出现。一个被认为会在明文的某个地方出现的词称为一个**明密对照**（crib）。直到第二次世界大战，对这种明密对照的熟练使用仍在密码分析中发挥了重要作用，但从那以后情况就有所不同了。

前面三种攻击方法是对应于对称加密系统的。在这三种攻击方法中，显然对密码分析者而言，唯密文的攻击是最难的一种攻击方法，而选择明文攻击则是最容易的一种方法。当然，任何一种加密系统都必须能够对抗唯密文攻击，因为对消息的窃听、截取是司空见惯的事情。通常，要想实施已知明文攻击或者选择明文攻击是很困难的，尽管仍有不少对这种情况老生常谈的描述。不论这种攻击的可信度如何，确实有能够对抗选择明文攻击的密码系统。结果是能否对抗选择明文攻击成为衡量一个加密系统的标准。因此，一些古典密码系统是由于不能对抗唯密文攻击而被废弃的，而事实上由现在的标准来衡量，因为它们不能对抗选择明文攻击而应当被坚决拒绝。我们还要考虑对古典密码可能实施的更加困难的唯密文攻击，这既是我们本来的目的，也是要表明一些有趣的问题。当然我们还会指出它们对已知明文攻击和选择明文攻击的脆弱性。读者应当理解，目前的标准就是：*一个密码系统应当能够对抗选择明文攻击*。

有一个词**试探性**（heuristic）我们会经常用到。对一个问题的试探性方法决不保证其是否工作或者是否正确，但却对解决问题的步骤或者什么是正确的提出了建议。在最佳情况下，这种方法可以得到验证。

术语**算法**是一个能够完全自动化（比如在计算机上编程）的计算或决策程序。一个**概率算法**则是一个不能总是正常工作或者不可能得出一个保证正确结果的算法。

我们还要指出，对于信息的度量，采用比特和字节等度量单位。一个**比特**是一个最小的度量单位，0 或 1（真或假、开或关）。有些文章中认为比特是"二进制位"的缩写，可能这也是正确的。一个**字节**指的是 8 个比特的串，但其中一位通常用作校验位（用于校验任何比特是否有错误），因此，一个字节传输的信息种类是 2^7 种而不是 2^8 种。此外 **1KB**（kilobyte）表示 1000 字节，**1MB**(megabyte)表示 1 000 000 字节，**1GB**(gigabyte)表示 1 000 000 000 字节的意思，**1TB**(terabyte)表示 1 000 000 000 000 字节等等。

在使用拉丁字母（A 到 Z 不包括发音符号）的国家，通常一个字符被编码为 0~255 之间的一个整数，即一个字节。这当中有许多是不可打印的字符或控制字符。当然还有其他字符体系，比如美国的 **ASCII 体系**是比较常用的：字符 0~9 的编码为 48~57，大写字母 A~Z 的编码为 65~90，而小写字母 a~z 的编码为 97~122，其他整数编码表示标点符号和控制字符。

Unicode 是一种针对较大字母表（象形文字系统，如汉字）的新型编码方法，通过使用两个字节来表示一个字符，这就可以提供 2^{16}=65 536 种字符编码，比单字节的 256 种字符编码有了很大的进步。

目　录