21世纪

高等院校规划教材

邓安文　编著

密码学——加密演算法

强调理论与实践相结合，注重专业技术技能的培养
引入典型工程案例，提高工程实用技术的能力

中国水利水电出版社
www.waterpub.com.cn

21世纪高等院校规划教材

密码学——加密演算法

邓安文　编著

中国水利水电出版社

内 容 提 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的特点：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。

本书配有免费电子教案，读者可以从中国水利水电出版社网站（www.waterpub.com.cn/softdown/）上下载电子教案及相关教学资源。

图书在版编目(CIP)数据

密码学：加密演算法 / 邓安文编著. —北京：中国水利水电出版社，2006
（21世纪高等院校规划教材）

ISBN 7-5084-3590-7

Ⅰ. 密… Ⅱ. 邓… Ⅲ. 密码术—高等学校—教材 Ⅳ. TN918.1

中国版本图书馆CIP数据核字（2006）第011658号

书　　名	密码学——加密演算法
作　　者	邓安文　编著
出版　发行	中国水利水电出版社（北京市三里河路6号　100044） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）63202266（总机）、68331835（营销中心）、82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京蓝空印刷厂
规　　格	787mm×1092mm　16开本　14.25印张　348千字
版　　次	2006年3月第1版　2006年3月第1次印刷
印　　数	0001—5000册
定　　价	22.00元

序

随着计算机科学与技术的飞速发展，计算机的应用已经渗透到国民经济与人们生活的各个角落，正在日益改变着传统的人类工作方式和生活方式。在我国高等教育逐步实现大众化后，越来越多的高等院校会面向国民经济发展的第一线，为行业、企业培养各级各类高级应用型专门人才。为了大力推广计算机应用技术，更好地适应当前我国高等教育的跨跃式发展，满足我国高等院校从精英教育向大众化教育的转变，符合社会对高等院校应用型人才培养的各类要求，我们成立了“21 世纪高等院校规划教材编委会”，在明确了高等院校应用型人才培养模式、培养目标、教学内容和课程体系的框架下，组织编写了本套“21 世纪高等院校规划教材”。

众所周知，教材建设作为保证和提高教学质量的重要支柱及基础，作为体现教学内容和教学方法的知识载体，在当前培养应用型人才中的作用是显而易见的。探索和建设适应新世纪我国高等院校应用型人才培养体系需要的配套教材已经成为当前我国高等院校教学改革和教材建设工作面临的紧迫任务。因此，编委会经过大量的前期调研和策划，在广泛了解各高等院校的教学现状、市场需求，探讨课程设置、研究课程体系的基础上，组织一批具备较高的学术水平、丰富的教学经验、较强的工程实践能力的学术带头人、科研人员和主要从事该课程教学的骨干教师编写出一批有特色、适用性强的计算机类公共基础课、技术基础课、专业及应用技术课的教材以及相应的教学辅导书，以满足目前高等院校应用型人才培养的需要。本套教材消化和吸收了多年来已有的应用型人才培养的探索与实践成果，紧密结合经济全球化时代高等院校应用型人才培养工作的实际需要，努力实践，大胆创新。教材编写采用整体规划、分步实施、滚动立项的方式，分期分批地启动编写计划，编写大纲的确定以及教材风格的定位均经过编委会多次认真讨论，以确保该套教材的高质量和实用性。

教材编委会分析研究了应用型人才与研究型人才在培养目标、课程体系和内容编排上的区别，分别提出了 3 个层面上的要求：在专业基础类课程层面上，既要保持学科体系的完整性，使学生打下较为扎实的专业基础，为后续课程的学习做好铺垫，更要突出应用特色，理论联系实际，并与工程实践相结合，适当压缩过多过深的公式推导与原理性分析，兼顾考研学生的需要，以原理和公式结论的应用为突破口，注重它们的应用环境和方法；在程序设计类课程层面上，把握程序设计方法和思路，注重程序设计实践训练，引入典型的程序设计案例，将程序设计类课程的学习融入案例的研究和解决过程中，以学生实际编程解决问题的能力为突破口，注重程序设计算法的实现；在专业技术应用层面上，积极引入工程案例，以培养学生解决工程实际问题的能力为突破口，加大实践教学内容的比重，增加新技术、新知识、新工艺的内容。

本套规划教材的编写原则是：

在编写中重视基础，循序渐进，内容精炼，重点突出，融入学科方法论内容和科学理念，反映计算机技术发展要求，倡导理论联系实际和科学的思想方法，体现一级学科知识组织的层次结构。主要表现在：以计算机学科的科学体系为依托，明确目标定位，分类组织实施，兼容互补；理论与实践并重，强调理论与实践相结合，突出学科发展特点，体现

学科发展的内在规律；教材内容循序渐进，保证学术深度，减少知识重复，前后相互呼应，内容编排合理，整体结构完整；采取自顶向下设计方法，内涵发展优先，突出学科方法论，强调知识体系可扩展的原则。

本套规划教材的主要特点是：

（1）面向应用型高等院校，在保证学科体系完整的基础上不过度强调理论的深度和难度，注重应用型人才的专业技能和工程实用技术的培养。在课程体系方面打破传统的研究型人才培养体系，根据社会经济发展对行业、企业的工程技术需要，建立新的课程体系，并在教材中反映出来。

（2）教材的理论知识包括了高等院校学生必须具备的科学、工程、技术等方面的要求，知识点不要求大而全，但一定要讲透，使学生真正掌握。同时注重理论知识与实践相结合，使学生通过实践深化对理论的理解，学会并掌握理论方法的实际运用。

（3）在教材中加大能力训练部分的比重，使学生比较熟练地应用计算机知识和技术解决实际问题，既注重培养学生分析问题的能力，也注重培养学生思考问题、解决问题的能力。

（4）教材采用“任务驱动”的编写方式，以实际问题引出相关原理和概念，在讲述实例的过程中将本章的知识点融入，通过分析归纳，介绍解决工程实际问题的思想和方法，然后进行概括总结，使教材内容层次清晰，脉络分明，可读性、可操作性强。同时，引入案例教学和启发式教学方法，便于激发学习兴趣。

（5）教材在内容编排上，力求由浅入深，循序渐进，举一反三，突出重点，通俗易懂。采用模块化结构，兼顾不同层次的需求，在具体授课时可根据各校的教学计划在内容上适当加以取舍。此外还注重了配套教材的编写，如课程学习辅导、实验指导、综合实训、课程设计指导等，注重多媒体的教学方式以及配套课件的制作。

（6）大部分教材配有电子教案，以使教材向多元化、多媒体化发展，满足广大教师进行多媒体教学的需要。电子教案用 PowerPoint 制作，教师可根据授课情况任意修改。相关教案的具体情况请到中国水利水电出版社网站 www.waterpub.com.cn 下载。此外还提供相关教材中所有程序的源代码，方便教师直接切换到系统环境中教学，提高教学效果。

总之，本套规划教材凝聚了众多长期在教学、科研一线工作的教师及科研人员的教学科研经验和智慧，内容新颖，结构完整，概念清晰，深入浅出，通俗易懂，可读性、可操作性和实用性强。本套规划教材适用于应用型高等院校各专业，也可作为本科院校举办的应用技术专业的课程教材，此外还可作为职业技术学院和民办高校、成人教育的教材以及从事工程应用的技术人员的自学参考资料。

我们感谢该套规划教材的各位作者为教材的出版所做出的贡献，也感谢中国水利水电出版社为选题、立项、编审所做出的努力。我们相信，随着我国高等教育的不断发展和高校教学改革的不断深入，具有示范性并适应应用型人才培养的精品课程教材必将进一步促进我国高等院校教学质量的提高。

我们期待广大读者对本套规划教材提出宝贵意见，以便进一步修订，使该套规划教材不断完善。

21 世纪高等院校规划教材编委会

2004 年 8 月

前　言

胜利是属于“公理正义”的一方。在历史长河中，取得战争胜利的一方，往往取得历史的“解释权”，他们的意识形态就理所当然地成为所谓的“主流价值观”，因此，胜利者会被“解释”成“公理正义”的一方，而失败者会被无情地“污名化”、“妖魔化”。一般而言，胜利是属于“掌握优势资源”的一方，这些优势资源包括了军事力量、先进科技、生产技术等等，同时也包括了为人讳言的“密码技术”。

二次世界大战中，日本海军联合舰队可以说是当时世界上最强的舰队，而美国在珍珠港战役之后，海军实力已处于劣势。然而，美国却能破译日本的密码，在一连串所破译的密电中，显示出了日本海军大将山本五十六的行踪以及联合舰队的动向，使美国能够在山本五十六飞往所罗门群岛途中将其狙杀，并以劣势兵力赢得中途岛海战，这是整个太平洋战役的转折点。

勿庸置疑，密码学的确是一门实用的科学；从以往王侯将相用来对他们所发布的信息加密，到今日的电子商务、“自然人认证”、网络安全等，其中所用的核心技术就是密码学。

谈到当代密码学的核心，我们就不可避免地要了解当代密码系统的运作机制；要想对其安全性评估，就不可避免地要了解密码系统的算法；如果只是将密码系统算法轻描淡写，或只是套用一些专业术语，充其量只能是“按图索骥”，对于使用密码学技术不会有实质性的帮助。因为任何密码学所能提供的安全保证，不是建立在“入侵者无知”的假设上，其所要面对的是精通各类信息技术、了解密码系统算法的超级骇客。

诚然，信息安全的漏洞，往往不是发生在所用的密码算法上，而主要是由系统管理员造成的；也许密码系统程序员能够遵循密码学算法，编写一份近乎“完美无缺”的系统，却可能忽略了运行系统随机产生的软硬件问题；有时甚至所使用的密码学产品本身就是泄密机。即使是以当代密码机 RSA、DES、Triple DES 为加密系统的“保健 IC 卡”或是“自然人认证”，都曾发生过资料保密上的纰漏，被人视为近乎“完美无缺”的系统，却无法保证非密码层面不出问题。

本书并不想对整个信息安全的大架构进行讨论，因为除了理论上的探讨外，必须很实际地，从管理层面探讨，这并非单从算法、协定中能解释清楚的，这是大师级的工作，绝非笔者所长，但是当代密码学各类算法，有精确的数学描述方式，可以将其程序化，并将这些内容列入教材，成效会丰常显著。

一个成熟耐用的密码系统，首先要有能经得起严谨理论考验的算法。综观当代密码系统，主要可分为公开密钥密码系统（Public Key Cryptosystem）以及对称密钥密码系统（Symmetric Key Cryptosystem）两类。以前者为代表的有 RSA、ElGamal、椭圆曲线密码系统，而以后者为代表的有 DES、AES 等。这些密码系统，都要用到一些数学上的概念，而用到最多的数学相关知识，是被数学王子高斯誉为“数学女王”、被人们视为最冷门的“数

论”（Number Theory）；由于真正“了解内情”的人实在不多，所以用当代密码技术为幌子行骗的空间很大，鉴于此，笔者特将相关的基础数论内容列入本书，其实就是大学“代数”以及部分“质数”理论，这些内容都是研究当代密码学的基础。

由于当代密码技术的应用已经不是只在“纸上谈兵”而已，必须依赖程序应用。所以在本书编排上，特别用类似 C/C++/Java 的语法，对部分已成熟的算法写成伪码，只需很少的修改，就可以执行运算。对于密码算法的学习，有相当的帮助。

尽管古典密码早已不符合当代信息安全的需求，但就其中所带来的益智性乐趣，笔者实在不想只是轻描淡写；就二次大战期间德国人所用的 Enigma 密码机而言，除了历史上的乐趣外，其中的加密解密运算，其实就是对称群的置换作用，就如同转动魔方一样，是绝佳的“群”作用范例，令人着迷不已。

记得 1998、1999 年冬天，曾与 RSA 的 A 合作过的黄明德在台湾大学讲述他的一系列工作，在那时笔者领略到高深的“数论”以及“代数几何”应用到密码学的研究是深邃而引人入胜的。

本书在撰写中，费时最久的是书中的每个例题，这些例题，除了少数参考了其他文献外，大多数都是程序执行的结果整理而成，部分也取自笔者的研究内容。

另外，本书部分内容，如 RSA 密码、非对称密钥密码与离散对数、数字签名以及部分古典密码的介绍，都是笔者在清云科技大学教授“密码学”、“公开钥密码系统”时讲授过的。笔者所指导的专题学生，也分别以“RSA 电子投票研究”、“保健 IC 卡研究”、“RSA 与 PGP 研究”当作专题研究方向，专题学生林俊余与黄明宗等人，也做出以 Java 撰写的 RSA 为基础的“电子投票系统”的半成品，虽然离成熟产品还有很大距离，但也属难能可贵。感谢这些专题学生林俊余、林罔永、许丰琳、杨贺杰、黄明宗、徐效群、林克儒、陈惠甄、陈华君、陈丽君、陈俞婷、李建志、潘丹尼、吴英绮的热心参与，使得笔者在密码学的授课以及学生研究会讨论过程中，增加不少互动。所谓“教学相长”，这对本书的撰写也有一定的帮助。

在本书即将完成之际，笔者仍发现密码学实在涉略广大，许多内容只好忍痛割舍，限于各种因素，无法面面俱到，作为教材不免有遗珠之憾。

特别感谢（台湾）中央研究院数学所谢春忠教授对本书算法及算式逐一检查校阅。感谢中央研究院数学所提供笔者短期访问的机会，不少研究密码学的相关文献资料，都是在此取得。更感谢清云科技大学的系主任李振焘教授及系同事的支持与协助。另外在 Lilie 的协助下，本书也加上了“福尔摩斯密码”一节，替本书增色不少。

本书部分函数图形由数学软件 Mathematica 产生，部分精美的图案由全华科技图书绘制而成。感谢 Bletchley Park Trust 所提供的珍贵照片及 Sue May 的协助，也感谢 Brian Smith 的居中联络。

邓安文

本书的繁转简工作由李强、方春明、郝思嘉、李鑫、黄浩、王晓青、马路、王成博、王艳等人完成，在此对他们的工作表示感谢。

目　　录

第 1 章　绪论

密码学（Cryptology，Cryptography）是指秘密书写、加密信息、隐藏信息内容的科学，同时也泛指与密码有关的科学。人类文明史本是尔虞我诈、纷争不断，自从发展大规模战争以来，密码的使用层出不穷。如罗马共和国时代的执政官凯撒（GaiusJuluis Caesar，公元前 100 年到公元前 44 年），就多次使用一种字母替代密码，称为恺撒挪移码（Caesar Shift Cipher）。二次世界大战中，因为盟军及时有效地破译了德国的 Enigma 密码机，至少挽救了百万生灵免受涂炭。二战后英国接收了为数众多的 Enigma 密码机当作战利品，多数卖给了英联邦成员国，这些英联邦成员国都相信这些德国货真能保密，这使得 Enigma 密码机成了为英国提供各国机密的一个渠道。

密码学的应用已经不再局限于“军国大事”了，虽然密码学的相关研究仍以负责“国家安全”的研究单位为主，这些研究单位拥有大量的研发人力资源（至少西方国家如此）。与大多数学科不同的是，密码学的许多研究成果是不公开的、也不希望被外界披露，密码技术的输出更受到严格管制，这也使得密码学的研究蒙上了神秘色彩。随着近十年 Internet 网络的发展，电子商务的开展、IC 卡的使用，都必须依赖可靠的通信安全，以防止怀有恶意的第三者——如骇客（Hacker）入侵，而密码学也因此成为大众科学。加上近来政府大力推广密码学技术，如电子公文交换系统、保健 IC 卡、身份证甚至将来可能面临使用的电子投票等；业界更是大力推销密码产品，好像不买不安全，买了就有了保障，这些密码学技术多半来自于所谓的“密码技术先进的国家”，大多数使用者不了解也无从检验其安全性。这些密码技术、密码商品是否真如推销者所言，还是另有玄机？

1995 年，德国的明镜杂志（Der Spiegel）以及美国的 Baltimore Sun 都报道了位于瑞士的一家著名密码公司 Crypto AG 在他们的部分密码商品上加了后门，并提供美国国家安全局（National Security Agency，NSA）后门细节，客户资料可由此后门窃取，这件事在当时举世哗然。

密码学的应用也早已超越单纯的信息安全的领域，逐渐渗透到我们的日常生活当中。可以确定的是，我们逐渐生活在一个密码技术的年代，希望这些密码技术真正能保障各种隐私，而不是以密码技术为幌子的加上后门的“特洛伊木马”来服务某些人，否则电影“全民公敌”的故事情节将会以密码技术为包装重演。

1.1　通信安全

密码学的核心就是密码加密方法，而每种密码法都可视为某种加密法，即算法（Algorithm）加上密钥（Key）的组合。加密解密的场景（Scenerio）如图 1-1 所示。

- Alice 为传递信息者即加密者，将明文（Plaintext）加密成密文（Ciphertext）。
- Bob 为接收信息者即解密者，将密文解密成明文。
- Eve 为敌对的第三者，它在传递信息的过程中截收密文。

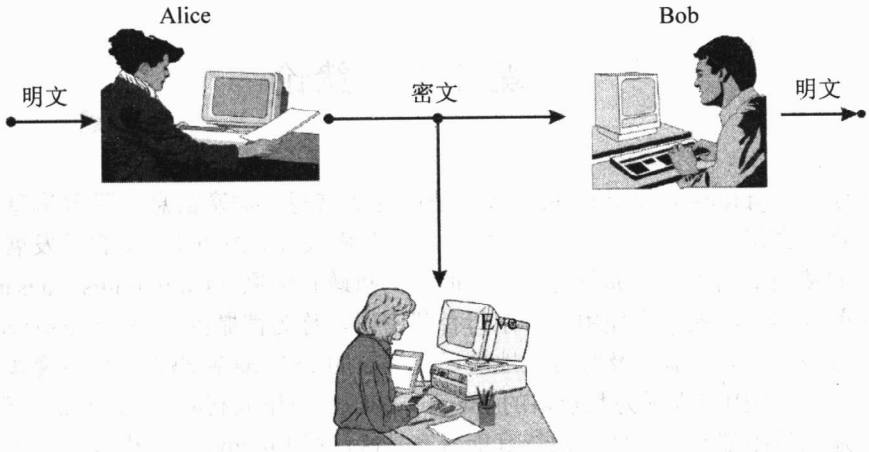

图 1-1 通信场景

Eve 可能会有以下目的：

（1）阅读密文。

（2）找出密钥，解读密文。

（3）篡改或修改 Alice 传给 Bob 的信息。

（4）假扮成 Alice，与 Bob 传递信息，让 Bob 误认为他还是与 Alice 通信。

若 Eve 只是阅读密文，似乎是无害的，而上述其他可能性的发生都来自于 Eve 的意愿和他分析密码的技术能力问题。可以依据 Eve 对信方式和密码系统掌握的程度，将攻击方式分为如下几类：

（1）破译密文层次的攻击方式。

- 密文攻击（Ciphertext-Only Attack）：Eve 只知道密文，尝试恢复成相应明文，或者找出密钥。
- 明文攻击（Known-Plaintext Attack）：Eve 知道至少一组明文/密文对照文，尝试找出密钥，或者尝试破译解读其他密文。
- 选择明文攻击（Chosen-Plaintext Attack）：Eve 能够将明文编译成密文，但不知道密钥，尝试找出密钥，或者破译解读其他密文。
- 选择密文攻击（Chosen-Ciphertext Attack）：Eve 能够将密文破译成明文，但不知道密钥，尝试找出密钥。

（2）主动式攻击（Active Attack）方式。这一大类的攻击方式有时也需要先进的硬件设备，也包括篡改信息、假扮传讯者的攻击方式，广义地说，也包括即时攻击（Timing Attack）和贿赂对方人员等。比如所谓的暴风雨攻击（Tempest Attack），就是指在 Alice 完成密文编译之前，Eve 能侦测出 Alice 电脑输入的明文的每一字母所发出的特有电磁波信息。

例 1.1 在第二次世界大战时，德国使用 Enigma 密码机，同盟国破译的攻击方式属于明文攻击。最常出现的例子就是，德国每天的气象报告的密电，将德文的气象信息，在密电中编译成密文，如此只要找出足够多明文/密文对照文，加以分析后就能破译出当日德国所使用的密钥。

例 1.2 在密文攻击中，若采取对所有可能的密钥进行检试，这种方法称为穷举法攻击

（Exhaustive Attack），或称为暴力攻击（Brute-Force Attack）。比如说密码 DES 的密钥有效长度为 56bit，一次所有可能的密钥数为 2^{56}，暴力攻击成功的可能性还是有的。

在现代密码学中，针对信息保密有一个非常重要的假设，即 Kerckhoffs 原理。

Kerckhoffs 原理：应该假设敌人已经知道所使用的密码系统的保密方法。

因此密码系统的使用，其安全性在于密钥的保密，而假设破译者早已知道算法。今天，算法应广义地包括密码系统的加密、解密算法、所用的密码元件、所使用的协议、随机数生成器、软件硬件设备。而密码系统应对信息安全提供以下四大功能：

（1）机密性（Confidentiality）：Eve 根本无法破译解读 Alice 传给 Bob 的密文，而其主要工具就是该密码系统的加密、解密算法。

（2）数据完整性（Data Integrity）：Bob 想要确定 Alice 所传递的信息未被篡改，但在传递上也可能会出错，此时就应该考虑具有侦错功能的编码理论（Coding Theory），而密码杂凑函数，提供了可侦测数据是否遭篡改的方法。

（3）可认证性（Authentication）：Bob 希望能确定传递的信息“应该”是由 Alice 本人所发送的，而非他人所伪造。

（4）不可否认性（Non-Repudiation）：Alice 不能否认是她所发送的信息。

可认证性与不可否认性似乎是相近的概念，但相互之间仍有区分：以传统的对称密钥密码（Symmetric Key Cryptosystems）为例，Alice 与 Bob 共同使用一把相同密钥对此对称密钥密码加密解密，在 Bob 收到密文之际，就假设除了 Bob 之外只有 Alice 知道密钥，因此密文应该是 Alice 传送的，而非他人伪造，因此可认证性自然成立；但在有争议时，Alice 否认是她发送这份信息的，因为不排除 Bob 也将密钥告诉了第三者，或伪造密文，两方各执一辞，因此不可否认性在此不可能实现。此时，不可否认性的解决方案，必须借助于公开密钥密码系统（Public Key Cryptosystem），如数字签名（Digital Signature）。不可否认性排除了 Alice 寻找不在场证明（Alibi）的可能性，这为电子商务，特别是网络交易提供了重要的安全功能。

如何界定一密码系统的安全程度？我们先讨论以下术语。

定义 1.1　一个密码系统为无条件安全（Unconditionally Secure）就是指即使接收到无限密文，也无法确定其密钥。

定义 1.2　一个密码系统为计算上安全（Computationally Secure）就是指该密码系统满足破解密文的花费远远大于所加密信息的价值，且破解密文所花费的时间远远多于该信息的有效时间。

定义 1.3　一个密码系统为可证明安全（Provable Secure）就是指该密码安全性问题可转化成某个研究人员公认的困难问题。

事实上，一个密码是无条件安全的，只有在密文的长度与密钥的长度大致相同时，才会成立，在实际上，只有单次密码本（One-Time Pad）才是无条件安全的，其他的都不是。而公开密钥密码系统 RSA，是可证明安全的，因为该密码系统的安全性问题，在大量的研究下，一般可转化成质因数解分的问题，而质因数分解的问题，一般认为是很困难的。事实上，能将密码的安全程度量化，关键就在计算上安全这个概念；这与度量某一个算法的时间与存储空间的计算复杂度（Computational Complexity）有直接关联。

例 1.3　函数 $4n^2+7n+12$ 的数量级为 n^2，通常用大写“O”或小写“o”表示为

$$4n^2+7n+12=O(n^2) \text{ 或者 } 4n^2+7n+12=o(n^3)$$

定义 1.4　令 f、g 为 n 的函数，

$$f(n)=O(g(n)) \Leftrightarrow \lim_{n\to\infty}\frac{|f(n)|}{|g(n)|}<c$$

对某正数c成立，则

$$f(n)=o(g(n)) \Leftrightarrow \lim_{n\to\infty}\frac{|f(n)|}{|g(n)|}=0 。$$

另外，信息时代常用的单位 MIPS（One-Million-Instruction-Per-Second，1 秒执行一百万次命令），20 年前的计算机 VAX-11/780 就大约是 1 MIPS 计算机，1 MIPS 计算机在一年约可执行 3×10^{13} 次指令，而 100 MHz Pentium 计算机是 50MIPS 计算机，运行大约是 VAX-11/780 的 50 倍，而 1GHz Pentium 计算机的运行速度 500MIPS。单位“MIPS 年”是指 1 MIPS 电脑在一年内所执行指令的次数，也可看作时间单位。表 1-1 所示为不同数量级算法处理 $n=10^6$ 在 1MIPS 电脑所需的时间。

表 1-1 算法处理 $n=10^6$ 在 1MIPS 电脑所需的时间

算法	计算复杂度	所需运算次数	1MIPS 电脑执行时间
常数	O(1)	1	1 μsec
线性	O(n)	10^6	1 sec
平方	$O(n^2)$	10^{12}	11.6 天
立方	$O(n^3)$	10^{18}	32000 年
指数	$O(2^n)$	10^{301030}	10^{301017}

例 1.4 RSA 密码系统是可证明安全的，该密码系统可转化成质因数分解的问题，以目前的代数域筛法（Algebraic Number Field Sieve Method）算法尝试破解，对于不同的 RSA 密钥长度，其运算次数如表 1-2 所示。

表 1-2 使用代数域筛法分解不同密钥长度的 RSA 模数的运算次数

RSA 密钥位数	MIP 年
512	8400
768	5×10^7
1024	6×10^{10}
2048	7×10^{19}
3072	3×10^{26}
4096	6×10^{31}

注意： 许多对称密钥密码以及所有的公开密钥密码系统皆可在 NP 时间内破解。[注[1]]

注[1] NP（Nondeterministc Polynomial）问题是指在 Nondeterministc Turing 机上所需多项式时间方可破解，即 $O(t^m)$时间 ($m\in R$)。而 Nondeterministc Turing 机器只指一有限状态机可作无限多次读写动作，且可平行尝试所有的猜想，并需多项式时间可破解，而与现在计算机较为相近的是 Nondeterministc Turing 机，有关此问题，可参阅：Daniel I.A.Cohen，“*Introduction Theory*”，Second Edition，John Wiley &Sons，Inc.（1997）

1.2　公开密钥密码系统与对称密钥密码系统

定义 1.5　考虑 Alice 传信息给 Bob，如图 1-2 所示。

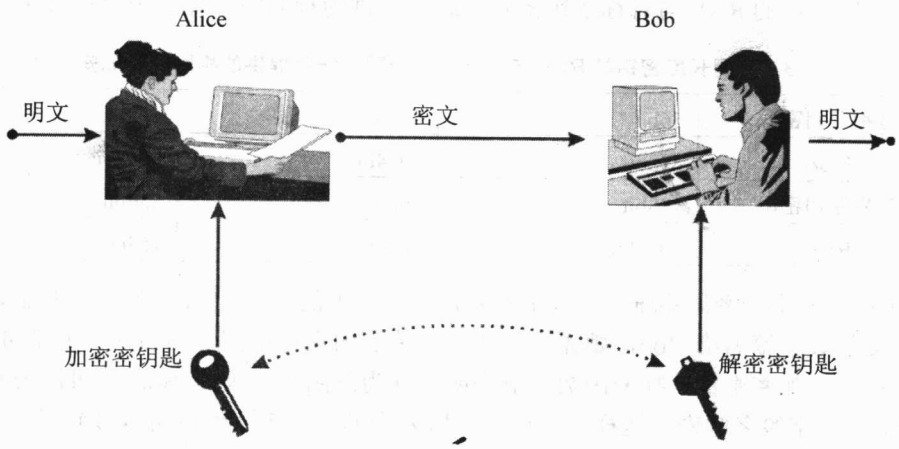

图 1-2　对称密钥/公开密钥密码系统

- 一密码系统为对称密钥密码系统（Symmetric Key Cryptosystem）
  ⇔ 其加密密钥=解密密钥，钥匙是保密的。
- 一密码系统为非对称密钥密码系统（Asymmetric Key Cryptosystem）
  ⇔ 其加密密钥≠解密密钥
- 一密码系统为公开密钥密码系统（Public Key Cryptosystem）
  ⇔ 其加密密钥≠解密密钥，且加密密钥为公钥（Public Key）而解密密钥为私钥（Private Key）

由此定义可知，所有的公开密钥密码系统都是非对称密钥密码系统，与对称密钥密码系统没有交集；另有一种称为 Pohlig-Hellman 的密码系统，它是非对称密钥密码系统，但不是公开密钥密码系统，它的加密密钥及解密密钥皆保密的。对称密钥密码系统包含所有传统的加密系统，如古代的凯撒挪移码、Viginere 码、单次加密簿以及二次大战所采用的 Enigma 密码机和战后计算机发明后所广为采用的 DES，及新的加密法 AES、IDEA 等。而公开密钥密码系统则有 RSA 密码、将 Diffie-Hellman 密钥交换加以推广的 Elgamal 密码、椭圆曲线密码（Elliptic Curve Cryptosystems）以及大多数的数字签名（Digital Signature）算法。

对称密钥密码系统与公开密钥密码系统在实际应用上有什么优劣？在不同的要求上有何特性？

（1）对称密钥密码系统一般而言，其运算的速度远远快于公开密钥密码系统，这在大批数据加密上有其实用价值，如 DES 的加密解密速度就比 RSA 密码系统快千倍以上。

（2）公开密钥密码系统的密钥长度可根据需求而增长，不像对称密钥密码系统的密钥长度是固定的，如对称密钥密码系统 DES 的密钥为固定的 56bit，AES 的密钥为固定的 128bit，192bit 和 256bit 三种，而公开密钥密系统 RSA 的密钥为 512bit，甚至可依据需求而增长，从而增加计算安全度，故拥有长密钥的 RSA，其计算安全度要远远高于 DES。通常，对称密钥

密码系统是以暴力攻击估计其计算安全度，所以它的计算复杂程度为指数函数 $O(2^n)$，其中对称密钥密码系统的密钥为 nbit；而 nbit 密钥的公开密钥密码系统 RSA 是以代数域筛法攻击估计其计算安全度的，其计算复杂度为亚指数（Subexponential）函数

$$e^{(1.923+o(1))(\ln n)^{1/3}(\ln\ln n)^{2/3}} = e^{O(e^{1/3}(\ln e)^{2/3})}$$

不同长度密钥的 RAS 与对称密钥密码系统所提供的相同的计算安全度如表 1-3 所示。

表 1-3 不同长度密钥的 RSA 与对称密钥密码系统所提供的相同的计算安全度

对称密钥密码	56bit	80bit	112bit
RSA	512bit	1024bit	2048bit
对称密钥密码	128bit	192bit	256bit
RSA	3072bit	7680bit	15360bit

（3）在公开密钥密码系统中，数字签名是可以实现的，以 RSA 为例，其方法如下：Alice 要对一个文件数字签名给 Bob，她先用私钥对要签名的文件加密，因为任何人都可取得 Alice 的公开密钥，即加密密钥，加密函数与解密函数互为反函数，因此 Bob 就可用公开密钥对已加密的 Alice 数字签名解密，这样，通信安全所要求的不可否认性就可以做到了。

（4）在实际应用中，所使用的加密软件大都是将对称密钥密码系统与公开密钥密码系统整合而成，如 PGP 电子邮件加密软件的早期版本[注[2]]，就使用了公开密钥密码 RSA 以及对称密钥密码系统 IDEA，分别在加密的速度上以及通信安全加以考虑，以 RSA 加密传送 IDEA 的密钥，而内文加密采用 IDEA，这样，加密速度与通信安全性得以兼顾，并能解决分配密钥的问题。

公开密钥密码系统的发展是比较短的，最早所思考的问题，是对传统对称密钥密码系统的密钥分配问题。考虑在一庞大的机构中，任何两人都可彼此利用对称密码加密解密信息，这导致密钥的总数相当庞大且不易管理；而公开密钥密码系统的概念大大简化了密钥的管理问题，在 1976 年 Diffie 与 Hellman 就提出一篇划时代的文章[注[3]]，其中提出公开密钥密码的概念，如单向陷门函数（Trapdoor One-way Function）等；而在 1977 年由 Rivest、Shamir、Adleman 所提出的一种加密法，即后来的 RSA 密码，在密码学的发展上起了根本的变化，公开密钥密码系统终于产生了。

注[2] 读者可以到http://www.pgpi.org 下载 PGP电子邮件加密软件。

注[3] Diffie and Hellman，“New directions in cryptography.” IEEE Trans.Inform Theory IT-22 P.644654,1976。

第2章　古典密码

近代密码技术必须在计算机上运行，而人类使用密码却已经有几千年的历史，使用密码的目的，就是不让敌方或不该知道信息内容的人知道信息内容。对使用汉字的中国人而言，很早就有妇女们所使用的“女书”，对于不该知道内容的男人而言，这就是一种密码技术。而西方使用字母拼音文字的民族，早期的密码技术主要以字母的代替（Substitution）以及字母的位移（Transposition）为主，有时也混合代码法代替整个单字或词组。

在中世纪的伊斯兰国家，学者致力于研究可兰经，甚至分析了经文每个不同字词及字母的出现频率；当时的伊斯兰国家正处于高度文明的时期，数学与语言学都处于很高水平，这也为密码分析学（Cryptanalysis）提供了可能的环境。在欧洲还处于黑暗时期时，远在中东与近东的回教徒早已熟悉用（Frequency Analysis）频率分析破译的单套字母代替密码；简单的单套字母替代密码在频率分析未发明之前如同无字天书，但在频率分析破译法产生后破译起来就易如反掌了。

16 世纪，一种名为 Vigenere 密码的多套字母替代密码诞生了，这在当时被视为无法破译的密码，一直到了 19 世纪才被破译，而破译的方法仍是以频率分析为主。

人类在这个时期，破译密码的技术要高于编译密码的技术。欧洲列强矛盾冲突引发了的第一次世界大战，密码学家此时无法提供高明的密码编译方法，只不过是将多套字母替代与位移结合产生密码，如 Playfair 或 ADFGVX 被勉强使用，除了刚出炉之际还可以应付一下，接下来就是等着对方密码分析师应用频率分析法破译。如此应急式的密码，再加上在当时防御武器优于进攻武器的情况下，任何“早已被破译的”进攻战计划岂有不败之理。

密码技术在此时的发展，实在令人沮丧，但一种真正无法破译的密码单次密码本（One-Time Pad）在战争末期发明了，值得一提的是，冷战时期，美苏之间领导人的热线就使用这种方式加密。然而此类密码法所需成本极高，每加密一次就要用不同的密钥，这在军事应用上尤其困难，故无法大量使用。

古典密码发展的最后一个阶段，应是二次大战前后所使用的滚轮（Rotor Machine）编码，最著名的应属德国所采用的 Enigma 密码机，拥有如同天文数字的密钥数量，这是无法用传统的频率分析法破译的，然而在德国发动战争之前，被波兰密码分析师破译成功，随着战争爆发，德国继续加强他们的密码机，这项破译技术也适时地转移到英国，Bletchley Park 的密码分析师继续试图破译德国的密码机，借助他们所制造的机器，对所截收密码的分析结果进行计算对比，而这种用来协助破译密码的机器 Colossus，就是计算机的前身。由于密码分析的需求，人们发明了计算机来对付机械密码机，而在计算机发明之后，人们又利用它发展更新、更强的当代密码技术。

在本章中，我们将讨论古典密码及其破译技术，所讨论的纲要如下：

- 凯撒挪移码。
- 仿射密码。
- 单套字母替代法与频率分析。