21世纪高等学校计算机规划教材

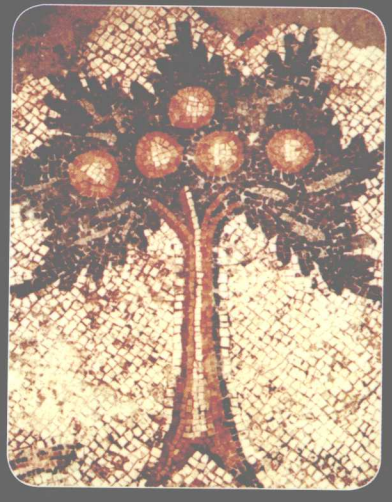
21st Century University Planned Textbooks of Computer Science

现代密码学

Modern Cryptography

何大可 彭代渊 唐小虎 何明星 梅其祥 编著

- 经典密码学内容
- 更强调网络背景
- 概念清楚、论述严谨
- 例题、习题丰富



名家系列

人民邮电出版社
POSTS & TELECOM PRESS

21世纪高等学校计算机规划教材

21st Century University Planned Textbooks of Computer Science

现代密码学

Modern Cryptography

何大可 彭代渊 唐小虎 何明星 梅其祥 编著

名家系列

人 民 邮 电 出 版 社

北 京

图书在版编目（CIP）数据

现代密码学 / 何大可等编著. —北京：人民邮电出版社，2009.9
21世纪高等学校计算机规划教材
ISBN 978-7-115-21157-6

Ⅰ. 现… Ⅱ. 何… Ⅲ. 密码－理论－高等学校－教材
Ⅳ. TN918.1

中国版本图书馆CIP数据核字（2009）第144326号

内 容 提 要

本书系统地讲述了密码学的基础理论与应用技术。主要内容包括密码学的信息论基础、密码学的复杂性理论、流密码、分组密码、公钥密码、Hash 函数、数字签名、密码协议和密钥管理。本书内容丰富，取材经典、新颖，概念清楚，各章后面配有大量习题。

本书可作为高等院校信息安全、通信工程等相关专业本科生的教材，也可供研究生与相关技术人员学习参考。

21 世纪高等学校计算机规划教材

现代密码学

◆ 编　　著　何大可　彭代渊　唐小虎　何明星　梅其祥
责任编辑　邹文波

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市海波印务有限公司印刷

◆ 开本：787×1092　1/16
印张：13.25
字数：344 千字　　2009 年 9 月第 1 版
印数：1－3 000 册　　2009 年 9 月河北第 1 次印刷

ISBN 978-7-115-21157-6

定价：24.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154

出版者的话

计算机科学与技术日新月异的发展，对我国高校计算机人才的培养提出了更高的要求。许多高校主动研究和调整学科内部结构、人才培养目标，提高学科水平和教学质量，精炼教学内容，拓宽专业基础，优化课程结构，改进教学方法，逐步形成了“基础课程精深，专业课程宽新”的良性格局。作为大学计算机教材建设的生力军，人民邮电出版社始终坚持服务高校教学、致力教育资源建设的出版理念，在总结前期教材建设的成功经验的同时，深入调研和分析课程体系，并充分结合我国高校计算机教育现状和改革成果，推出“推介名师好书，共享教育资源”的教材建设项目，出版了“21世纪高等学校计算机规划教材”名家系列。

本套教材的突出特点如下：

（1）作者权威 本套教材的作者均为国内计算机学科中的学术泰斗或高校教学一线的教学名师，他们有着深厚的科研功底和丰富的教学经验。可以说，这套教材汇聚了众师之精华，充分显示了这套教材的格调和品位。无论是刚入杏坛的年轻教师，还是象牙塔内的莘莘学子，细细品读其中的章节文字，定会受益匪浅。

（2）定位准确 本套教材是为普通高等院校的学生量身定做的精品教材。具体体现在：一是本套教材的作者长期从事一线科研和教学工作，对高校教学有着深刻而独到的见解；二是本套教材在选题策划阶段便多次召开调研会，对普通高校的教学需求和教材建设情况进行充分摸底，从而保证教材在内容组织和结构安排上更加贴近实际教学；三是组织有关作者到较为典型的普通高等院校讲授课程教学方法，深入了解教师的教学需求，充分把握学生的理解能力，以教材内容引导授课教师严格按照科学方法实施教学。

（3）教材内容与时俱进 本套教材在充分吸收国内外最新计算机教学理念和教育体系的同时，更加注重基础理论、基本知识和基本技能的培养，集思想性、科学性、启发性、先进性和适应性于一身。

（4）一纲多本，合理配套 根据不同的教学法，同一门课程可以有多本不同的教材，教材内容各具特色，实现教材系列资源配套。

总之，本套教材中的每一本精品教材都切实体现了各位教学名师的教学水平，充分折射出名师的教学思想，淋漓尽致地表达着名师的教学风格。我们相信，这套教材的出版发行一定能够启发年轻教师们真正领悟教学精髓，教会学生科学地掌握计算机专业的基本理论和知识，并通过实践深化对理论的理解，学以致用。

我们相信，这套教材的策划和出版，无论在形式上还是在内容上都能够显著地提高我国高校计算机专业教材的整体水平，为培养符合时代发展要求的具有较强国际竞争力的高素质创新型计算机人才，为我国普通高等教育的计算机教材建设工作做出新的贡献。欢迎各位老师和读者给我们的工作提出宝贵意见。

人民邮电出版社

前 言

密码学（Cryptology）包括密码编码学（Cryptography）和密码分析学（Cryptanalytics），后者的研究内容，也称为密码破译（Cipher-break）。密码是在非安全信道中为保证交换信息的机密性而诞生的。

人类使用密码已经有几千年了，在历史上它往往和军事、间谍等工作联系在一起。由于成功的密码编码、密码使用或密码分析，使密码工作者多次在世界军事史上留名并且影响到历史的进程。纳瓦霍语密码是密码编码的传奇；破译德国“恩尼格玛”密码和破译日本“紫密”密电是密码分析的传奇——它们已经成为脍炙人口的故事。以战争为主要驱动力的密码学，和通信理论、电子学一样在第二次世界大战后得到高度重视，随着社会日益增长的保密需求，其研究在更大范围内受到关注和支持。在近代密码学的发展史上，以下几个事件具有特殊的意义。

1949 年 C.E.Shannon 发表了“Communication theory of secrecy system”，将密码学的研究引入了科学的轨道——虽然该文在 20 多年后才得到密码学界足够的重视。20 世纪 70 年代，有两个可以称为里程碑的事件：一是美国国家标准局（NBS）正式公布实施美国数据加密标准（DES），由此导致密码的广泛商业应用和密码研究的平民化；另一个是 W.Diffie 和 M.E.Hellman 公开发表“New directions in cryptography”一文，提出了不同于传统对称密码体制的非对称密码体制或双钥密码体制——由于加密与解密密钥中的一个可以公开，所以也被称为公钥密码体制。它们是现代密码学诞生的主要标志。将公钥密码体制改用于认证时，唯一拥有秘密密钥的一方如果用该密钥加密授权书（或其压缩映像），则既定的验证者均可利用对应的公钥解密以上结果得到原来的授权书（或其压缩映像）。上述过程可以提供加密者拥有该秘密密钥的证据，同时也能达到防止他人篡改其原始文件的目的——这就是数字签名得以立法的理论基础（我国法律名为“中华人民共和国电子签名法”）。于是，利益不一致的参与者之间要求个人信誉保证的所有商务、金融活动等交易，都可能从传统的在契约上以手书签名的运作方式，转移到网络上来进行——因为数字签名可以代替手书签名甚至效果更佳，而将交易信息加密又可以保证交易的机密性。不难想象，这样的变革对人类社会的影响是多么巨大，因为需要“签署”以证明信用或便于审计的不止是商业和金融业，政府、军队也是如此。于是，电子政务、电子商务近年得以迅猛发展，事实上还包括“电子军务”。

密码编码学的任务与密码分析学的任务如同制造坚固的盾与制造锋利的矛。同古老的盾与矛一样，它们也逃不出“相互争斗，永无休止”的哲学。自然，在这里需要的不再是铁与火，而是数学、电子学、信息论、计算复杂性理论等，以及在此基础上表现出的智力、技巧、微电子制造甚至 DNA 技术，同时还需要一点谦逊、谨慎和预见——因为现实社会中参与密码搏弈的对手对其真实的密码设计水平与密码破译能力始终是秘而不宣。正因为如此，很难准确地评估各国的密码研究水平。不过，有证据表明，中国密码学研究虽然与国际领先水平有不小差

距，但并不缺少亮点。就公开的案例来讲，IDEA 的设计与流行，找出 MD5、SHA-1 等 Hash 函数的碰撞都是国际密码学界近 15 年内有代表性的成果，所以中国国内及国外的华裔密码学家在国际上得到了应有的尊重。希望中国下一代密码学研究者有更好的表现。

本书是为大学信息安全及相关专业本科生编写的。全书分为 5 个部分：第 1 部分即第 1 章，介绍密码学的基本概念和一些基础知识；第 2 部分包括第 2 章和第 3 章，介绍单钥密码体制；第 3 部分即第 4 章，介绍公钥密码体制；第 4 部分包括第 5 章和第 6 章，介绍 Hash 函数、消息认证和数字签名；第 5 部分包括第 7 章和第 8 章，介绍密码学应用中必需的密码协议和密钥管理。本书在介绍必要的基础知识的前提下，还以少量笔墨提及 AKS 素性判别法、王小云等对若干 Hash 函数的攻击、在选择密文攻击下可证明其安全性的公钥密码等内容，力图勾勒出现代密码学理论较新的概貌。密码学涉及的研究内容很广，本书只介绍主要的基本理论和技术，特别是只介绍了如今广泛应用的数字数据加密理论和技术，对于较早使用的对模拟消息直接变换置乱的加密技术并没有涉及。为了让学生能更好地理解这些基本知识或为师生提供更多的相关知识，在各章末附有难度不同的习题，供使用本书的师生选用。使用本书大致需要 54 学时，如果能再配以 1 至 2 学分的实验课则更好。

28 年前，第一作者有幸从师肖国镇教授和屈家淦教授学习密码学，并于 1989~1990 年在王育民教授指导下参与了《保密学——基础与应用》（西安电子科技大学出版社）一书的编著，受益良多。本书的编写参考了该书和此前国内外专家的众多专著，在此表示衷心的感谢。作者还要感谢本套教材编审委员会的各位专家，是他们的宝贵意见帮助作者确定了本书的章节，规范了内容选材，以及对编写时间的宽容。本书编写过程中，赖欣博士参与了统稿，张文芳博士通读了第 1 章至第 6 章书稿并且对一些笔误做了更正，余位驰博士、李国民博士、博士研究生郭伟、路献辉和硕士研究生张弦、赵洁、曹慧娟、曹杨，以及西华大学的李虓副教授在准备和校阅初稿方面提供了不少帮助，在此一并致谢！

本书前言和第 1 章由何大可执笔，第 2 章和第 3 章由唐小虎执笔，第 4 章由梅其祥执笔，第 5 章和第 6 章由彭代渊执笔，第 7 章和第 8 章由何明星执笔。全书由彭代渊统稿，何大可复核。

由于编者水平所限，书中难免存在错误之处，恳请读者批评指正！

编　者

2009 年 8 月于成都

目 录

第1章 概论

本章介绍信息安全基本概念、密码系统模型、密码体制分类、简单密码算法、初等密码分析、密码学的信息论基础和计算复杂性理论基础。

1.1 信息安全与密码技术

随着人类步入信息时代的21世纪，信息安全变得越来越重要。这里，不可避免地要涉及信息（Information）、数据（Data）、知识（Knowledge）、信息系统几个概念。

信息的一般定义属于哲学范畴。信息是事物运动的状态与方式，是事物的一种区别于物质与能量的属性。信息与物质、能量的概念处于同一层次，成为组成世界的三大要素。消息是信息的外壳或表象，信息是消息的内核；信号是信息的载体；数据是记录信息的一种形式。知识是认识主体（人、猩猩等）加工、序化的信息。

信息系统是指有目的、和谐地处理信息的人—机系统（人、传感器、通信设备、计算机硬件、软件等），它能对一定形态、形式的信息进行处理（如采集、发送、传递、接收、检测、度量、变换、存储），并且最终转换为可以由人类感知器直接感知的结果（传统的感知器有视觉、听觉、触觉感知器；而嗅觉、味觉感知器已经或者即将被利用）。下面是信息系统的一些实例：公众移动通信系统，民航/铁路客运售票系统，地理信息系统，保安监控系统，地震、海啸监测预警系统（可能包含以某些动物作为探测器的预警子系统）。信息系统按社会功能可分为：企业生产/营销业务系统，党政内部网络系统，电子政务系统，电子商务系统，军队信息系统（如指挥–控制–通信–计算机–情报系统 C^4I，信息作战系统），大国间的战略导弹核查系统等。目前的一个趋势是：若干信息系统经集成或互联（比如经互联网），形成了十分复杂的网络拓扑结构，使信息安全保障的形势变得更加严峻。

在讨论信息安全时，可以把比较抽象的“信息”狭义地理解为消息或记录它的一种形式——数据。人们对信息的基本安全要求大致有如下几条。

机密性（Confidentiality）——拥有数据的一方或交换数据的各方不希望局外人或对手获得、进而读懂这些数据。

完整性（Integrity）——数据在交换及保存中不被未授权者删除或改动，或者合法的接收者能方便地判断该数据是否已经被篡改。

认证性（Non-Repudiation）——也称“不可否认性”或“抗抵赖”，包括信源端和接收端认证性，即信息系统中的实体不能否认或抵赖曾经完成的发送消息或接收消息的操作。利用信源端证

据可以检测出消息发送方否认已发送某消息的抵赖行为，利用接收端证据可以检测出消息接收方否认已接收某消息的抵赖行为。此类证据通常还包括时间/时序或“新鲜性”证据。

可用性（Availability）——授权用户能对信息资源有效使用。显然，信息系统可靠性是其支撑之一。

公平性（Fairness）——信息具有的社会或经济价值只能在交互中体现。公平性就是指交换规则或交互协议要使得参与信息交互的各方在承担安全风险上处于相同或相当的地位。

可控性（Controllability）——是指对信息的传播及传播的内容以至信息的机密性具有控制能力的特性。一般指信息系统或（社会）授权机构根据某种法规对信息的机密性、信息的传播通道、特定内容信息的传播所具备的控制能力的特性，以及获取信息活动审计凭证能力的特性，如“密钥托管”（Key Escrow）、“匿名撤销”（Anonymity Revocation）、实时内容检测与过滤、计算机犯罪或诉讼的司法取证等。

也可将以上特性归结为数据安全（机密、完整、抗抵赖）、可用、交互公平、传播可控。所有对信息安全的威胁或攻击，都可以归结为对信息的以上属性的侵害。例如，属于人为故意的威胁或攻击中，窃取、破译是对机密性的侵害；篡改是对完整性的侵害；伪造、重放是对认证性的侵害；干扰、占用、资源耗尽以至摧毁信息处理器或载体是对可用性的侵害；在电子媒体商品的网上交易中，获得商品后不按时付款或者收取货款后不按时提供商品，是对公平性的侵害。表 1.1 所示例举了一些属于人为故意的威胁或攻击手段。

表 1.1　　信息安全面临的某些威胁——按安全特性的划分

侵害对象	威胁或攻击手段	案　例
机密性	入侵系统取得高级授权	猜测口令，利用操作系统漏洞，安置木马
	破译密码	穷举法搜索 DES 密钥，对密码器件的边信道攻击（Side-Channel Attack）
完整性	插入、删除、篡改	用原消息 m 的 MD5 碰撞 m' 取代 m
可用性	信道干扰	无线干扰
	摧毁系统硬件	微波炸弹，处理器内潜藏破坏性指令，嗜晶片微生物
	扰乱以至摧毁系统软件	计算机病毒
	用户恶意占用	内部用户资源占用、资源耗尽
	业务拒绝	“轰炸”通信端口
认证性	发送方身份假冒	中间人攻击
	破坏收发审计记录	删除或篡改设备运行日志
公平性	非对等的密钥协商	单方面控制生成密钥参数
	利用非公平交易协议获取利益	中途终止不满足“公平性”的交易协议
可控性	破坏“密钥托管”，阻止“匿名撤消”	攻击相关协议，被收买或不诚实的托管人
	抗内容检测过滤的“穿透”	采用“特征字”变异技术
	阻止司法取证	破坏记录设备或介质，删改设备运行日志

实际上，信息系统安全问题即信息系统中信息资产所有者（Owners）与威胁施动者（Threat Agents）的搏弈问题。1999 年国际标准化组织（ISO）及国际电工委员会（IEC）联合制定了信息

系统的“通用安全评价准则”（ISO/IEC15408：Common Criteria，CC，2001 年我国等同采用为国家标准 GB/T 18336），在其第 1 部分给出了如图 1.1 所示的安全概念和关系模型。

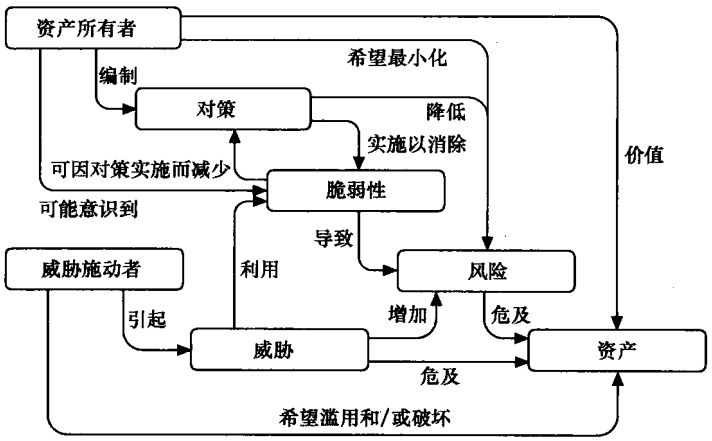


图 1.1　ISO/IEC 15408：安全概念和关系模型

在图 1.1 所示的关系模型中，资产所有者拥有资产（Assets），威胁施动者引起威胁（Threat），通过系统的脆弱性（Vulnerability）对资产构成风险（Risk），资产所有者则通过不断调整其对策（Countermeasures）以求消除系统脆弱性、降低风险来维护资产价值，达成系统使命。

按照以上模型，在信息系统安全工程中首先要做的就是信息系统的安全风险评估。表 1.2 所示为某个信息系统安全风险评估基础数据表的例示（该表由 A、V、T 3 个表拼接而成[注]）。一种 T（威胁、外因）通过一种 V（系统脆弱性，内因）可能对一种系统资产 A 造成危害——即安全风险。系统安全风险的量化和评级，即对 A·V·T 的每一种可能的组合出现的概率进行估计，产生的危害程度和后果进行计算与分析。注意，有的 A·V·T 组合属于不可能事件，将不在系统安全风险的量化和评级表中出现。

表 1.2　信息系统安全风险评估基础数据表——例示

系统资产（A）			系统脆弱性（V）			安全威胁（T）		
类别	名　称	价值	类别	名　称	影响	种类	名　称	频度
以实物为主的物理资产	核心交换机	高[注1]	基本硬件	损坏，老化，过载	大	自然灾害	地震、水灾火灾	极低
	核心服务器	高		射频、声频泄漏	中		雷击、太阳黑子	低
	密码机	高	基本软件	设备维护后门		不达标环境	接地不良、静电	低
	防火墙（硬）	中		操作系统漏洞	大		电源、温度湿度	低
	存储设备	中		数据库缺陷			射频干扰	
	光缆	中	密码系统	密码体制缺陷		人为非故意	误操作	低
	电源/稳压电源	中		密码实现缺陷			密码使用错误	低
	用户终端	低	安全协议	安全性未证明协议			开发方忘交钥匙	

注：3 个表横向栏目（行与行）没有对应关系。其中，“价值”、“影响”、“频度”部分栏目之值，对于不同的信息系统差异可能很大，所以没有给出。

续表

系统资产（A）			系统脆弱性（V）			安全威胁（T）		
类别	名　称	价值	类别	名　称	影响	种类	名　称	频度
以软件、记录为主的数据资产	操作系统	高	安全协议	采用弱安全模式		人为故意	开发方不交钥匙	
	数据库管理系统	高		抗并发攻击缺陷			越权使用资源	
	配置与管理数据	高		抗合谋攻击缺陷			利用阈下信道[注2]	
	运行日志	高	业务软件	设计缺陷			用户合谋攻击	
	安全运控软件及安全事件纪录	高		编程残余 BUG	中		抵赖	
				多软件集成冲突	中		抗追踪、抗审计	
	入侵检测软件	高	内存控管	进程间交互失控			删除日志、数据	
	病毒防治软件	中	用户控管	认证系统缺陷	大		非法接入系统	高
	专用业务软件	中	复杂边界	多入口/无线接入	中		假冒用户	
	业务数据	高/中	信息发布	网站服务器防护差	中		重放、篡改消息	
	用户资料	高/中	入侵检测	检测项数效率矛盾	中		伪造消息	
系统文档资产，管理、人力及信誉资产	系统设计文档		安全态势	准确评价难度大	大		伪造签名	
	系统开发文档		应急反应	业务/存储灾备弱	大		木马、计算机病毒	高
	系统服务商合同			决策慢，联动差	大		信道窃听、截获	高
	管理制度养成		密钥管理	不支持数据签名			侦测射频泄漏	高
	人员配备			他人知签名私钥			分析密码体制	
	可用性口碑			开发方未交钥匙			边信道攻击	
	安全资质及口碑			密钥未按期更新			攻击通信协议	高
			人员管理	对根权限审计缺失	大		干扰、阻断通信	
				弱口令、密钥泄漏	大		拒绝服务 DoS	高
				载体丢失	大		摧毁硬件	低[注3]

注1　或者量化为适当的整数级，比如 1～8（价值由低到高）。系统脆弱性的“影响”和安全威胁的“频度”也可按类似方法量化处理。

注2　阈下信道（Subliminal Channel）也译为“潜信道”。

注3　指非军用系统、非战争状态。

图 1.2 所示为供网络通信系统进行安全性分析的一个构架示例，其用意是提醒系统的建设维护者：在网络环境中，攻击者可能“无处不在”。这里约定将参与信息交换的设备单元或人员统称为实体，并且按照情况与习惯分别称为“实体”、“用户”、“攻击者”等。在图 1.2 中，双箭头线代表交互信道；T 表示可信赖的实体，如仲裁者、认证服务器；U_i 表示系统用户；A 表示攻击者（非授权接入的实体，若干个），他们或者窃听该信道实施被动攻击，或者将自己以类似中继设备的方式插入该信道实施主动攻击。需要注意的是图中用户 U_2（为代表的一类）的嘴部表情——虽然他是一个合法用户，但他仍然可能是一个攻击者（本身就是一个攻击者或被“劫持”成为一个攻击者），甚至彼此（包括与 A）勾结实施合谋攻击。

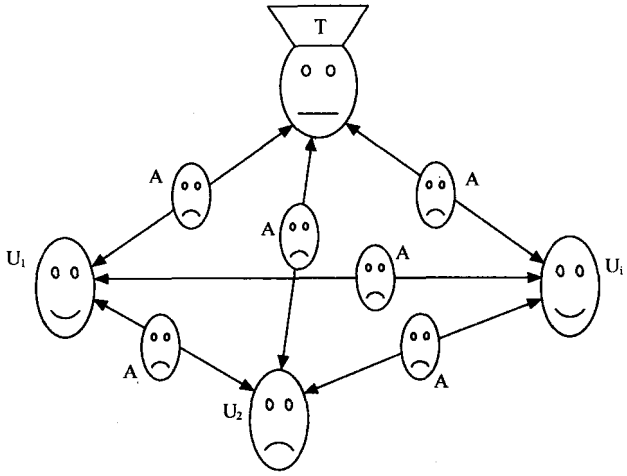


图 1.2　网络通信系统安全性分析构架示例

要有效避免或者降低信息系统安全风险，达成信息安全的要求，目前主要是依靠现代密码学提供的基本理论和技术的支持，因此，现代密码学成为信息安全专业的一门核心课程。

1.2　密码系统模型和密码体制

一个密码通信系统可以用图 1.3 所示的模型表示，它主要由下述几部分组成：明文消息空间 $\mathscr{M}$（按加密体制要求规范的信源），密文消息空间 $\mathscr{C}$，加密密钥空间 $\mathscr{K}_1$，解密密钥空间 $\mathscr{K}_2$，加密变换簇 $\mathscr{E}_{\mathscr{K}_1}$，解密变换簇 $\mathscr{D}_{\mathscr{K}_2}$，所以用六元组 $(\mathscr{M},\mathscr{C},\mathscr{K}_1,\mathscr{K}_2,\mathscr{E}_{\mathscr{K}_1},\mathscr{D}_{\mathscr{K}_2})$ 表示。

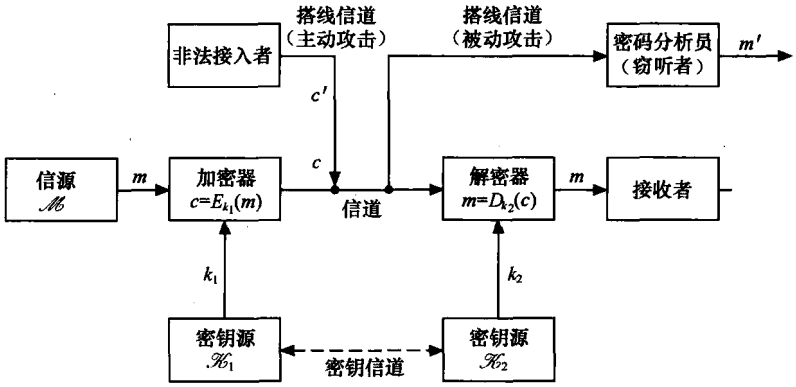


图 1.3　密码系统基本模型

加密变换簇 $\mathscr{E}_{\mathscr{K}_1}$ 中由任一加密密钥 $k_1(\in\mathscr{K}_1)$ 确定的加密变换记为 E_{k_1}。E_{k_1} 必须有左逆，即总能在解密变换簇 $\mathscr{D}_{\mathscr{K}_2}$ 中找到由某个解密密钥 $k_2(\in\mathscr{K}_2)$ 确定的解密变换 D_{k_2}，成为加密变换 E_{k_1} 的左逆，即

$$c=E_{k_1}(m)\in\mathscr{C},\quad \forall m\in\mathscr{M},\quad k_1\in\mathscr{K}_1 \tag{1.1}$$

$$m = D_{k_2}(c) = D_{k_2}\left(E_{k_1}(m)\right), \quad \exists k_2 \in \mathcal{K}_2 \tag{1.2}$$

可见，$m = D_{k_2}E_{k_1}(m) = I(m), \forall m \in \mathcal{M}$，即在 $\mathcal{M}$ 上 $D_{k_2}E_{k_1} = I$，这里的 I 表示恒等变换或幺变换。在上述模型中，称 m 为明文，c 为密文，k_1 为加密密钥，k_2 为解密密钥。如果 k_1=k_2，或者 $k_1 \leftrightarrow k_2$，即从加密密钥（解密密钥）可以非常方便地得到解密密钥（加密密钥），则密码体制称为对称密码体制。如果以上性质不满足，则密码体制称为非对称密码体制。

图 1.3 中所示的密钥信道的任务是解决加密密钥 k_1 和解密密钥 k_2 的协商问题，一般假设该信道是安全信道；而供密文 c 传输的信道则是公共信道或非安全信道，比如无防护的传输线或无线信道，故该信道也是通信双方之外的敌对方——密码通信系统攻击者的活动场所。在图 1.3 中，非法接入者和窃听者都是攻击者，他们代表了对密码通信系统的两类典型攻击模式：主动攻击和被动攻击。除阻断密码通信的目的之外，主动攻击就是要篡改加密者发送的密文，包括对密文实施置换、插入、删除、复制重放等，以达到欺骗接收者的目的。被动攻击不篡改信道中的密文，只是接收信道中传输的密文，再对截获的密文进行分析处理，以便获得解密密钥，或者在不知道解密密钥的情况下恢复出密文 c 对应的明文 m 或者 m 的部分信息。需要注意的是，攻击者有时享有更为有利的分析条件，如在战场上缴获了通信方尚未销毁密钥的加密器（加密机）或解密器（解密机）。关于密码分析（或密码破译）中攻击者的工作条件，将在稍后做进一步讨论。

密码学中的术语“系统或体制”（System）、“方案”（Scheme）和（加解密）“算法”（Algorithm）在本质上是相同或相近的，本书中会根据介绍该部分内容的视角或历史原因交替使用它们。

下面讨论对称密码体制与非对称密码体制的一些差别。

对于对称密码体制，以下总是假设 k_1= k_2= k。对数据进行加密的对称密码系统如图 1.4 所示。

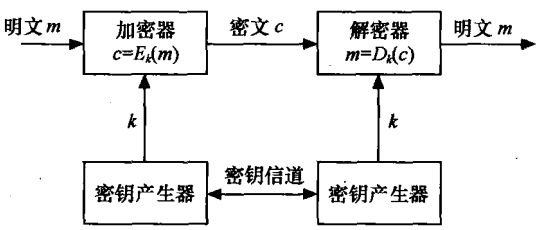


图 1.4　对称密码系统

对称密码根据对明文加密方式的不同可分为两大类，即分组密码（Block Cipher）与流密码（Stream Cipher）。分组密码将明文消息分为包含若干个符号的组，在选定密钥 k 后使用固定的（非时变的）加密变换 $E_k(*)$对明文分组逐组地进行加密。当采用硬件实现时，其加密变换本身的实现电路中无记忆元件是它的类特征。流密码将明文消息分为连续的符号 m_0，m_1，…，m_t，…，在选定密钥 k 后利用有记忆元件的电路生成密钥流 k_0，k_1，…，k_t，…，对明文符号，m_t 实施加密变换 $E_{k_t}(*)$，即加密变换 $E_{k_t}(*)$ 是时变的。当采用硬件实现时，其实现电路中有记忆元件是它的类特征。例如，GSM（Global System for Mobile Communications，全球移动通信系统）移动台（手机）到基站 BS 之间无线传输中使用的加密算法 A5/1 是一种流密码；而 1977 年公布的美国数据加密标准 DES 和近年公开征集评选出的高级加密标准（Advanced Encryption Standard，AES）Rijndael 则是分组密码。

对称密码体制的古典算法有简单代换、多名代换、多表代换等，在 1.3 节将对这些对称密码体制进行介绍。

非对称密码体制由 W.Diffie 和 M.E.Hellman 于 1976 年首先公开提出[1]，而英国数学家 Clifford Cocks 早在 1973 年关于非对称密码体制的开创性工作由于保密原因直到 1997 年才为公众所知。使用非对称密码体制的每一个用户 U 都有一对选定的密钥，一个是可以公开的，称为公开密钥，简称为公钥，用 pk_u 表示；另外一个则是秘密的，称为秘密密钥，简称为私钥，用 sk_u 表示。公钥 pk_u（以及相应算法）可以像电话号码一样进行注册公布，任何人都可以获得，因此，非对称密码

体制又称为双钥密码体制或公钥密码体制（Public Key Cryptosystem）。

公钥密码体制的主要特点是将加密能力与解密能力分开并分别授予不同的用户，因而可以实现多个用户加密的消息只能由一个用户解读，或只能由一个用户加密消息而使多个用户解读。前者主要用于公共网络中的保密通信以降低密钥管理的代价，后者主要在认证系统中用来对消息进行数字签名。

用于保密通信的公钥密码体制可以用图 1.5 表示。图中假设用户 A 向用户 B 发送需要保密的消息 m。用户 A 首先在公钥簿上查找到用户 B 采用的双钥体制种类 $\mathscr{E}$ 和公开密钥 pk_B，从而获得加密变换 E_{pk_B}，用 E_{pk_B} 对消息 m 进行加密得到密文 $c=E_{pk_B}(m)$，再将 c 发送给用户 B；用户 B 用由自己的私钥 sk_B 确定的解密变换 D_{sk_B} 对 c 进行解密，得到对方发送的消息

$$m=D_{sk_B}(c)=D_{sk_B}\left(E_{pk_B}(m)\right) \tag{1.3}$$

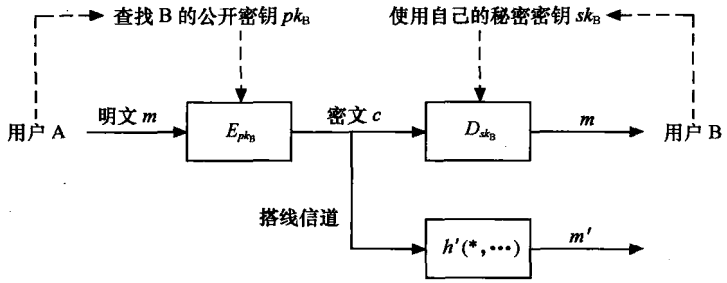


图 1.5　公钥保密通信系统

系统的安全保障在于从公开密钥 pk_B 和密文 c 要推导出私钥 sk_B 或者明文 m 在计算上是不可行的。由于任一用户都可以完成以上的加密并且向 B 发送密文 c，所以此处的密文 c 不能提供对发送者的确证信息，或者说，此处的密文 c 不能提供源端不可否认性（源端抗抵赖）。

公钥密码体制也可以用来构造认证系统（Authentication System）。为了使用户 A 发送给用户 B 的消息具有确证性，可以将公开密钥（及算法）和秘密密钥（及算法）反过来使用，参见图 1.6。用户 A 用自己的秘密密钥 sk_A 对消息 m 进行“加密”，得到密文 $c=D_{sk_A}(m)$ 送给用户 B。用户 B 收到 c 后用 A 的公开密钥 pk_A 对 c 进行“解密”，得到恢复的消息

$$m=E_{pk_A}(c)=E_{pk_A}\left(D_{sk_A}(m)\right) \tag{1.4}$$

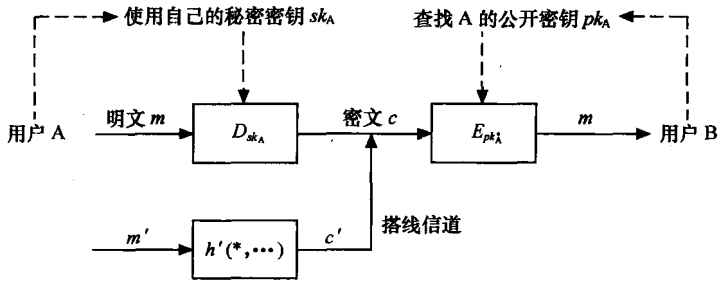


图 1.6　公钥认证系统

由于 sk_A 是保密的，其他人都不可能伪造密文 c，但使用 A 的公钥可以得到有意义的消息 m。由此可以验证消息来自于 A 而不是其他人，从而实现对消息 m 源端 A 的确证。或者说，此处的

密文 c 提供了源端不可否认性（抗源端抵赖）。

为了同时实现通信的保密性和源端不可否认性，可采用双重加密（解密）或签密方案。双重加密（解密）方案如图 1.7 所示。用户 A 要向 B 传送具有源端不可否认性的、需要保密的消息 m，可以将接收者 B 的一对密钥作为加密和解密使用，而将发送者 A 的一对密钥作为认证使用。A 发送给 B 的密文为

$$c = E_{pk_B}\left(D_{sk_A}(m)\right) \tag{1.5}$$

B 恢复明文的运算过程为

$$m = E_{pk_A}\left(D_{sk_B}(c)\right) \tag{1.6}$$

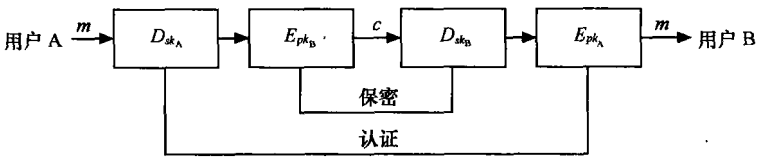


图 1.7　公钥保密通信和认证系统

注意，这里并不要求用户 A 与用户 B 必须使用同一种类的公钥密码体制，但是要使得以上变换顺利完成，必须保证 $D_{sk_A}(m) \in \mathcal{M}_B$，即消息 m 经变换 D_{sk_A} 得到的结果 $D_{sk_A}(m)$ 必须落在加密变换 E_{pk_B} 的明文空间 $\mathcal{M}_B$ 之中。如果用户 A 与用户 B 使用同一种公钥密码体制，则要求该体制的解密变换既是加密变换的左逆，也是加密变换的右逆；或者说该体制的加密、解密变换是可交换的。实际上，在前面的式（1.4）中已经按惯例加上了这一假设（反之，则需要改变若干惯用的符号并且增加许多附加的说明）。

公钥密码体制特别适合解决网络中的多用户通信安全问题，它大大减小了多用户之间通信所需的密钥数量和实施密钥分配的工作量，便于密钥管理。公钥密码体制的出现是密码学研究的一项重大突破，它标志着现代密码学的诞生。本书第 4 章将专门介绍公钥密码体制。

不论是对称密码还是公钥密码，任何一个合格的密码系统均应满足以下要求。

（1）解密的一致性，即要求 $\forall k_1 \in \mathcal{K}_1$，$\exists k_2 \in \mathcal{K}_2$，使得 $\forall m \in \mathcal{M}$，$D_{k_2}E_{k_1}(m) = m$。实际上，这是对加密变换簇 $\mathcal{E}_{\mathcal{K}_1}$ 及其定义域 $\mathcal{M}$ 和解密变换簇 $\mathcal{D}_{\mathcal{K}_2}$ 的要求。

（2）系统的保密性不依赖于对加密体制或加（解）密算法的保密，而仅依赖于非公开密钥（对称密码的密钥或公钥密码的私钥）的保密。此即密码系统安全性分析中著名的 Kerckhoff 假设。

（3）系统或者是理论上不可破的，或者是实际上不可破的。前者即要求 $p_r\{m' = m\} = 0$，其中 m、$m' \in \mathcal{M}$，m 是密文 c 对应的明文，m' 是密码分析者根据截获的密文 c 及其他条件设计变换 h 后得到的关于 m 的猜测：$m' = h(c, \cdots)$。后者是说，确定密钥或者确定任意一段密文所对应的明文的代价是密码分析者无法接受的，如所要求的计算资源超过全球总的计算资源，或者破译时间远远超过密文的保密期。

（4）系统便于实现和使用方便。为了防止攻击者使用穷搜索的蛮力攻击方法来确定密钥，为密码系统设计的密钥空间的元素个数$|\mathcal{K}_1|$与$|\mathcal{K}_2|$一定要充分大，称$|\mathcal{K}_1|$（或$|\mathcal{K}_2|$）为密钥量。

前面已经提到，公钥密码体制也可以用来构造认证系统，以防止消息被篡改、删除、重放和伪造。一个安全的认证系统，应该满足下述条件。

（1）既定的接收者能够验证消息的合法性和真实性。

（2）合法的消息发送者对所发送的消息不能抵赖。

（3）消息发送者之外的其他人不能伪造合法的消息，而且在已知合法密文 c 和相应消息 m 的条件下，要确定加密密钥或者系统地伪造合法密文在计算上不可行。

（4）必要时可以由第三方进行仲裁。

认证理论和技术是最近 30 年随计算机与通信网络的普及而发展起来的，它成为密码学研究的一个扩展的重要领域。它在保证信息的完整性、认证性、可控性等方面起着关键的作用。其中，可以取代手书签名的数字签名（Digital Signature）技术正在当今社会生活中为表达信用与承诺扮演越来越重要的角色。关于认证理论和技术，将在第 5 章和第 6 章中介绍、讨论。

下面介绍最常用的代换密码（Substitution Cipher）。

令 $\mathscr{A}$ 表示明文字母表，含有 q 个“字母”或“字符”，如 95 个可打印的 ASCII 字符，或者国标 GB 2312 中 6 763 个汉字“字符”。可以将 $\mathscr{A}$ 抽象地表示成为一个整数集合

$$Z_q=\{0,1,\cdots,q-1\}$$

在加密时常将明文消息划分成为 L 长的消息单元，称为明文（组），用 $\boldsymbol{m}$ 表示，如

$$\boldsymbol{m}=(m_0,m_1,\cdots,m_{L-1}),\quad m_l\in Z_q$$

$\boldsymbol{m}$ 也称作 $L-$报文，它是定义在 Z_q^L 上的随机变量，Z_q^L 表示 Z_q 上的 L 维矢量空间。此时明文空间 $\mathscr{M}=\{\boldsymbol{m},\boldsymbol{m}\in Z_q^L\}$。

令 $\mathscr{A}'$ 表示密文字母表，含有 q' 个字母，可以将 $\mathscr{A}'$ 抽象地表示成整数集

$$Z_{q'}=\{0,1,\cdots,q'-1\}$$

密文（组）为

$$\boldsymbol{c}=(c_0,c_1,\cdots,c_{L'-1}),\quad c_{l'}\in Z_{q'}$$

$\boldsymbol{c}$ 是定义在 L' 维空间 $Z_{q'}^{L'}$ 上的随机变量。密文空间 $\mathscr{C}=\{\boldsymbol{c},\boldsymbol{c}\in Z_{q'}^{L'}\}$。当 $\mathscr{A}'=\mathscr{A}$ 时，有 $\mathscr{C}=\{\boldsymbol{c},\boldsymbol{c}\in Z_q^{L'}\}$，即密文和明文由同一个字母表构成。

这里只讨论对称密码。加密变换是由明文空间到密文空间上的映射

$$f_k:\boldsymbol{m}\to\boldsymbol{c},\quad \boldsymbol{m}\in\mathscr{M},\quad \boldsymbol{c}\in\mathscr{C},k\in\mathscr{K}$$

一般的加密变换，并不排斥一对多的映射，即可以允许将一个明文（随机地）映射为不同的密文，因为这不妨碍解密的实现。如果假定函数 f_k 是 1 对 1 映射，则可以用加密映射 f_k 的逆映射 f_k^{-1} 来表示解密变换

$$f_k^{-1}(\boldsymbol{c})=f_k^{-1}\cdot f_k(\boldsymbol{m})=\boldsymbol{m},\quad \boldsymbol{m}\in\mathscr{M},\quad \boldsymbol{c}\in\mathscr{C},\quad k\in\mathscr{K}$$

加密变换 f_k 通常可以由加密变换簇 $\mathscr{E}_{\mathscr{K}}$ 的映射函数 $f(k,\boldsymbol{m})$，经指定其中的密钥参数后确定，即

$$E_k(\boldsymbol{m})\equiv f_k(\boldsymbol{m})=f(k,\boldsymbol{m}),\quad k\in\mathscr{K}$$

在实际系统中，可以把映射函数 $f(k,\boldsymbol{m})$ 视为加密机，“注入”（即指定）加密密钥 k 后就完成了加密变换 $E_k\equiv f_k$ 的选定。所以，有时也把加密变换簇的映射函数 f 叫做加密变换。对于以上