21世纪

高等学校信息安全专业规划教材

密码学简明教程

邓元庆 龚晶 石会 编著

清华大学出版社

21世纪高等学校信息安全专业规划教材

密码学简明教程

邓元庆　龚　晶　石　会　编著

清华大学出版社
北　京

内 容 简 介

本书介绍现代密码学的基础理论及典型应用，是作者长期从事密码学教学和研究的结晶。

全书共分10章，内容包括绪论、密码学的数学基础、古典密码技术、对称密码体制与典型算法、非对称密码体制与典型算法、hash函数与消息认证码、消息认证与数字签名、密钥管理、电子邮件安全系统PGP、密码学的知识拓展。各章配有大量例题、习题和思考题，书末附有计算性习题的参考答案和AES算法的教学演示程序及雪崩效应特性测试数据。

教材选材新颖，逻辑严密，使用方便，适用面广，既可作为电子、信息、计算机、通信等专业的密码学教材，也可作为信息安全领域相关技术人员的学习与参考用书。

图书在版编目(CIP)数据

密码学简明教程/邓元庆，龚晶，石会编著. —北京：清华大学出版社，2011.8
(21世纪高等学校信息安全专业规划教材)
ISBN 978-7-302-26056-1

Ⅰ. ①密… Ⅱ. ①邓… ②龚… ③石… Ⅲ. ①密码—理论—高等学校—教材 Ⅳ. ①TN918.1

中国版本图书馆CIP数据核字(2011)第131823号

责任编辑：魏江江　徐跃进
责任校对：焦丽丽
责任印制：何　芊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：三河市君旺印装厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：19.5　**字　数**：476千字
版　　次：2011年8月第1版　　**印　　次**：2011年8月第1次印刷
印　　数：1～3000
定　　价：32.00元

产品编号：035448-01

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能

力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

(3) 实施精品战略，突出重点。规划教材建设把重点放在专业核心(基础)课程的教材建设上；特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

(4) 支持一纲多本，合理配套。专业核心课和相关基础课的教材要配套，同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源的配套。

(5) 依靠专家，择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

21 世纪高等学校信息安全专业规划教材

联系人：魏江江 weijj@tup.tsinghua.edu.cn

前　言

随着密码技术、电子通信技术和计算机网络技术的飞速发展，信息系统的信息安全保密问题越来越突出，信息安全保密的难度也越来越大。作为实现信息安全保密最核心的技术手段，密码技术在信息安全保密领域起着举足轻重且不可替代的作用。为此，国内不少高校、不少专业已经将密码学列为学生必修的专业基础课程或专业课程，并由此催生出种类众多的密码学教材，包括翻译教材和原创教材。正是在这样的背景下，我们根据多年来从事密码学教学和研究工作的经验，并紧密结合国内外密码学的发展潮流，编写了本书，以给广大师生和密码工作者提供更多的密码学教材选择。

本书共分 10 章，内容包括绪论、密码学的数学基础、古典密码技术、对称密码体制与典型算法、非对称密码体制与典型算法、hash 函数与消息认证码、消息认证与数字签名、密钥管理、电子邮件安全系统 PGP、密码学的知识拓展。各章配有大量例题、习题和思考题，书末附有计算性习题的参考答案和 AES 算法的教学演示程序及雪崩效应特性测试数据。本书建议学时为 50～60 学时。

与其他密码学教材相比，本书力图突出以下几个特色：

(1) 逻辑严密，结构合理。密码学的内容众多，处理好各部分内容的关系至关重要。本书按照绪论、数学基础、密码技术、密码算法、密码应用、知识拓展的逻辑结构编排内容，不仅逻辑性好，而且结构更加合理。

(2) 内容新颖，与时俱进。密码技术发展十分迅速，作为教材，必须紧跟时代的前进步伐，使其尽可能快地反映密码学的最新成果。为此，本书在分组密码算法中，删除了一般教科书中广泛介绍而实际上已经过时的 DES 算法，重点介绍本世纪最重要也最流行的两种密码算法：美国的高级加密标准(AES)算法和欧洲密码标准的 Camellia 算法，并在书末附有 AES 算法的教学演示程序和雪崩效应特性测试数据；在公钥密码算法中，重点介绍 RSA 和椭圆曲线密码，较好地兼顾了现实与未来两个方面的需求；在 hash 函数中，淘汰了已经被我国著名密码学家王小云教授破解的 MD4、MD5 和 SHA-1 算法，直接介绍安全性更高的 SHA-512 和 Whirlpool 算法。在教材的最后，还简要介绍了混沌密码、量子密码、公钥基础设施(PKI)等内容，作为密码学的知识延伸，拓展学生的视野。

(3) 习题细化，方便教学。习题是教材的重要内容，合适的习题可以帮助学生更好地理解和掌握所学知识。本书不仅例题丰富，而且对典型算法的各个环节设计了细化的习题，克服了一般教科书中动不动就是整个算法编程的问题，更加方便教学。而附录

中给出的计算性习题参考答案，更有助于学生查找学习中存在的问题，更深入地理解所学内容，从而更有效地提高学习效果。

本书选材新颖，逻辑严密，使用方便，适用面广，既可作为电子、信息、计算机、通信等专业的密码学教材，也可作为信息安全领域相关技术人员的学习与参考用书。

本书由解放军理工大学邓元庆教授主持编写，龚晶、石会参编。邓元庆编写第1～第5章，并负责编写大纲的制定和全书的统稿、定稿及其他相关事宜；龚晶编写第6～第9章，石会编写第10章和附录。清华大学出版社的员工为本书的出版付出了辛勤的劳动，解放军理工大学理学院的各级领导及编者的家人为本书的编写提供了大量的支持，张松洋、李佳雨、赵浩、王普、李云鹏、许晗询、许昌等学员为本书的编写做了大量的前期准备工作，谨在此表示由衷的感谢。

由于编者水平有限，书中难免存在不妥之处，恳请读者雅正。

编 者

2011年7月于南京

目　录

第1章 绪 论

公元前405年，古希腊斯巴达国北路军司令莱桑德在率部征服雅典时，从捕获的雅典信使身上搜出了一条布满杂乱无章希腊字母的普通腰带。当他无意中把腰带呈螺旋形缠绕在手中的剑鞘上时，原来腰带上那些杂乱无章的字母竟组成了一段清晰的文字："波斯军队将在斯巴达军队发起对雅典的最后攻击时，对斯巴达军队进行突然袭击。"莱桑德当机立断，马上改变作战计划，先以迅雷不及掩耳之势一举击溃毫无防备的波斯军队，解除后顾之忧后迅速回师征伐雅典，终于取得了古希腊历史上著名的伯罗奔尼撒战役的最后胜利。西方密码学界认为，莱桑德无意中破译的腰带情报，是有文字记载以来世界上最早的密码情报。

如今，两千多年过去了，人类早已进入信息时代。密码已经不只用于军事情报的保密，还广泛用于政府、团体和个人信息的保密。只是随着电子技术、通信技术、计算机技术和密码技术的飞速发展，信息的保密与窃密斗争越演越烈，保密的难度也已经越来越大，稍有不慎便可能失密。

本章作为全书的绪论，将简要介绍密码学的发展简史、基本概念和信息安全的基本内容，为学习现代密码学打下良好的基础。

1.1 引 言

今天，密码对于一般人而言，可能还会感到有些神秘，但绝不会感到陌生。因为不管愿意还是不愿意，密码都已经实实在在地走进了人们的生活。例如，银行卡需要密码保护资金的安全，电子信箱需要密码保护隐私，手机通信需要密码保护通话的秘密，信息系统需要密码验证访问权限……类似的例子不胜枚举。

那么，密码究竟是什么呢？

简单地说，密码是将公开信息变换为秘密信息的暗号或技术的总称，是实现信息系统安全保密的一种主要的技术手段。窃密者若不能掌握破译密码的有效方法，将无法获取用密码保护的原始信息。

在军事斗争中，密码具有特殊的意义。用电视剧《暗算》的第二部《看风》中男主人公安在天的俄国老师安德罗的话说，"密码是欺诈，是躲藏，是暗算。密码是兵器，是兵器中的暗器。兵不厌诈，研究和破译密码的人都是撒旦"。在密码大师安德罗的眼里，密码不仅是兵器，更是兵器中的暗器，由此可见密码的战斗力非同一般。正因为如此，所以历代兵家都十分重视密码的编制、使用和保护，同时也不遗余力地窃取和破译对手的密码。数千年惊心动魄的世界战争史告诉人们，密码对于战争的胜利起着不可替代的举足轻重的作用。下面列举几例发生在近、现代的相关史实。

第一次世界大战中，美国为了自身的利益，宣布保持中立。然而，1917年2月下旬，第一次世界大战爆发还不到三年，英国海军情报机关破译的一份德军情报，无情地打破了美国

“事不关己，高高挂起”的偏安梦。在这份由德国外长齐默尔曼签发的密报中，德国宣称将在欧洲进行无限制的潜艇战，即使是中立国家的船队也在德军的打击之列。密报中甚至还要求墨西哥与德国结盟，在美国不再保持中立时对美国宣战。2 月 22 日，当美国从英国外交部转交的密报中获知德国的阴谋时，怒不可遏，决定不再保持中立，并采取先发制人的战争策略。在经过 5 个星期的短暂准备后，美国公开对德宣战并立即出兵西线，既避免了美国本土燃起战火，同时也加速了协约国的胜利、同盟国的失败。次年 11 月，人类历史上的首次世界大战便宣告结束。

第二次世界大战中，1943 年 4 月 18 日，日本军方的战争狂人和精神支柱、海军大将山本五十六在巡视太平洋战区的所罗门群岛时，因乘坐的飞机被美军击落而葬身丛林，太平洋战局从此转向有利于美国的方向发展，其中的原因就是日军使用的“紫密”密码被美国情报机关破译。

1982 年 4 月 2 日，位于南大西洋的马尔维纳斯群岛（福克兰群岛）发生了英阿马岛之战。由于英军驻岛兵力不多，因此，4 月 10 日，距离开战仅仅 8 天，以阿根廷陆军第 5 军军长兼马尔维纳斯战区司令加西亚中将为作战总指挥的阿根廷军队便攻占了马岛，并建立了以梅嫩德斯准将为军事长官的马岛行政机构。英国在外交斡旋失败后，立即开始了以武力重夺马岛的大规模军事行动。6 月 15 日，英国正式宣布成功夺回马岛，至此，历时 74 天的马岛战争以阿军失败、英军胜利而结束。令人感到蹊跷的不是战争的结局，而是战争的过程，因为在英军反攻马岛的隆隆炮火中，梅嫩德斯将军的指挥部总能够平安无事。阿根廷军方战后说，梅嫩德斯将军的指挥部之所以安然无恙，并不是因为英军仁慈，也不是因为梅嫩德斯将军福星高照，而是因为阿军低劣的密码通信救了梅嫩德斯将军和他的指挥部随员的命。因为阿军战时使用的密码实在太过低级，通过密报发出的情报、命令无一例外地被英军轻松获悉，以至于英军实在不愿意因毁掉梅嫩德斯将军的指挥部而失去这个可靠的情报来源。

2003 年 3 月 20 日爆发的伊拉克战争中，以美国为首的多国部队基本掌握了制信息权，在密码战场上也上演了一幕不对称的战争剧。美军的所有通信系统，上至国防网，下至战术电台，甚至包括武器制导、飞行控制、目标探测、导航系统、视频通信系统等，都毫无例外地采用了高强度的加密保护，形成了陆、海、空、天一体化的保密网络，使伊拉克军队很难获得对手的军事情报。相反，伊拉克军队的保密通信设备不仅大部分依赖进口，而且设备陈旧、技术落后，其军事行动在多国部队面前几乎无密可保、有密难保，难免陷于被动挨打的境地。这也是伊拉克军队不堪一击、迅速溃败的重要原因。

历史是最好的老师。它告诉人们，密码战的结局不仅关系着战争的胜败，更关系着国家、民族的兴衰。在当前的国际大背景下，保密就是保生命，保密就是保平安，保密就是保胜利，保密就是保发展，应该也必须成为举国一致的共识。

1.2 密码学的发展简史

密码学是一门非常古老而又生机勃勃的学科。经过数千年的发展，密码学已经发展成为包括数学、语言学、电子学和计算机科学等众多学科领域的一门综合性学科。密码学发展

至今，大致上可以划分为古典密码、近代密码和现代密码三个阶段。

1.2.1 古典密码阶段

这一阶段大约是指19世纪末以前的漫长时期，其基本特点是手工加密和解密，即无论加密还是解密，都必须由人亲自动手才能完成。因此，该阶段也称为手工密码时代。

有关密码的起源，国外最早可以追溯到数千年前的古埃及、古巴比伦、古罗马和古希腊。如在古希腊神话和古巴比伦王朝的《旧约圣书》中，就有许多传奇式的密码故事。本章开头提到的密码故事，则是发生在古希腊的一个真实事件，它所用的密码是一种置乱(换位)式密码，其原理非常简单：将一条宽1厘米、长20厘米左右的羊皮带螺旋形斜绕在一根特定规格的棍棒上，然后沿长轴方向在羊皮带上按行书写情报，取下羊皮带后其上面的文字杂乱无章，无人能懂所书内容；而收取情报的人，只要按照同样方式将羊皮带螺旋形环绕在一根同样规格的棍棒上，然后逐行阅读，就可获知情报。

我国有文字记载的最早密码，大约出现在殷商末年。据中国古代兵书《六韬·龙韬》记载，殷商末年的军事家太公望，在协助周武王伐纣的战争中，曾巧妙地采用“阴符”、“阴书”等密码方法来秘密传递军事情报。“阴符”是用八个不同规格的物件，分别表示“大胜克敌”、“破军擒将”、“降城得邑”、“却敌报远”、“警众坚守”、“请粮益兵”、“败军亡将”、“失利亡土”等比较简单的军事情报。比较复杂的军事情报则用“阴书”传递，它是在三份竹简上按字轮流书写一份完整的军事情报，由三位信使分别递送，接收者将其合而为一就可得到全部的情报内容，而敌人截获任何一位信使都无法了解军事情报的完整内容。从密码学的角度看，“阴符”属于一种代换式密码，依靠字符代换来保守秘密；“阴书”则属于一种置乱式密码，依靠打乱字符位置来保守秘密。代换与置乱是古典密码中两种最基本的密码技术。

在古典密码的实践中，还有一种“隐写术”，其作用与密码类似，也能在一定程度上实现保密，但所用方法不同(因保密度有限，今后不再提及)。例如，公元前440年，古希腊战争中，奴隶主为了向结盟的部落秘密传送军事情报，先将信使的头发剃光然后将情报写在头皮上，等信使的头发长长后便可大摇大摆地将情报安全地送到结盟的部落去，而收信的部落只要剃光信使的头发就可以看到情报。我国古代文人墨客时兴的藏头诗、藏尾诗、拆字诗、回文诗，实际上也是一种“隐写术”文字游戏，因为只有熟悉这种风格的人，才能读懂它的“话外之音”。下面就是一首来源于唐伯虎点秋香故事的影视剧中的藏头诗，相信聪明的读者很快就可以明了“唐伯虎”在诗中所隐含的“话外之音”：

我画蓝江清悠悠，
爱晚亭前枫叶愁。
秋雾茫茫笼佛寺，
香烟袅袅绕经楼。

在众多的古典密码中，最著名也最有代表性的密码当推恺撒密码和维吉尼亚密码。

恺撒密码是古罗马皇帝恺撒(公元前102年至公元前44年)发明的一种密码，它将明文中的字母用字母表中该字母后面的第3个字母取代，便可获得密文。例如，字母a用字母D取代，字母b用字母E取代，依次类推(此处以小写或大写形式区别明文或密文)。像这种通过移位的方式就可以实现加密或解密的密码称为移位密码，它是“单表代换”密码的一种特例。所有的“单表代换”密码都有一个共同点，那就是相同的明文必然产生相同的密文。

用今天的眼光看,“单表代换”密码的保密度很低。

维吉尼亚密码是16世纪的法国外交官维吉尼亚(1523—1596)发明的一种“多表代换”密码,它将26个移位密表合成一个“维吉尼亚密表”,从而可以使相同的明文产生不同的密文,因此,其保密度远高于“单表代换”密码。维吉尼亚本人当年曾经宣称,该密码可以保证300年无人能破。其后的事实证明,维吉尼亚所言并非大话。

古典密码虽然简单,但它的基本原理至今还在使用。例如,特务使用“化学密写”的方法传递情报,就属于一种隐写术的应用。再如,话音保密通信中,可以将话音信号分成多个微小的时段或频带,然后打乱它们的位置再进行传输,就属于置乱密码术在信息时代的应用。在名扬全世界、独领风骚20年的数据加密标准(DES)算法中,更是广泛使用了代换和置乱两种基本的密码技术。

1.2.2 近代密码阶段

这一阶段是指20世纪初期到40年代末的大约50年的时间,尽管其间还存在手工加、解密的情形,但就整个阶段而言,其主要的特点还是采用机械或机电密码机进行加密和解密。因此,该阶段也称为机电密码时代。

使用机械密码机后,不仅将人从枯燥的手工作业中解放了出来,大大提高了加、解密的速度,而且还因为密码机的众多转轮可以实现极其复杂的密码代换,因此保密的强度也大大增强。机电密码机在技术上更进一步,它能够在使用者敲击键盘输入明文字符时将加密后的密文字符以莫尔斯电码的形式发送出去,因而初步解决了在线实时加密的技术难题,使密码技术和密码通信技术产生了实质性的飞跃。

近代密码阶段历经了到目前为止仅有的两次世界大战,密码机在这两次世界大战中建立了不朽的历史功勋。例如第二次世界大战中,德国、英国、法国、美国等国分别使用了ENIGMA、TYPEX、C-36、M-209等型号的转轮密码机,用于保障本国的通信秘密。这些密码机都使用了远比维吉尼亚密码复杂得多的密码代换技术,变动密码机转轮的位置(密钥),就可方便地选择转轮密码机的密码代换表。例如,三个转轮的ENIGMA密码机,其密钥量就已经多达10 586 916 764 424 000$\approx 10^{12}$,由此可见其保密强度之高。

历史上最负盛名的两种转轮密码机M209(美国)和ENIGMA(德国)分别如图1-1和图1-2所示,它们既分别是机械密码机和机电密码机的典型代表,也是同类密码机产品中的巅峰之作。

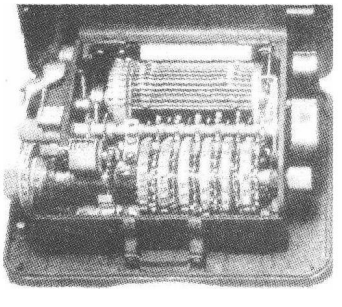

图1-1 M-209密码机

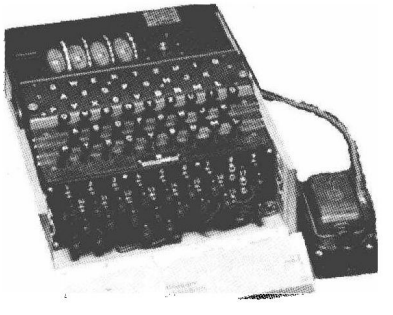

图1-2 ENIGMA密码机

针对密码机的出现和使用，这一时期的密码破译技术也与时俱进，出现了与密码机针锋相对的密码破译机。例如，“二战”后期盟军曾利用 ENIGMA 密码破译机多次破译纳粹德国军队的 ENIGMA 密码，及时掌握了德军的情报。仅在欧战结束前的 11 个月里，盟军就利用破译 ENIGMA 密码获得的情报，在欧洲战场上击沉了 300 多艘德军潜艇，给了纳粹德国军队致命的打击。研究“二战”历史的专家估计，盟军成功破译德军的 ENIGMA 密码，至少使“二战”缩短了一年。不过可惜的是，为了保守密码破译的秘密，“二战”结束时，英国首相丘吉尔下令销毁了英国所有的 ENIGMA 密码破译机，今天人们能够见到的 ENIGMA 密码破译机几乎都是复制品。

1.2.3 现代密码阶段

这一阶段大约是指 20 世纪 50 年代以来的时期，其主要特点是采用电子计算机进行加密和解密。因此，该阶段也称为计算机密码时代。这一阶段的密码技术与计算机技术和电子通信技术紧密相关。

在密码学发展史上，有三个重大的事件标志着现代密码学的诞生。

一是 1949 年，香农发表了划时代的“保密系统的通信理论”论文，不仅在人类历史上第一次提出了保密系统的理论模型，使得人们从此可以对保密系统进行理论分析，而且从理论上首次提出了提高保密系统保密度的途径——增大密钥量、减小多余度，为人们设计高保密度保密系统指明了方向。只是令人遗憾的是，该论文没能像香农的信息论那样，一提出就受到人们的重视，而是差不多等了 30 年即到了 20 世纪 70 年代中期后，才开始受到人们的重视。

二是 1973 年，美国国家标准局(NBS)为适应计算机数据加密的需要，公开向外界征求可以公开的数据加密标准算法，并在 1977 年正式颁布数据加密标准(DES)。公开征集密码算法，让公众参与密码的讨论，公开作为标准使用的数据加密算法，这在密码学历史上，无疑都是开天辟地的第一回。它使得长期以来被少数人和机构垄断、在“黑屋子”里研究、使用和发展的密码学首次脱去了神秘的外衣，因而极大地调动了密码爱好者的积极性，极大地推动了密码学的研究和发展。也正是从这个时候开始，密码才真正从军政系统独享大量扩展到商业民用。

三是 1976 年，美国的迪菲和赫尔曼两位新锐密码学家发表了“密码学的新方向”论文，首次提出了适应网络保密通信的公开密钥密码思想，在密码学发展史上掀开了崭新的一页。1978 年，第一个实用的公钥密码算法——RSA 问世，并很快成为事实上的公钥密码标准。从此，公钥密码就以全新的面貌出现，成为现代密码学中最热门的研究热点，基于不同理论的各种公钥密码算法(公钥密码体制)如雨后春笋般涌现出来。公钥密码的诞生，解决了传统密码学中无法解决的大量问题，把现代密码学迅速推进到了一个崭新的发展阶段。正因为如此，所以有人说，没有公钥密码的诞生和热火朝天的研究，就没有现代密码学。纵观现代密码学的发展史，这个评价其实一点也不过分。

现代密码阶段有代表性的两款密码产品分别如图 1-3 和图 1-4 所示。图 1-3 是 1996 年由瑞士一家公司设计制造的一款计算机密码板，可提供计算机访问控制、信息保密、完整性检验和病毒防护功能。图 1-4 是美国在 20 世纪 80 年代后期开始投入使用的一款军民两用的数字电话保密机，它采用数字加密技术对话音信号实施加密保护。根据国外资料显示，尽