普通高等教育“十一五”国家级规划教材

高等学校信息安全专业规划教材

密码学引论

第二版

张焕国　王张宜　编著

WUHAN UNIVERSITY PRESS
武汉大学出版社

本书得到以下项目的资助：

国家自然科学基金项目（90104005，69973034，60373087，60673071）
国家863计划项目（2006AA01Z442，2007AA01Z411）

普通高等教育“十一五”国家级规划教材

高等学校信息安全专业规划教材

密码学引论

第二版

张焕国　王张宜　编著

江苏工业学院图书馆
藏书章

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

密码学引论/张焕国,王张宜编著.—2版.—武汉:武汉大学出版社,2009.3

普通高等教育"十一五"国家级规划教材

高等学校信息安全专业规划教材

ISBN 978-7-307-06704-2

Ⅰ.密… Ⅱ.①张… ②王… 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(2008)第194963号

责任编辑:黄金文　　责任校对:刘　欣　　版式设计:支　笛

出版发行:**武汉大学出版社**　(430072　武昌　珞珈山)

(电子邮件:cbs22@whu.edu.cn 网址:www.wdp.com.cn)

印刷:通山金地印务有限公司

开本:787×1092　1/16　印张:18.75　字数:469千字　插页:1

版次:2003年9月第1版　2009年3月第2版

2009年3月第2版第1次印刷

ISBN 978-7-307-06704-2/TN·33　定价:29.00元

版权所有,不得翻印;凡购买我社的图书,如有缺页、倒页、脱页等质量问题,请与当地图书销售部门联系调换。

高等学校信息安全专业规划教材

编　委　会

主　　任：沈昌祥（中国工程院院士，教育部高等学校信息安全类专业教学指导委员会主任，武汉大学兼职教授）

副 主 任：蔡吉人（中国工程院院士，武汉大学兼职教授）

刘经南（中国工程院院士，武汉大学校长）

肖国镇（中国密码学会名誉理事，武汉大学兼职教授）

执行主任：张焕国（中国密码学会常务理事，教育部高等学校信息安全类专业教学指导委员会副主任，武汉大学教授）

编　　委：张孝成（江南计算所研究员）

冯登国（信息安全国家重点实验室主任，教育部高等学校信息安全类专业教学指导委员会副主任，武汉大学兼职教授）

卿斯汉（原中国科学院信息安全技术工程中心主任，武汉大学兼职教授）

屈延文（原国家金卡工程办公室安全组组长，武汉大学兼职教授）

吴世忠（中国信息安全产品测评认证中心主任，武汉大学兼职教授）

朱德生（总参通信部研究员，武汉大学兼职教授）

覃中平（华中科技大学教授，武汉大学兼职教授）

谢晓尧（贵州师范大学副校长，教授）

何炎祥（武汉大学计算机学院院长，教授）

王丽娜（武汉大学计算机学院副院长，教授）

黄传河（武汉大学计算机学院副院长，教授）

执行编委：黄金文（武汉大学出版社计算机图书事业部主任，副编审）

内容提要

本书是在武汉大学出版社2003年出版的《密码学引论》（第一版）基础上改版而成的，旨在为信息安全专业本科生提供一本适用的密码学教材。本书以信息安全专业指导性专业规范中对密码学知识和实践能力的要求为依据，从理论与实际相结合的角度介绍密码学的基本理论、基本技术和实际应用。全书共分为九章。第一章，概论。第二章，密码学的基本概念。第三章，分组密码。第四章，序列密码。第五章，公开密钥密码。第六章，数字签名。第七章，HASH函数。第八章，认证。第九章，密钥管理。

本书与第一版相比，主要进行了以下调整和改写：其一是修正了一版书中已发现的一些错误；其二是增加了一些新内容，以反映密码学的新发展；其三是为了方便教学使用，对一部分内容的叙述方法进行了调整和改写，增加了密码算法的实现示例和习题。

本书是普通高等教育“十一五”国家级规划教材，适合用作信息安全专业和其他相关专业的本科生教材，也可用作信息安全和其他相关领域研究生和工程技术人员的技术参考书。

此为试读，需要完整PDF请访问：www.ertongbook.com

序　言

二十一世纪是信息的时代，信息成为一种重要的战略资源。信息科学成为最活跃的学科领域之一，信息技术改变着人们的生活和工作方式，信息产业成为世界第一大产业。信息的安全保障能力成为一个国家综合国力的重要组成部分。

当前，以 Internet 为代表的计算机网络的迅速发展和“电子政务”、“电子商务”等信息系统的广泛应用，正引起社会和经济的深刻变革，为网络安全和信息安全开拓了新的服务空间。

世界主要工业化国家中每年因利用计算机犯罪所造成的经济损失远远超过普通经济犯罪。内外不法分子互相勾结侵害计算机系统，已成为危害计算机信息安全的普遍性、多发性事件。计算机病毒已对计算机系统的安全构成极大的威胁。社会的信息化导致新的军事革命，信息战、网络战成为新的作战形式。

总之，随着计算机在军事、政治、金融、商业等部门的广泛应用，社会对计算机的依赖越来越大，如果计算机系统的安全受到破坏将导致社会的混乱并造成巨大损失。因此，确保计算机系统的安全已成为世人关注的社会问题和计算机科学的热点研究课题。

信息安全事关国家安全，事关经济发展，必须采取措施确保我国的信息安全。

发展信息安全技术与产业，人才是关键。培养信息安全领域的专业人才，成为当务之急。2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003 年经国务院学位办批准武汉大学建立信息安全博士点。现在，全国设立信息安全本科专业的高等院校已增加到 70 多所，设立信息安全博士点的高等院校和科研院所也增加了很多。2007 年“教育部高等学校信息安全类专业教学指导委员会”正式成立，并在武汉大学成功地召开了“第一届中国信息安全学科建设与人才培养研讨会”。我国信息安全学科建设与人才培养进入蓬勃发展阶段。

为了增进信息安全领域的学术交流、为信息安全专业的大学生提供一套适用的教材，2003 年武汉大学组织编写了一套《信息安全技术与教材系列丛书》。这套丛书涵盖了信息安全的主要专业领域，既可用做本科生的教材，又可作为工程技术人员的技术参考书。这套丛书出版后得到了广泛的应用，深受广大读者的厚爱，为传播信息安全知识发挥了重要作用。现在，为了能够反映信息安全技术的新进展、更加适合信息安全教学的使用和符合信息安全类专业指导性专业规范的要求，武汉大学对原有丛书进行了升版。

我觉得升版后的这套新教材的特点是内容全面、技术新颖、理论联系实际，努力反映

信息安全领域的新成果和新技术，符合信息安全类专业指导性专业规范的要求，适合教学使用。在我国信息安全专业人才培养蓬勃发展的今天，这套新教材的出版是非常及时的和十分有益的。

我代表编委会对图书的作者和广大读者表示感谢。欢迎广大读者提出宝贵意见，以便能够进一步修改完善。

中国工程院院士，武汉大学兼职教授

沈昌祥

2008 年 8 月 28 日

前　言

21 世纪是信息的时代。信息成为一种重要的战略资源，信息技术改变着人们的生活和工作方式，社会的信息化程度大大提高，信息产业成为世界第一大产业。信息的获取、处理和安全保障能力成为一个国家综合国力的重要组成部分。

当前，一方面信息技术与产业欣欣向荣，处于空前繁荣的阶段。可是另一方面，危害信息安全的事件不断发生，信息安全的形势是严峻的。敌对势力的攻击和破坏、利用计算机犯罪、计算机病毒、“黑客”入侵等，已经成为危害我国信息安全的主要威胁。我国已经成为世界信息产业大国，但是目前我国还不是信息产业强国，特别是我国在信息产业的基础性产品方面还比较薄弱，例如计算机操作系统和关键集成电路芯片方面我国现在还依赖国外产品，这就使得我国的信息安全基础不够牢固。

总之，随着计算机和网络在军事、政治、金融、工业、商业等部门的广泛应用，社会对计算机和网络的依赖越来越大，如果计算机和网络系统的安全受到破坏，将导致社会的混乱并造成巨大的损失。因此，确保计算机和网络系统的安全已成为世人关注的社会问题和信息科学技术领域的热点研究课题。

信息安全事关国家安全，事关社会稳定，必须采取措施确保我国的信息安全。

我国政府十分重视信息安全技术和产业的发展，先后在成都、上海和武汉建立了信息安全成果产业化基地。2004 年我国颁布了电子签名法，2006 年我国政府公布了我国自己的商用密码算法，2007 年中国密码学会正式成立，这些都是我国密码界的大事，推动了我国密码事业的繁荣。

2001 年经教育部批准，武汉大学创建了我国第一个信息安全本科专业。2003 年，经国务院学位办批准，武汉大学又建立了信息安全硕士点、博士点和博士后产业基地，形成了信息安全人才培养的完整体系。目前，全国设立信息安全本科专业的高等院校已超过 70 多所，设立信息安全硕士点、博士点的院校也已很多。2007 年国家信息安全类专业教学指导委员会成立，在教育部的支持下，正在研究制定我国信息安全类专业指导性专业规范。我国信息安全学科建设和人才培养进入更加规范化的良性发展阶段。

信息系统的硬件结构安全和操作系统安全是确保信息系统安全的基础，密码、网络安全等技术是关键技术。而且，必须从法律、管理、教育和技术等方面综合采取措施，才能比较有效地确保信息系统的安全。

为了给信息安全专业的本科生提供一本适用的教材，增进密码学知识的交流，2003 年我们在武汉大学出版社出版了《密码学引论》一书。《密码学引论》一书得到许多高校的采用，受到了广大读者的厚爱。经过几年的使用，许多读者提出了很好的建议与修改意见。另外，随着信息科学技术的发展，密码技术得到越来越广泛的应用，密码学的理论与技术发展十分迅速，出现了许多新技术。为了适应密码学教学的新要求，并反映密码学的新发展，我们在原书的基础上进行了修订改版，出版了《密码学引论（第二版）》。《密码学引论（第

二版)》获批为“普通高等教育“十一五”国家级规划教材”。

本书是作者在武汉大学计算机学院长期从事信息安全教学和科研的基础上写成的。其研究工作得到国家自然科学基金、国家863计划等项目的资助。

本书以信息安全类专业指导性专业规范中对密码学知识和能力的要求为依据，从理论和实际相结合的角度介绍密码学的基本理论、基本技术和实际应用。期望读者通过阅读本书，能够掌握密码学的基本理论和基本技术，提高实际应用能力，为实际工作和进一步的深造奠定基础。

因作者学术水平所限，书中难免会有不妥和错误之处。对此，作者恳请读者的理解和批评指正，并于此先致感谢之意。

本书共分九章。第一章，概论。第二章，密码学的基本概念。第三章，分组密码。第四章，序列密码。第五章，公开密钥密码。第六章，数字签名。第七章，HASH函数。第八章，认证。第九章，密钥管理。为了便于学习，每章后面都给出了一定数量的习题。

本书的第二版较之第一版，除了对原有内容进行了调整和改写之外，还增加了主要密码算法的实现示例、我国商用密码算法、HASH函数SHA-2、密码协议概论、Kerberos认证系统、组合公钥算法简介等方面的新内容。

本书的第七章和第八章由王张宜编写，其余由张焕国编写，并由张焕国对全书进行统编。研究生童言和杨启提供了密码算法的实现示例，研究生王后珍、韩海清、李春雷进行了习题的解答和整理。

作者衷心感谢给予作者指导、支持和帮助的所有领导、专家和同行，衷心感谢本书的每一位读者。

张焕国　王张宜

于武汉珞珈山

2008年6月

目 录

此为试读，需要完整PDF请访问：www.ertongbook.com

第1章 概 论

随着计算机和网络在军事、政治、金融、工业、商业等部门的广泛应用，社会对计算机和网络的依赖越来越大，如果计算机和网络系统的信息安全受到破坏将导致社会的混乱并造成巨大损失。因此，确保计算机和网络系统的信息安全已成为世人关注的社会问题和计算机科学与技术领域的研究热点。

当前，以 Internet 为代表的计算机网络的迅速发展和广泛应用，正引起社会和经济的深刻变革，极大地改变着人们的生活和工作方式。Internet 已经成为我们生活和工作中的一个不可缺少的组成部分。基于计算机网络的“电子政务”、“电子商务”和“电子金融”等应用正在兴起，它们的兴起在政务、商务和金融领域引起了一场革命。对此，发展我国的电子政务、电子商务和电子金融已成为建设具有中国特色社会主义强国的不可回避的选择。

然而，目前影响电子政务、电子商务、电子金融应用的主要技术障碍是信息安全问题。由于 Internet 原来缺少安全设计，再加上 Internet 的开放性和无政府状态，使 Internet 成为一个不安全的网络。这就使得 Internet 不能适应电子政务、电子商务和电子金融等系统对信息安全的要求。

世界主要工业国家中每年因利用计算机犯罪所造成的经济损失令人吃惊，据美国 FBI 的调查报告，美国每年因利用计算机犯罪所造成的经济损失就高达 1700 多亿美元，远远超过普通经济犯罪所造成的经济损失。据美国的一项调查报告，有 40% 的被调查者承认在他们的机构中曾发生过利用计算机犯罪的事件。在我国利用计算机犯罪的案例也在迅速上升。例如，最近几年我国的网络银行屡屡发生金融欺诈事件。

“黑客”入侵已成为危害计算机网络和信息安全的经常性、多发性事件，国内外都屡屡发生严重的“黑客”入侵事件。外国情报部门利用“黑客”窃取别国情报是世人皆知的事。

2000 年 2 月 7 日起的一周内，“黑客”对 Internet 网站发动了大规模的攻击，著名的美国雅虎、亚马逊、伊贝等 8 大网站相继被攻瘫痪，造成直接损失 12 亿美元。

2001 年 5 月 1 日前后发生了一场中美网络“黑客”大战。双方互相攻击对方的计算机网站，双方都有很大的损失。这一事件留给我们的思考是发人深省的。

2003 年 1 月 25 日 13 时 30 分到 19 时 30 分的 6 个小时内，北美、欧洲和亚洲的 Internet 全部陷入瘫痪和半瘫痪状态，其原因至今尚不清楚。

据美国 FBI 的估计，大型计算机网络每被攻破一次所造成的损失为 50 亿美元，而一个银行的数据中心的计算机每停机一秒钟的损失为 5 000 美元。

除了金融信息系统外，政治、军事等重要的信息系统也是不法分子攻击的重点。德国几名青年曾攻入五角大楼和北约的计算机数据库。美国通用动力公司的一名软件设计师设计的逻辑炸弹破坏了太空导弹数据库，致使电脑数据库的数据无法恢复，造成无法弥补的损失。被称为“美国头号电脑黑客”的 Kevin Mitnick 15 岁时就闯入“北美空中防务指挥系统”主机，翻阅了美国所有的核弹头资料，并与中央联邦调查局的特工恶作剧。后来他又向圣地亚哥超级计

算机中心、摩托罗拉、NOVELL、SUN 公司及芬兰的 NOKIA 公司的电脑系统发动攻击，盗走各种程序和数据，价值 4 亿多美元。英国、法国和韩国也发生过类似事件。

社会的信息化导致第三次军事革命，信息战、网络战成为新的作战形式，数字化部队和数字化战场已经诞生。美国早就提出了信息战的概念。早在 1995 年 1 月美国国防部就成立了“信息战执行委员会”。1995 年海湾战争期间，美国成功地对伊拉克发动了信息战。战争一开始美国便激活了埋藏在伊拉克计算机系统中的病毒，并用电子干扰机对伊拉克的防空及通信系统实施电子干扰，致使计算机和通信系统瘫痪，使伊拉克处于被动挨打的地位。在科索沃战争期间，美国也曾发动信息战袭击南斯拉夫的电脑系统。在 2003 年的伊拉克战争中，美国的信息战和电子战的优势就更加明显。最近美国又成立网络作战司令部，统一部署和指挥美国的网络作战。

过去被认为是科学幻想的计算机病毒，现已活生生地出现在我们的面前，对计算机系统的安全构成极大的威胁。1988 年 11 月 3 日美国康耐尔大学的一年级研究生罗特·莫里斯编制的称为蠕虫的计算机病毒通过 Internet 大面积传播，致使 6 000 台 UNIX 工作站和小型机被传染，直接经济损失达 6 000 万美元以上。据有关统计，目前计算机病毒已增至上万种，而且还在继续高速度增加。中国台湾人编制的 CIH 病毒是世界上第一个直接攻击计算机主板硬件的病毒，曾在国内和东南亚地区多次大范围传染发作，造成重大经济损失。随着 Internet 的迅速发展和广泛应用，目前计算机病毒也进入了 Internet 时代，主要通过 Internet 进行传播。美国军方早就出钱资助军用计算机病毒的研究。随着移动通信的迅速发展，手机的使用越来越普及，最近又出现了手机病毒。在国内，计算机病毒的传染现象也很严重，特别是大中小学的公用实验室的微机几乎都被计算机病毒传染过。在国内流行的计算机病毒除了由国外传入外，还有一些国内不法分子编制的国产计算机病毒。随着计算机病毒的出现，人们便开始与计算机病毒作斗争。目前反病毒技术已发展到很高的水平。我国的反病毒技术处于世界先进水平。随着反病毒技术的提高，人们对计算机病毒已不像最初那样恐慌。但是，计算机病毒仍然是非常讨厌的，它们的传染发作，都将消耗大量的计算机资源，重者将造成重大损失。过去，大多数计算机病毒的作者只是为了炫耀自己的技术，而现在却更多的是为了获取经济和政治利益，而且呈现出群体作案的特点。这一变化是我们必须认真思考和认真对付的。

面对如此严重危害计算机和网络信息安全的种种威胁，必须采取措施确保计算机和网络的信息安全。特别是中美“黑客”网络大战等事件，使我们清醒地认识到，为了确保国家的安全，必须建立我国自己的信息安全体系。

虽然我国在信息安全技术方面整体上落后于美国等发达国家，但我国在信息安全领域中的许多方面有自己的特色。如，在密码技术、计算机病毒防治、软件加密等方面我国都有自己的特色，而且具有很高的水平。可信计算是近年来发展起来的一种信息安全新技术，它已经在世界范围内形成热潮。我国在可信计算领域起步不晚，水平不低，成果可喜[1]。我国政府大力支持信息安全技术和产业的发展。因此可以相信，我国的信息安全技术和产业将会得到迅速的发展。

国际标准化组织 ISO 在其网络安全体系设计标准（ISO 7498—2）中定义了计算机网络系统的六大安全服务功能：身份认证服务、访问控制服务、数据加密服务、数据完整性服务、不可否认服务和安全审计，比较全面地描述了计算机网络系统安全的内涵，而且强调了信息安全的服务职能。

随着信息技术的发展和应用，人们对信息安全的认识越来越全面，越来越深刻。

众所周知，能源、材料、信息是支撑现代社会大厦的三根支柱。在这三根支柱中能源和材料是具体的、物质的，而信息是抽象的、逻辑的。信息不能脱离信息系统而孤立存在。因此，我们就不能脱离信息系统安全而孤立地谈信息安全。换句话说，当我们讨论信息安全问题时总是要讨论信息系统的安全。

我们认为，信息系统的安全主要包括四个侧面：设备安全（Safety and Security of Equipment），数据安全（Data Security），内容安全（Contents Security）和行为安全（Behavior Security）[1]。

信息系统的设备安全是指确保信息设备的稳定性（Stability）、可靠性（Reliability）和可用性（Availabity）。这里的设备既包括硬件，也包括软件。信息系统的设备安全是信息系统安全的物质基础，如果失去了这个物质基础，信息系统安全就变成空中楼阁。对信息设备的任何损坏都将危害信息系统的安全，如人为破坏、火灾、水灾、雷击等都可能导致信息系统设备的损坏。信息安全行业中的一句行话，“系统设备稳定可靠的工作是第一位的安全”，用通俗的语言精辟地说明了信息系统设备安全的基础作用。

信息系统的设备安全是信息系统安全的物质基础，但是仅仅有信息系统的设备安全是远远不够的。即使计算机系统的设备没有受到损坏，其数据安全也可能已经受到危害，如机密数据可能被泄露，数据可能被篡改。由于危害数据安全的行为在很多情况下并不留下明显痕迹，因此常常在数据安全已经受到危害的情况下，用户还不一定能发现。而对计算机设备安全的损害，用户一般都能直接发现。因此，必须在确保信息系统设备安全的基础之上，确保数据安全。确保数据安全就是要采取措施保护数据，使之免受未授权的泄露、篡改和毁坏。换句话说，数据安全性主要包括数据的秘密性（Secrecy）、数据的真实性（Authenticity）和数据的完整性（Integrity）三个侧面。所谓秘密性就是该知道的就让其知道，不该知道的就不能让其知道。使数据免受未授权的泄露，就是确保数据的秘密性。所谓真实性就是数据真实无伪，使数据免受未授权的篡改，就是确保数据的真实性。所谓完整性就是数据正确无误、完整不缺，使数据免受未授权的毁坏，就是确保数据的完整性。

数据是用来表达某种意思的，因此只确保数据不泄密和不被篡改是远远不够的。还要确保数据所表达的内容是合法的、健康的、积极向上的。换句话说，内容安全是信息安全在法律、政治、道德层次上的要求。即确保数据的内容在法律上是符合国家法律法规的，在政治上是健康的，在道德上是符合中华民族优良的道德规范的。

如果数据中充斥着违法的、不健康的、消极颓废的内容，即使它是保密的、未被篡改的，也不能说是安全的。因为这会危害国家安全、社会稳定和精神文明。因此，必须在确保信息系统设备安全和数据安全的基础上，进一步确保数据内容的安全。

数据安全在本质上是一种静态的安全。而在信息系统中许多数据是程序，编写程序的目的是要进行某种处理，处理的过程称为行为。程序在静态存储时就是一种数据，因此数据安全是静态安全。而程序在运行时（也就是动态时）表现为一系列的行为。如果程序的行为方式和结果是预期的，我们称行为是可信的，否则行为是不可信的。与数据安全相对应，行为安全包括行为秘密性、行为完整性和行为可控性三个侧面。行为的秘密性是指，行为不能危害数据的秘密性，必要时行为的过程和结果也是秘密的。行为的完整性是指，行为不能危害数据的完整性，行为的过程和结果是预期的。行为的可控性是指，当行为的过程出现偏离预期时，能够发现、控制或纠正。

早在20世纪70年代美国军方就开始研究导弹系统的行为安全。行为安全的概念符合哲

学上“实践是检验真理的唯一标准”的科学观点，同时也符合我国政府的“安全可控”的信息安全策略。

目前，习惯上人们把信息系统安全简称为信息安全，这种简称不会带来理解上的歧义，因此本书也采用这种简称。

要确保信息安全，必须采取措施，必须付出代价，这代价就是资源，时间资源或空间资源。所采取的安全措施主要包括法律措施、教育措施、管理措施和技术措施等。

确保信息安全是一个系统工程，必须综合采取各种措施才能奏效。一个系统只有所有子系统都是安全时才是安全的，而只要有一个子系统不安全，则整个系统就不安全。虽然某种措施对付某种危害可能更有效，但是没有一种措施能全面解决信息安全问题。特别应当强调的是，绝不能忽视法律、教育、管理措施，在许多情况下它们的作用大于技术措施。

确保信息安全的技术措施，包括信息系统的硬件结构安全、操作系统安全、数据库安全、网络安全、密码技术、恶意软件防治技术、信息隐藏技术、数字版权保护技术、物理安全技术等。在这些众多的技术措施中，信息系统的硬件结构安全和操作系统安全是信息系统安全的基础，密码技术和网络安全等技术是关键技术。

本书讨论信息安全的关键技术——密码技术。

密码技术是一门古老的技术，大概自人类社会出现战争便产生了密码（Cipher）。由于密码长期以来仅用于政治、军事、公安、外交等要害部门，其研究本身也只限于秘密进行，所以密码被蒙上神秘的面纱。在军事上，密码成为决定战争胜负的重要因素之一。有些军事评论家认为，盟军在破译密码方面的成功，使第二次世界大战提前十年结束。

然而，随着计算机和网络技术的迅速发展和普及应用，出现了电子政务、电子商务、电子金融等重要的应用信息系统。在这些系统中必须确保信息的安全，因此密码技术有了更广泛的应用空间。

密码技术的基本思想是伪装信息，伪装就是对数据施加一种可逆的数学变换。伪装前的数据称为明文（Plaintext），伪装后的数据称为密文（Ciphertext）。伪装的过程称为加密（Encryption），去掉伪装恢复明文的过程称为解密（Decryption）。加解密要在密钥（Key）的控制下进行。将数据以密文的形式存储在计算机的文件中或送入网络信道中传输，而且只给合法用户分配密钥。这样，即使密文被非法窃取，因为未授权者没有密钥而不能得到明文，因此未授权者也不能理解它的真实含义，从而达到确保数据秘密性的目的。同样，因为未授权者没有密钥也不能伪造出合理的明密文，因而篡改数据必然被发现，从而达到确保数据真实性的目的。与能够检测发现篡改数据的道理相同，如果密文数据中发生了错误或毁坏也将能够检测发现，从而达到确保数据完整性的目的。

由此可见，密码技术对于确保数据安全具有特别重要和有效的作用。

密码的发展经历了由简单到复杂、由古典到近代的发展历程。在密码发展的过程中，科学技术的发展和战争的刺激都起了巨大的推进作用。

1946 年电子计算机一出现便用于密码破译，使密码技术进入电子时代。

1949 年商农（C. D. Shannon）发表了题为《保密系统的通信理论》的著名论文，把密码置于坚实的数学基础之上，标志着密码学作为一门科学的形成[2]。

然而对于传统密码，通信的双方必须预约使用相同的密钥，而密钥的分配只能通过其他安全途经，如派专门信使等。在计算机网络中，设共有 n 个用户，任意两个用户都要进行保密通

此为试读，需要完整PDF请访问：www.ertongbook.com