21世纪高职高专规划教材

计算机应用系列

计算机安全技术

张同光 主 编
张有为 张家平 常 青 副主编

清华大学出版社

21世纪高职高专规划教材
计算机应用系列

计算机安全技术

张同光　主　编
张有为　张家平　常　青　副主编

清华大学出版社
北　京

内 容 简 介

本书本着“理论够用，重在实践”的原则，采用案例引导理论阐述的编写方法，内容注重实用，结构清晰，图文并茂，通俗易懂，力求做到让读者在兴趣中学习计算机安全技术。

本书共8章，主要内容包括：计算机安全概述、实体和基础设施安全、密码技术、操作系统安全技术、计算机网络安全技术、数据库系统安全技术、应用安全技术、容灾与数据备份技术。

本书适合作为高职高专及成人高等院校电子信息类专业教材，也可供培养技能型紧缺人才的相关院校及培训班教学使用。

图书在版编目（CIP）数据

计算机安全技术/张同光主编. —北京：清华大学出版社，2010.9
（21世纪高职高专规划教材. 计算机应用系列）
ISBN 978-7-302-23565-1

Ⅰ. ①计… Ⅱ. ①张… Ⅲ. ①电子计算机－安全技术 Ⅳ. TP309

中国版本图书馆CIP数据核字（2010）第158200号

责任编辑：张龙卿（sdzlq123@163.com）
责任校对：李　梅
责任印制：李红英

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：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185×260　　**印　张**：23.5　　**字　　数**：569千字
版　　次：2010年9月第1版　　**印　　次**：2010年9月第1次印刷
印　　数：1～3000
定　　价：36.00元

产品编号：034472-01

前　言

随着计算机的普及以及互联网的建设向纵深发展(比如物联网的迅速发展),计算机技术和网络技术已深入到社会的各个领域,人类对计算机和计算机网络的依赖越来越大,计算机安全问题已经成为全社会关注和讨论的焦点。如何保护企业或个人的计算机系统免遭非法入侵,如何防止计算机病毒、木马等对内部网络的侵害,都是信息时代企业或个人面临的实际问题。因此,社会对计算机安全技术的需求也越来越迫切。为了满足社会的需要,各高等院校计算机相关专业相继开设了计算机安全方面的课程。但是,目前多数计算机安全技术方面的教材偏重于理论,不能很好地激发学生学习这门课的兴趣,所以,为了满足计算机安全技术教学方面的需求,笔者编写了本书。

本书以解决具体计算机安全问题为目的,全面介绍计算机安全领域的实用技术,帮助读者了解计算机安全技术体系,掌握维护计算机系统安全的常用技术和手段,解决实际计算机系统的安全问题,使读者从全方位建立起对计算机安全保障体系的认识。

本书共 8 章。

第 1 章介绍计算机安全的基本概念、计算机安全面临的威胁以及计算机安全技术体系结构。通过本章的学习,使读者对计算机安全有一个整体的认识。

第 2 章通过对环境安全、设备安全、电源系统安全以及通信线路安全的详细介绍,帮助读者了解物理安全的相关知识,并且能够运用本章介绍的知识和技术来保障计算机系统的物理安全。

第 3 章介绍常用加密方法、密码学的基本概念、破解用户密码的方法、文件加密的方法、数字签名技术以及 PKI,并且通过对一系列实例的介绍,加深读者对基础安全方面的基础知识和技术的理解,使读者能够运用一些工具软件来保护自己在工作或生活中的机密或隐私数据。

第 4 章主要介绍 Windows 系统中账号安全管理、网络安全管理、IE 浏览器的安全设置、组策略的使用、Windows 权限的概念及其设置、Windows 安全审计,然后简单介绍 UNIX/Linux 系统安全的配置,通过本章的学习,使读者了解 Windows 系统安全的多个方面,从而提高读者安全使用 Windows 系统的水平。

第 5 章介绍端口与漏洞扫描以及网络监听技术、缓冲区溢出攻击及其防范、ARP 欺骗、DoS 与 DDoS 攻击检测与防御、防火墙技术、入侵检测与入侵防御技术、恶意软件、蜜罐技术、VPN 技术、HTTPTunnel 技术以及无线网络安全等内容,并且通过对一系列实例的介绍,加深读者对网络安全和攻防方面的基础知识和技术的理解,帮助读者提高解决实际网络安全问题的能力。

第 6 章介绍 SQL 注入式攻击的原理、对 SQL 注入式攻击的防范、常见的数据库安全问

题及安全威胁、数据库安全管理原则等内容。同时通过对一系列实例的介绍，加深读者对数据库安全管理方面的基础知识和技术的理解，帮助读者提高维护数据库安全的能力，并且在进行 Web 开发时要注意防范 SQL 注入式攻击。

第 7 章介绍 Web 应用安全、XSS 跨站攻击技术、电子邮件加密技术、网络防钓鱼技术、QQ 的安全使用、网上银行账户安全常识以及 WinHex 的使用。通过本章的学习，使读者对网络应用中存在的一些威胁有一个清楚的认识，进而提高读者安全使用网络的水平和技能。

第 8 章介绍容灾技术的基本概念、RAID 级别及其特点、数据备份技术的基本概念以及 Ghost 的使用。通过本章的学习，使读者理解容灾与数据备份技术在计算机安全领域有着举足轻重的地位，在以后的生活或工作中，强化安全意识，采取有效的容灾与数据备份技术，尽可能地保障系统和数据的安全。

本书由张同光担任主编，张有为、张家平、常青担任副主编，参加编写的还有叶涛、赵晓莉和陈栋。其中张有为编写第 8 章，张家平编写第 6 章和 7.7 节，常青编写 5.1 节和 5.2 节，叶涛编写 3.4 节和 3.5 节，赵晓莉编写 2.1～2.4 节，陈栋编写第 1 章，张同光编写 2.5 节和第 2 章小结与习题、3.1～3.3 节、3.6～3.7 节和第 3 章小结与习题、第 4 章、5.3～5.14 节和第 5 章小结与习题、7.1～7.6 节、7.8 节和第 7 章小结与习题。全书最后由张同光(jsjoscpu@163.com)统稿和定稿。

由于编者水平有限，书中难免存在疏漏之处，敬请广大读者批评指正。

张同光

2010 年 6 月

目　录

第1章　计算机安全概述

本章学习目标：

- 认识到计算机安全的重要性
- 了解计算机系统面临的威胁
- 了解计算机安全基本概念
- 了解计算机安全技术体系结构
- 了解安全系统设计原则以及人、制度和技术之间的关系

美国总统奥巴马于2009年5月29日公布网络安全评估报告时指出，来自网络空间的威胁已经成为美国面临的最严重的经济和军事威胁。为应对来自网络空间的威胁，为了打击黑客和敌对国家的网络攻击，酝酿筹备近一年的美军“网络司令部”于2010年5月21日正式启动，将于2010年10月全面运作。网络司令部隶属美国战略司令部，位于马里兰州的米德堡军事基地，编制近千人，主要职责是进行网络防御和网络渗透作战。一直以来美军各部门都在网络领域孤军作战，网络司令部将统一管理、强化对策，并将积极寻求国际合作。美国国防部长盖茨称：“网络司令部的成立旨在改变网络的脆弱性，从而更好地应对越来越多的网络威胁。”

网络攻击有可能使现代社会的机能陷入瘫痪。而且，在现代战争中信息技术已变得不可或缺。因此，美国把网络防御定位为国家安全保障上的重大课题。

美国是世界上第一个提出网络战概念的国家，也第一个将其应用于实战，但美军尚未形成统一的网络战指挥体系。舆论认为，组建网络司令部，意味着美国准备加强争夺网络空间霸权的行动。网络战正在以一种全新的战争样式走上战争舞台。

组建网络司令部表明，美军研制多年的网络战手段已基本成熟，并做好了打网络战的准备。目前美军已经拥有大批网络战武器，在软件方面，已研制出2000多件“逻辑炸弹”等计算机病毒；在硬件方面，则研发了电磁脉冲弹、次声波武器、高功率微波武器，可对敌方网络进行物理攻击。尤其值得注意的是，美国利用其握有核心信息技术的优势，在芯片、操作系统等硬软件上预留“后门”，植入木马病毒，一旦需要即可进入对方网络系统或激活沉睡的病毒。

除美国外，英国、日本、俄罗斯、法国、德国、印度、朝鲜等国家都已建立成体系的网络战部队。

近年来，各种网络战手段已经在局部战争中得到多次运用。

早在1991年的海湾战争中，美军就对伊拉克使用了一些网络战手段。开战前，美国中央情报局派特工秘密打入伊拉克内部，将伊军购买自法国的防空系统使用的打印机芯片，换上了染有病毒的芯片，在空袭前用遥控手段激活病毒，致使伊军防空指挥中心主计算机系统程序错乱，防空计算机控制系统失灵。

在1999年的科索沃战争中，前南斯拉夫联盟共和国组织黑客，使用多种计算机病毒，使北大西洋公约组织（北约）的一些计算机网络一度瘫痪。北约方面也不甘示弱进行网络反击，在南军计算机网络系统中植入大量病毒和欺骗性信息，导致南防空体系失效失能。

2003年的伊拉克战争中，美军网络战手段升级，在战前就往数千名伊拉克军政要员的邮箱中发送“劝降信”，开战后4小时不到就封杀了持中立立场的半岛电视台，对伊军心士气造成极大打击。

2003年夏天，冲击波蠕虫在全世界范围传播，对于运行着Microsoft Windows系统的不计其数的主机来说简直就是场噩梦，同时给广大网民留下了悲伤的回忆。

从2008年年底开始，Conficker蠕虫病毒开始利用Windows操作系统的漏洞感染计算机系统，并开始广泛传播。截至2009年6月，已有数百万台计算机系统受到Conficker病毒的控制。

随着计算机及网络技术应用的不断发展，伴随而来的计算机系统安全问题越来越引起人们的关注。计算机系统一旦遭受破坏，将给使用单位造成重大经济损失，并严重影响正常工作的顺利开展。

计算机安全是一个涉及多知识领域的综合学科，只有全面掌握相关的基础理论和技术原理，才能准确把握和应用各种安全技术与产品。

2008年3月6日，全球计算机行业协会（CompTIA）公布了《全球IT技术状况》报告，评出了“全球最急需的10项IT技术”，“安全/防火墙/数据隐私类技术”排名第一。

1.1 计算机安全基本概念

在计算机系统中，所有的文件，包括各类程序文件、数据文件、资料文件、数据库文件，甚至硬件系统的品牌、结构、指令系统等都属于信息。

信息已渗透到社会的方方面面，信息的特殊性在于：无限的可重复性和易修改性。

信息安全是指秘密信息在产生、传输、使用和存储过程中不被泄露或破坏。信息安全涉及信息的保密性、完整性、可用性和不可否认性。综合来说，就是要保障信息的有效性，使信息避免遭受一系列威胁，保证业务的持续性，最大限度减少损失。

1. 计算机安全的4个方面

（1）保密性

这是指对抗对手的被动攻击，确保信息不泄露给非授权的个人和实体。采取的措施包括：信息的加密解密；划分信息的密级，为用户分配不同权限，对不同权限用户访问的对象进行访问控制；防止硬件辐射泄露、网络截获和窃听等。

（2）完整性

这是指对抗对手的主动攻击，防止信息被未经授权的篡改，即保证信息在存储或传输的

过程中不被修改、破坏及丢失。完整性可通过对信息完整性进行检验、对信息交换真实性和有效性进行鉴别以及对系统功能正确性进行确认来实现。该过程可通过密码技术来完成。

(3) 可用性

这是保证信息及信息系统确为接受者所使用，确保合法用户可访问并按要求的特性使用信息及信息系统，即当需要时能存取所需信息，防止由于计算机病毒或其他人为因素而造成系统拒绝服务。维护或恢复信息可用性的方法有很多，如对计算机和指定数据文件的存取进行严格控制、进行系统备份和可信恢复、探测攻击及应急处理等。

(4) 不可否认性

这是保证信息的发送者无法否认已发出的信息，信息的接收者无法否认已经接收的信息。例如，保证曾经发出过数据或信号的发送方事后不能否认。可通过数字签名技术来确保信息提供者无法否认自己的行为。

2. 计算机安全的组成

一般来说，计算机安全主要包括系统安全和数据安全两个方面。

(1) 系统安全

系统安全一般采用防火墙、防病毒及其他安全防范技术等措施，是属于被动型的安全措施。

(2) 数据安全

数据安全主要采用现代密码技术对数据进行主动的安全保护，如数据保密、数据完整性、数据不可否认与抵赖、双向身份认证等技术。

3. 计算机系统的可用性

可用性(Availability)是指系统在规定条件下，完成规定功能的能力。可用性的定量还可以表现为以下 3 个方面。

(1) 可靠性

如果系统从来没有故障，那么可用性就是 100%，但这是不可能的，所以引进一个辅助参数可靠性(Reliability)，即在一定的条件下，在指定的时期内系统无故障地执行指令任务的可能性。系统可靠性在数值的度量中采取可靠度衡量。

可靠度的定义是：在 t_0 时刻系统正常的条件下，在给定的时间间隔内，系统仍然能正确执行其功能的概率称为可靠度。可靠性测度有 3 种：抗毁性、生存性和有效性。可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性和环境可靠性等方面。

提高计算机的可靠性一般采取两项措施：避错和容错。

① 避错。提高软硬件的质量，抵御故障的发生。要求组成系统的各个部件、器件、软件具有高可靠性，不允许出错，或者出错率降至最低。通过元器件的精选、严格的工艺、精心的设计来提高可靠性。在现有条件下避错设计是提高系统可靠性的有效办法。

② 容错。对于一个系统来说，无论采用多少避错设计方法，对可靠性的提高都是有限的，总是不能保证永远不出错。因此发展容错技术，使得在发生故障时系统仍能继续运行，并提供服务与资源。容错设计是在承认故障存在的情况下进行设计的，是指在计算机内部出现故障的情况下，计算机仍能正确地运行程序并给出正确结果的设计。

(2) 可维修性

可维修性指系统发生故障时容易进行修复,以及平时易于维护的程度。

(3) 维修保障

维修保障即后勤支援能力。

1.2 计算机安全研究的重要性

计算机资源易受到自然因素和人为因素的不利影响,原因有以下几个:①计算机是电子技术产品,其所处理的信息也是各种电子信号;②系统运行是靠程序控制的,一个大型计算机信息系统具有数百万个受各种程序控制的逻辑联结;③自身抗外界影响的能力还比较弱,安全存取控制功能还不够完善;④其运行环境要求比较高;⑤现代化管理不够完善。

1. 计算机系统的脆弱性

计算机系统的脆弱因素包括以下几个方面。

(1) 数据输入部分:数据通过输入设备输入系统进行处理,数据易被篡改或输入假数据。

(2) 数据输出部分:经处理后的数据要在这里译成人能阅读的文件,并通过各种输出设备输出,信息有可能被泄露或被截取。

(3) 数据库部分:数据库存有大量的各种数据,有的数据资料价值连城,如果遭到破坏,损失是难以估计的。

(4) 程序部分:用语言写成机器能处理的程序,这种程序可能会被篡改或盗窃。

(5) 操作系统:操作系统是操纵系统运行、保证数据安全、协调处理业务和联机运行的关键部分,如被破坏就等于破坏了系统功能。

(6) 硬件部分:除软件以外的所有硬设备,这些电子设备最容易被破坏或盗窃。

(7) 通信部分:信息或数据要通过它在计算机之间、主机与终端之间及网络之间传送,通信线路一般是电话线、专线、微波、光缆,前 3 种线路上的信息易被截取。

(8) 电磁波辐射:计算机设备本身就有电磁辐射问题,也怕外界电磁波的辐射和干扰,特别是自身辐射带有信息,容易被别人接收,造成信息泄露。

(9) 辅助保障系统:水、电、空调中断或不正常,会影响系统运行。

(10) 存取控制部分:安全存取控制功能还比较弱。

(11) 自然因素:水、电、火、静电、灰尘、有害气体、地震、雷电、强磁场和电磁脉冲等危害。这些危害有的会损害系统设备,有的则会破坏数据,甚至毁掉整个系统和数据。

(12) 人为因素:安全管理水平低、人员技术素质差、操作失误或错误、违法犯罪行为等。

以上计算机的不安全因素说明,计算机自身的脆弱性十分严重。现在计算机已经应用到民航、铁路、电力、银行和其他经济管理、政府办公、军事指挥控制等国家重大要害部门或涉及全国性的大型信息系统之中,如果某个关键部分出了问题,不但系统内可能产生灾难性的多米诺反应,而且会造成严重的政治、经济损失,甚至危及人民生命财产的安全。如果系统中的重要数据遭破坏或某些敏感信息被泄露,其后果也是不堪设想的。

2. 计算机系统面临的威胁

由于信息系统的复杂性、开放性以及系统软硬件和网络协议的缺陷，导致了信息系统的安全威胁是多方面的：网络协议的弱点、网络操作系统的漏洞、应用系统设计的漏洞、网络系统设计的缺陷、恶意攻击、病毒、黑客的攻击、合法用户的攻击、物理安全、管理安全等。

另外，非技术的社会工程攻击也是信息安全面临的威胁，通常把基于非计算机的欺骗技术称为社会工程。社会工程中，攻击者设法伪装自己的身份让人相信他就是某个人，从而去获得密码和其他敏感的信息。目前社会工程攻击主要包括两种方式：打电话请求密码和伪造 E-mail。

计算机安全的实质是计算机资源存在着的各种各样的威胁。从造成这些威胁的人员对计算机的接近程度的不同，可以将其分为以下 4 类。

(1) 外部人员：不能进入计算机中心或机房的人员。由于外部人员不能进入计算机中心，因此他们只能在外面进行攻击，主要攻击目标是网络中的通信线路等外部设施，可能产生的威胁有以下几种。

① 搭线窃听：在计算机的通信线路上搭上一个侦听设备，从而获得线路上传输的机密信息。

② 电磁辐射：通过接受计算机系统辐射出的信号而获得机密信息。

③ 口令猜测：通过猜测口令而进入到网络系统中。

④ 密文分析：通过分析线路上传输的加密信息而得到明文。

⑤ 流量分析：通过观察通信线路上的信息流量，得到信息的源点和终点、发送频率、报文长度等，从而推断出信息的某些重要特性。

⑥ 愚弄：愚弄或欺骗计算机中心的人员，从而达到自己的非法目的。

防止这些攻击的唯一有效办法是：将通信线路上的信息加密，并且在网络中实行可靠的协议，防止信息在加密之前从机房中泄露出去。

(2) 物理存取人员：这类人员能进入计算机中心但没有多少上机的权利。

他们的主要攻击目标是计算机中心内部，可以产生如下一些威胁。

① 窃听：将窃听器安装在中心里，录下中心人员之间的谈话。

② 窥视：站在终端用户的身后，观察其操作过程。

③ 插入：当用户离开终端后，攻击者利用仍开着的终端做他自己的事情。

④ 蒙面：在计算机中心的某些地方，得到粗心大意的人写下的口令，从而冒称该人，使用机器。

⑤ 推导：从统计数据库中获得的统计信息出发，推导出某些不应该知道的信息。

⑥ 浏览：通过观察中心内部的情况或机器中的某些公用文件而获得有用的信息。

⑦ 废物：从当作废物的打印纸中寻找有用的信息。

⑧ 设备安装：攻击者将 EPROM 或类似的电路芯片替换并重新插入机器中，使机器按照攻击者的目的运行。

对于这些攻击，有效的防范办法是：加强机房的出入管理，包括人员的进出管理、记录机密信息的媒介出入机房的管理。

(3) 系统存取人员：这类人员通常是计算机中心的普通用户，他们在系统里拥有的权

利不是太多。

他们能够实际操作机器，具有较大的危险性，构成的威胁有以下几种。

① 强制崩溃：在程序中制造某些故意的错误，强制使机器停止运转。

② 天窗：有些操作系统为了日后的维护而留下了入口，攻击者可利用这些入口作为进入操作系统的天窗。

③ 聚合：将能合法得到的几项信息综合起来，从而知道一些不应该知道的保密信息。

④ 复制：将有关程序和数据复制下来带出计算机中心。

⑤ 骚扰：攻击者在终端上做出某些令操作员生气的事情，使其容易发生错误，从而达到自己的目的。

他们具有的特权比较少，很想扩大自己的特权，系统管理员要严密监视他们的工作，特别注意一些奇异现象的发生，如机器发生的崩溃次数太多等，要立即采取有效措施。

(4) 编程特权人员：这类人员能在计算机上编制自己的程序，通常是指那些系统编程人员和系统维护人员。

他们通常是能够深入到系统里面去的人，构成的威胁极大，有以下几种。

① 特洛伊木马：修改某些程序，使得这些程序仍能正常工作，看上去是好的，实际上其中隐藏着一些破坏性的指令。

② 逻辑炸弹：一种只有当特定事件出现才进行破坏的程序。

③ 病毒：实际上是一种逻辑炸弹，不同之处在于它不断地繁殖其自身。

④ 滥用实用程序：有些机器上的实用程序可以被修改以满足不同的需要，攻击者可利用实用程序达到自己的目的。

⑤ 意大利香肠术：这是对财务系统进行的攻击。它从每个客户的账目中偷出一点点钱，客户往往不注意这种微弱损失，而攻击者将众多客户的钱加在一起，其数目很大。

对于上面这些攻击很难防止。有效的办法就是加强管理，选择可靠的系统工作人员，记录这些人的行为，以便及时准确地发现蓄意破坏者。

总之，由于计算机系统的脆弱性以及面临的各种威胁，因此，计算机系统安全研究的重要性不言而喻。

1.3 计算机安全技术体系结构

计算机安全技术是一门综合的学科，它涉及信息论、计算机科学和密码学等多方面知识，它的主要任务是研究计算机系统和通信网络内信息的保护方法以实现系统内信息的安全、保密、真实和完整。一个完整的计算机安全技术体系结构由物理安全技术、基础安全技术、系统安全技术、网络安全技术以及应用安全技术组成。

1.3.1 实体和基础设施安全技术

物理安全在整个计算机网络信息系统安全体系中占有重要地位。计算机信息系统物理安全的内涵是保护计算机信息系统设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏。它包含的主要内容为环境

安全、设备安全、电源系统安全和通信线路安全。

(1) 环境安全

计算机网络通信系统的运行环境应按照国家有关标准设计实施，应具备消防报警、安全照明、不间断供电、温湿度控制系统和防盗报警，以保护系统免受水、火、有害气体、地震、静电等的危害。

(2) 设备安全

要保证硬件设备随时处于良好的工作状态，应当建立、健全使用管理规章制度，建立设备运行日志。同时要注意保护存储介质的安全性，包括存储介质自身和数据的安全。存储介质本身的安全主要是指安全保管、防盗、防毁和防霉；数据安全是指防止数据被非法复制和非法销毁，关于存储与数据安全这一问题将在第 2 章具体介绍和解决。

(3) 电源系统安全

电源是所有电子设备正常工作的能量源，在信息系统中占有重要地位。电源安全主要包括电力能源供应、输电线路安全、保持电源的稳定性等。

(4) 通信线路安全

通信设备和通信线路的装置安装要稳固牢靠，具有一定对抗自然因素和人为因素破坏的能力。它包括防止电磁信息的泄露、线路截获以及抗电磁干扰。

1.3.2 密码技术

随着计算机网络不断渗透到各个领域，密码学的应用也随之扩大。数字签名、身份鉴别等都是由密码学派生出来的新技术和应用。

密码技术(基础安全技术)是保障信息安全的核心技术。密码技术在古代就已经得到应用，但仅限于外交和军事等重要领域。随着现代计算机技术的飞速发展，密码技术正在不断地向更多其他领域渗透。它是结合数学、计算机科学、电子与通信等诸多学科于一身的交叉学科，它不仅具有保证信息机密性的信息加密功能，而且具有数字签名、身份验证、秘密分存、系统安全等功能。所以，使用密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性和确定性，防止信息被篡改、伪造和假冒。

密码学包括密码编码学和密码分析学，密码体制的设计是密码编码学的主要内容，密码体制的破译是密码分析学的主要内容。密码编码技术和密码分析技术是相互依存、相互支持、密不可分的两个方面。

从密码体制方面而言，密码体制有对称密钥密码技术和非对称密钥密码技术。对称密钥密码技术要求加密与解密双方拥有相同的密钥；非对称密钥密码技术是加密与解密双方拥有不相同的密钥。

密码学不仅包含编码与译码，而且包括安全管理、安全协议设计、散列函数等内容。不仅如此，密码学的进一步发展，涌现了大量的新技术和新概念，如零知识证明技术、盲签名、比特承诺、遗忘传递、数字化现金、量子密码技术、混沌密码等。

我国明确规定严格禁止直接使用国外的密码算法和安全产品，这主要有两个原因：一是国外禁止出口密码算法和产品，所谓出口的安全密码算法国外都有破译手段；二是担心国外的算法和产品中存在“后门”，关键时刻危害我国安全。当前我国的信息安全系统由国家