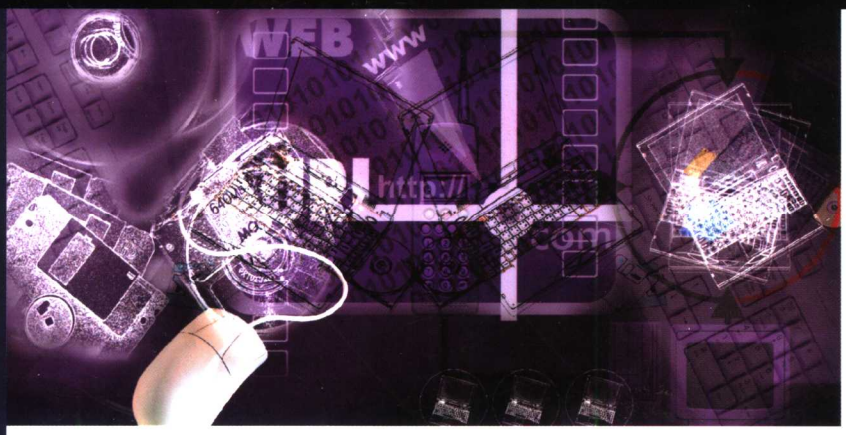

Data Security Techniques in Computer Science

计算机数据安全技术

凌 捷 编著

科学出版社
www.sciencep.com

计算机数据安全技术

凌　捷　编著

科学出版社

北京

内 容 简 介

本书介绍了计算机数据安全技术及相关的信息安全方面的知识。主要内容包括数据加密算法、数字签名技术、磁盘加密技术、信息隐藏技术、计算机反病毒技术、数据库安全技术、网络加密及网络防火墙技术等，涉及范围较广，知识内容较新，并在附录中提供了部分计算机信息安全管理方面的国家法规。

本书可作为从事计算机信息安全技术研究与开发的工程技术人员的参考资料，也可供计算机信息安全相关专业的大专院校高年级学生及研究生学习使用。

图书在版编目(CIP)数据

计算机数据安全技术/凌捷编著.—北京：科学出版社，2004
ISBN 7-03-013677-2

Ⅰ.计… Ⅱ.凌… Ⅲ.电子计算机-数据管理-安全技术
Ⅳ.TP309.2

中国版本图书馆 CIP 数据核字（2004）第 056186 号

策划编辑：吕建忠 / 责任编辑：陈砺川

责任印制：吕春珉 / 封面制作：东方人华平面设计部

科学出版社 出版
北京东黄城根北街16号
邮政编码:100717
http://www.sciencep.com

双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2004 年 7 月第 一 版 开本：B5（720×1000）
2004 年 7 月第一次印刷 印张：16 1/2
印数：1—4 000 字数：311 000

定价：24.00 元

（如有印装质量问题，我社负责调换〈环伟〉）

前　言

随着计算机技术的迅速发展与网络的普及，信息网络已成为社会发展的重要推动因素，计算机与网络技术的应用已渗透到政府、军事、文教与日常生活的各个方面。在社会经济生活中，有大量的重要数据，包括政府的宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据和科研数据等，其中有许多是敏感信息，甚至是国家机密的数据，这些数据需要存储、传送和交换，所以经常会吸引来自世界各地的各种人为攻击，包括信息窃取、数据篡改、数据删添、计算机病毒等，同时还要经受自然灾害等方面的考验，因此如何保护计算机数据的安全已成为计算机信息安全研究的热点，也越来越受到社会各界人士的关注。

本书是在作者近几年给硕士研究生讲授“数据安全技术”这门课程的基础上加以充实整理而成的。为了使本书能反映数据安全研究领域的最新理论和技术，我们参阅了国内外大量最新的研究文献，浏览了许多专业网站，也整理了笔者所在科研项目课题组的部分理论研究成果，努力使本书尽量接近数据安全研究的前沿，同时尽可能地用通俗易懂的语言和例子描述数据安全的基本理论、基本知识和常用技术，以适合不同层次的读者。

全书共分 8 章，第 1 章介绍了数据安全的概念，分析了数据安全面临的威胁；第 2 章介绍了三类主要的数据加密算法，包括对称加密算法、公开密钥算法和序列加密算法；第 3 章介绍了数字签名的原理及各种各样的签名方案；第 4 章介绍了磁盘加密技术和 USB 软件狗加密技术；第 5 章介绍了信息隐藏技术；第 6 章分析了计算机反病毒技术，特别介绍了这方面的国家法规；第 7 章分析了数据库安全的一般要求，特别介绍了通常的访问控制技术不能解决的一类统计数据库的安全问题及其解决方案；第 8 章介绍了计算机网络的加密方式和防火墙技术。

本书可作为从事计算机信息安全技术研究与开发的工程技术人员的参考资料，也可供计算机信息安全相关专业的大专院校高年级学生及研究生学习使用。

由于计算机数据安全技术涉及内容广，而且技术本身的发展十分迅速，难以在本书中全面地反映出来，书中难免存在一些疏漏和缺点，在此恳请有关专家和广大读者批评指正。

编　者

2004 年 1 月

目　录

第1章 绪 论

1.1 什么是数据安全

随着计算机科学技术的迅速发展与计算机在社会生活各个领域的广泛应用，计算机安全问题不仅成为计算机科学中一个重要的研究课题，也已经成为一个人们日益关心的社会问题。如在病毒和黑客横行的互联网上，人们越来越担心网上电子邮件传输、电子商务、电子支付过程中，重要数据是否被拦截、被篡改，敏感信息是否被泄漏、被假冒等。计算机安全所涉及的方面非常广泛，包括计算机道德教育、计算机安全条例及相关法规的研究和制定、对来自自然和环境的安全防护、对计算机硬件资源的安全管理、对人员合法身份的验证和确认、对计算机内所存放的数据（包括数据库、数据文件）的安全保护、各种安全产品的设计制造和使用等。本书的主要任务是研究其中的数据安全问题。

计算机能处理的数据来源包括数字、文本、语音、音乐、静止图像、视频图像、图形、动画等多种形式，这些数据经过数字化转化为 0 和 1 的二进制数据流而存储在计算机中。数据安全问题是计算机安全的一个核心问题，从技术的角度上看，数据安全的技术特征主要有以下几个方面：①数据的完整性（Integrity），指数据在存储或传输过程中保持不被偶然或蓄意地修改、删除、伪造、乱序、重置等的破坏和不丢失的特性；②数据的保密性（Confidentiality），是指数据防止数据泄漏给非授权个人或实体，只供授权用户使用的特性；③数据的可用性（Availability），指数据在需要时应可以被已授权的用户合法使用的特性。

计算机数据安全主要分为物理安全和安全服务两部分。

数据的物理安全是指在物理介质上对存储和传输的数据的安全保护，是数据安全的最基本的保障。这一类的不安全因素主要有自然灾害、物理损坏、电磁辐射、操作失误等。提供这一类的安全保护主要通过采取各种安全措施、制定安全规章制度、状态检测、报警确认、数据备份、应急恢复等来完成。

数据的安全服务是指通过对数据的存储、传输和处理过程的监控和管理提供的安全保护。这一类安全保护通常是通过数据加密、用户身份认证、访问权限控制、互连设备与接口模块的状态监控、防火墙等手段来实现的。

应该指出的是，数据与信息是有区别的。计算机中数据是用来记录和传送信息的，或者说数据是信息的载体。数据本质上是对信息的一种符号化表示，在计

算机上通常使用的是 0 和 1 这两种符号。信息是数据的内涵，人们通过解释、推理、归纳、分析、综合等方法，从数据中获得有意义的内容就是信息。例如，一个学生可用如下的数据记录来描述（5140204036，陈文，M，GZ，1985，2002）。对这样的记录，一般人可能不解其意，但大致知道这个记录含义的人，可以从中得知陈文是位男大学生，学号为 5140204036，1985 年出生，籍贯是广州，2002 年入学。而熟悉学号编码方法的人，更可以从中得知陈文是计算机系（5）、软件专业（1）、四年制本科（4）、2002 级（02）、4 班（04）第 36 号（036）学生。对于计算机和人类的推理和计算来说，真正有用的不是数据本身，而是数据所携带的信息。我们通过研究数据安全技术来实现信息的安全。

1.2 数据安全面临的威胁

数据安全所面临的威胁来自许多方面，并且随时间的变化而有所变化。一般可分为自然威胁和人为威胁两种。

自然威胁主要来自以下几种：

1. 自然灾害

自然灾害包括水灾、火灾、风暴、地震、雷击等，这些自然灾害对计算机的影响非常大，往往会使计算机遭受毁灭性的损坏。

2. 恶劣的场地环境

计算机是一种复杂精密的电子设备，对环境的要求很高，如它所处环境是比较恶劣的，那么计算机很容易发生故障，轻则造成工作不正常或缩短工作寿命，重则造成重大损坏。对计算机影响较大的环境因素有：

（1）温度

计算机工作环境的温度不能太高，也不能太低。当温度过高时，使集成电路内离子的扩散或漂移加剧，电子的运动速度加快，使穿透电流成倍增大，引起结温升高，如此循环下去将会引起热击穿，造成集成电路的损坏。据统计，当器件周围的温度超过 60℃时，计算机器件就可能会发生故障，稳定温度每升高 10℃，计算机可靠性就会下降 25%。当温度过高时，计算机机内电阻元件的阻值将会发生变化，电解电容器电介质中的水分容易蒸发，从而降低了容量。插头、插座和开关，在高温下由于热胀冷缩易产生接触不良。磁盘、磁带等精密机械由于热胀冷缩的影响会出现读写错误。温度过高或过低时，都会影响到晶体振荡器电路的时钟的主振频率，会造成器件失效和机械部分运转不正常。国内外计算机机房的温度要求一般定为：

机房温度为21℃±2℃，温度变化比不超过3℃/h；从人的舒适度考虑，冬季机房温度为16℃～23.5℃，夏季机房温度为8℃～26℃。从节能和舒适度出发，一般夏季取允许的上限温度值，冬季取允许的下限温度值为控制机房的温度值。

（2）湿度

湿度过高除了使工作人员感到不舒服外，还会使电子元件表面吸附一层水膜，当湿度为65%以上时，水膜厚度可达0.001~0.01μm（微米），这种水膜会造成“导电通路”，影响集成电路的电气性能，造成错误的逻辑判断。同时，湿度过高还会影响磁性材料的导磁率，造成磁盘、磁带的读写错误。湿度过高时接插件和集成电路的引脚等易氧化和生锈霉烂，造成接触不良或断路。湿度过高不利于导走空气中的静电。机房中各个转动的机器、活动地板等有摩擦的部件都易产生静电，当静电电荷大量积聚而使静电电压超过2kV（千伏）时，将会引起高速运转的磁盘、磁带读写错误，甚至烧坏场效应管等半导体器件。磁盘带静电将会吸附灰尘从而损坏磁头，划坏磁盘。当湿度为20%以下时，由于打印机、磁带机等转动与摩擦，将会使静电压高达10kV。当静电放电时，会产生瞬时干扰脉冲，造成微机故障。

国外计算机机房的湿度一般控制在45%~65%，相对湿度波动控制在每小时±6%。实践证明，机房的空气调节系统应具有加湿装置和去湿装置，并要求安装有湿、温度提示及自动调节装置。当相对湿度在30%以下时，计算机的故障发生率会急剧增加至正常情况的10~30倍。

（3）振动

计算机不能在经常振动的环境中工作，计算机磁盘驱动器中的磁头和磁盘在工作中的接触是非常精密的，稍为强烈的振动即会损坏磁头和磁盘。

（4）粉尘

粉尘对计算机的影响也非常大，粉尘的积聚也会给计算机造成漏电、静电感应、磁头磁盘磨损等故障。空气中含有直径在10μm以上的灰尘称为粗尘，它在空气中以加速度下降，在空气中停留时间很短；直径为0.1~10μm的灰尘称浮尘，它在静止空气中缓慢下降；直径在0.01～0.1μm的灰尘称为烟尘，在静止的空气中呈布朗运动而缓慢沉降。空气中的粉尘99%直径在1μm以下，而0.5μm以下的粒子约占90%。当空气中粉尘很大时，粉尘落在磁盘上将损伤磁头和磁层擦伤。磁头与磁盘间隙理论计算为2～3μm，而实际盘面并不是绝对水平，转动时也存在摆动，硬盘的转速一般为7200r/min（转/分），磁盘与磁头间的实际缝隙很小，转动时一般在0.8~1μm左右。当磁盘自身净化设备不良时，很易受大于1μm的尘埃的侵害，当温度梯度太大引起机械缺陷时，就会引起磁头、磁盘相碰，出现磁头划掉磁性涂层的现象，这样，不仅无法正确地进行读写信息，而且要损坏磁盘盘片和磁头。计算机的集成电路上吸附尘埃过多时，将会使元器件散热能力降低。

计算机外设及 UPS 电源等设备具有冷却通风过滤设备，当灰尘量太大时，容易堵塞过滤器，使机器内部温度过高，而影响机器正常运行。元器件内落入导电性尘埃后，使元器件间的绝缘性能降低或短路，同时也会造成插件接触不良。国外机房内空气含尘量一般要求不超过 1～0.75mg/m^3，尘粒粒径不大于 3μm。

3. 物理损坏

如意外的外力破损等。

4. 设备故障

1）设备硬件偶然失常。任何一种设备都不是十全十美的，或多或少都存在着这样或那样的缺陷。电子计算机是一种相当复杂的电子设备，存在的问题就更复杂。有时它会出现一些比较简单的故障，而有些故障则是灾难性的。计算机硬件机能失常往往会使计算机工作中断、功能失效，甚至破坏机内数据或其他外部设备，后果有时是十分严重的。当然软件系统的“BUG”造成的后果同样是严重的，它可能会发出错误的指令，使一些控制过程出现混乱甚至瘫痪。

2）设备使用寿命到期，导致永久性故障。

3）电源故障。由于各种意外的原因，计算机供电电源电压的过高、过低波动或突然中断，可能会造成计算机停止工作，如果这时计算机正在进行数据操作，这些数据就可能会出错或丢失；也有可能使计算机硬件或外部设备造成损坏。

5. 电磁辐射和电磁干扰

计算机辐射主要有四个部分：显示器的辐射、通信线路（连接线）的辐射、主机的辐射、输出设备（打印机）的辐射。计算机是靠高频脉冲电路工作的，由于电磁场的变化，必然要向外辐射电磁波。这些电磁波会把计算机中的信息带出去，犯罪分子只要具有相应的接收设备，就可以将电磁波接收，从中窃得秘密信息。据国外试验，在 1000m 以外能接收和还原计算机显示终端的信息，而且看得很清晰。计算机工作时，在开阔地带距其 100m 外，用监听设备就能收到辐射信号。计算机电磁辐射大致分为两类：第一类是从计算机的运算控制和外部设备等部分辐射，频率一般在 10MHz 到 1000MHz 范围内，这种电磁波可以用相应频段的接收机接收，但其所截信息解读起来比较复杂。第二类是由计算机终端显示器的阴极射线管辐射出的视频电磁波，其频率一般在 6.5MHz 以下。对这种电磁波，在有效距离内，可用普通电视机或相同型号的计算机直接接收。接收或解读计算机辐射的电磁波，现在已成为国外情报部门的一项常用窃密技术，并已达到很高水平。解决的措施主要有：①使用低辐射计算机设备；②对计算机机房或主机内部件加以屏蔽；③对计算机的辐射信号进行干扰，增加接收还原解读的难度，保护计算机辐射的秘密信息。

这些自然威胁的共同特点是突发性、自然性、非针对性。这类不安全因素不仅对数据安全造成威胁，而且严重威胁着整个计算机系统的安全，因为物理上的破坏很容易毁灭整个计算机信息管理系统以及网络系统。解决这类不安全隐患的有效方法是采取各种预防措施、制定安全规章、进行数据备份及有针对性地选择应用新技术等。

人为威胁又分为无意威胁和有意威胁。

无意威胁主要有：

1）操作失误。人比机器更容易出错，由于操作人员不经意、不小心、经验不足，以及对操作的错误理解等都可能产生误操作（如操作不当、未经许可使用、误用存储媒体、误删除、误格式化等）。计算机的设计如同其他电子设备一样，对于人为的误操作有一定的保护，使计算机不致于轻易出现误动作，但这种保护也不是十全十美的，即使是非常有经验的程序员也会在设计保护措施时留下某些漏洞或逻辑错误。一旦发生保护不了的误操作，就有可能产生不良后果。

2）能力缺陷。如编程经验不足、检查漏项、水平所限、维护不力等，它通常来自没有明显的恶意企图与目的的偶然事故。

人为的有意威胁是指通过攻击系统暴露的要害或弱点，使数据的完整性、保密性、可用性受到损害，造成不可估量的重大经济和政治上损失。人为的有意威胁是有目的的恶意攻击，这种攻击可以分为主动攻击和被动攻击。主动攻击是指以各种方式有选择地破坏数据（如修改、删除、伪造、添加、重放、乱序、冒充、制造病毒等）；被动攻击是指在不干扰计算机系统正常工作的情况下进行侦收、截获、窃取、破译、业务流量分析和电磁泄漏等。

对计算机的人为的攻击破坏具有明显的目的和主动性，这是计算机安全保密面临的最主要、最危险的威胁。主要的人为攻击有：

1）敌对势力的窃密和破坏。由于计算机系统所处的地位重要，所以它成为敌对情报机构、间谍和敌对分子、恐怖分子攻击破坏、窃取秘密的主要目标。他们采取的手段是多种多样的，主要的手段有通过搭线窃听或截取线路传输的信息，接收解调计算机电磁辐射信号，窃取或盗取数据磁盘以及计算机网络的密码和口令，通过联网线路寻找计算机的弱点和暗道，植入非法程序以骗取控制权限，或植入病毒感染计算机软件，非法复制、修改，甚至删除数据文件，破解密码窃取秘密军事经济情报，毁掉操作系统或系统文件，破坏计算机房或计算机实体，使计算机不能正常工作或陷于瘫痪。这类敌对攻击的目的很明确，所针对的也是一些有关国防、经济、科技、政治等方面的重要过程的控制管理计算机，一旦攻击成功，所造成的后果是很严重的，往往危及到一个国家的某一方面的安全。

2）内部人员的泄密和破坏。由计算机操作人员、安全管理人员、程序编制维

护人员本身进行的泄密、破坏行为对计算机系统安全保密造成的威胁是所有人为攻击中最具危险性和隐蔽性的，在某种程度上可以说是无法防备的。因为他们熟悉自己操作管理的计算机的一切弱点和秘密所在。这种计算机内部人员的作案原因很复杂，往往源于各种动机，有受雇于敌对分子或竞争对手的、有企图谋取非法利益的、有对上级或雇主不满而发泄报复的，甚至有出于变态心理的。

3）计算机犯罪。这里所指的计算机犯罪主要指为谋取非法权限或非法利益而进行的计算机入侵、盗用、诈骗、偷窃等行为，也包括制造和传播计算机病毒。计算机犯罪者既有计算机的合法用户，甚至内部人员，也有非法用户。他们在计算机犯罪过程中的操作是非法的操作，除了危及计算机各方面的安全保密性之外，还损害了其他用户的正当权益。

由于人为恶意攻击有明显的企图，其危害性相当大，给数据安全、系统安全带来巨大的威胁。人为恶意攻击具有下列特征：

1）智能性。从事恶意攻击的人员（如黑客）大都具有相当高的专业技术水平和熟练的操作技能，甚至有些人还是具有一定社会地位的部门业务主管，他（她）们在攻击前都经过周密预谋和精心策划。

2）隐蔽性。人为恶意攻击的隐蔽性很强，不易引起怀疑，作案的技术难度大。一般情况下，犯罪证据存在于软件的数据和信息资料之中，若无专业知识很难获取侦破证据。相反，犯罪行为人却很容易毁灭证据。

3）多样性。攻击手段千变万化，如窃听、流量分析、破坏完整性、重发、假冒、拒绝服务、资源的非授权使用、干扰、病毒等。

4）严重性。对金融、证券业的恶意攻击，由于资金数额巨大，往往会使金融机构和相关企业蒙受重大损失，也给社会稳定带来震荡；对军事、国防计算机系统重要数据的恶意攻击更可能危害到人们生命财产安全以及国家安全。

人为恶意攻击能得逞的原因是计算机系统本身有安全缺陷，其中有些安全缺陷可以通过人为努力加以避免或改进，有些缺陷则是各种折衷所必须付出的代价。较常见的安全缺陷有：

1）通信链路缺陷。在大规模的计算机网络信息系统中，由于终端分布的广泛性和地理位置不同，网络分布在几百至上千公里的范围内，通常用有线信道（同轴电缆、光纤等）和无线信道（微波、卫星信道等）来作通信链路。对有线信道而言，易受自然和人为破坏，非授权用户可以通过搭线窃听攻击侵入网内获得重要信息，甚至可以插入、删除信息。由于串音和电磁辐射，导致网络信噪比下降，误码率增加，信息的安全性、完整性、可用性受到威胁。无线信道的安全脆弱性更加显而易见，被动攻击几乎不可避免。

2）电磁辐射缺陷。计算机及其外围设备在进行数据处理时，会产生电磁泄漏，即电磁辐射。电磁辐射分辐射发射和传导发射。当计算机设备进行数据处理和传

输时，各种高频脉冲通过各种电器元件和分布参数的耦合、调制、迭加成一个包含有用信息的频带信号，由电源线、电缆、电话线等通信链路传导出去，造成信息泄漏。而当各种高频脉冲通过电路元件传导时，又会向空中以电磁波的形式辐射信息，导致信息泄漏。在计算机中以视频显示器的辐射发射最为严重。一些发达国家研制的设备能在1km以外收集计算机的电磁辐射信息，并且能区分不同计算机终端的信息。

3）引进技术缺陷。我国的计算机芯片基本依赖于进口，即使是自己开发的芯片，由于半导体技术与微电子精微制造技术落后，目前也需要到境外去加工，完全受制于人；引进外国的先进设备一般都不转让知识产权，不能获得完整的技术档案，为今后的扩容、升级和维护带来麻烦。更严重的是，有些引进设备在出厂时就隐藏了恶意的“定时炸弹”或“陷门”，在非和平时期，这些预设的机关可能会对我们的计算机系统构成致命的打击。

4）软件漏洞。有些软件甚至有些操作系统留有陷门，陷门一旦被发现，将带来严重的安全后果；有些软件预设有逻辑炸弹，对数据安全有严重威胁；有些数据库将原始数据以明文形式存储，留下被技术较高的入侵者从系统的后备存储器上窃取或篡改数据的隐患。

5）网络服务的漏洞。TCP/IP 协议是目前在因特网上最常用的协议，但由于TCP/IP通信协议在设计初期并没有考虑到安全性问题，留下许多安全漏洞。电子邮件是因特网上使用最多的服务，但是电子邮件的被窃、用户密码泄漏、受到病毒攻击却始终是压在网络用户，特别是商业用户心头的三块大石。匿名FTP是因特网上的一项重要服务，它允许任何网络用户通过FTP访问系统上的软件，但不正确的配置将严重威胁计算机系统的安全：FTP虽然是一个合法的账户，但它不应该具有可工作的Shell，任何以FTP登录到系统的用户都不应该具有创建文件和目录的权限，因为黑客完全可以在一个具有写权限的目录内设置一个特洛伊木马，静静地等待用户上钩。远程登录可以给用户带来很大方便，但同时也给黑客提供了便利的入侵机会，给数据安全带来极大威胁：在网络上运行如rlogin、rcprexec等远程命令时，由于要跨越一些网络的传输口令，而TCP/IP对所传输的信息又不进行加密，所以网络黑客只要在所攻击的目标主机的IP包所经过的一条路由上运行“嗅探器”程序，就可以截取目标口令。

第 2 章　数据加密算法

消息（Message）被称为明文（Plain Text），用某种方法伪装消息以隐藏它的内容的过程称为加密，加密后的消息称为密文（Cipher Text），把密文转变为明文的过程称为解密。使消息保密的技术和科学叫做密码编码学，而密码分析学则是破译密文的科学和技术，即揭穿伪装。计算机密码学包括密码编码学和密码分析学两部分。

密码系统一般由算法以及所有可能的明文、密文和密钥组成的。基于密钥的算法通常有两类：对称算法和公开密钥算法。

对称算法是指算法的加密密钥能够从解密密钥中推算出来，反过来也成立。在大多数对称算法中，加解密密钥是相同的。这类算法也叫秘密密钥算法或单密钥算法，它要求发送者和接收者在安全通信之前，商定一个密钥。对称算法的安全性依赖于密钥，泄漏密钥就意味着任何人都能对消息进行加/解密。只要通信需要保密，密钥就必须保密。

对称算法可分为两类。一次只对明文中的单个位（有时对字节）运算的算法称为序列算法（Stream Algorithm）或序列密码（Stream Cipher）；另一类算法是对明文的一组二进制位进行运算，这些位组称为分组，相应的算法称为分组算法（Block Algorithm）或分组密码（Block Cipher）。现代计算机密码算法的典型分组长度为 64 位——这个长度大到足以防止分析破译，但又小到足以方便使用（在计算机出现前，算法普遍地每次只对明文的一个字符运算，可认为是序列密码对字符序列的运算）。

公开密钥算法（Public-key Algorithm，也叫非对称算法）是这样设计的：用作加密的密钥不同于用作解密的密钥，而且解密密钥不能根据加密密钥计算出来（至少在合理假定的长时间内）。之所以叫做公开密钥算法，是因为加密密钥能够公开，即陌生者能用加密密钥加密信息，但只有用相应的解密密钥才能解密信息。在这些系统中，加密密钥叫做公开密钥（Public Key，简称公钥），解密密钥叫做私人密钥（Private Key，简称私钥），私人密钥有时也叫秘密密钥。为了避免与对称算法混淆，此处不用秘密密钥这个名字。

密码编码学的主要目的是保持明文（或密钥，或明文和密钥）的秘密以防止偷听者知晓。这里假设偷听者完全能够截获收发者之间的通信。密码分析学是在不知道密钥的情况下，恢复出明文的科学。成功的密码分析能恢复出消息的明文或密钥。密码分析也可以发现密码体制的弱点，最终得到上述结果。

对密码进行分析的尝试称为攻击（Attack）。常用的密码分析攻击有如下五类：

1）惟密文攻击（Ciphertext-only Attack）。密码分析者得到一些消息的密文，这些消息都用同一加密算法加密。密码分析者的任务是恢复尽可能多的明文，或者最好是能推算出加密消息的密钥来，以便可采用相同的密钥解出其他被加密的消息。密码分析者已知的东西是：①加密算法；②待破译的密文。

2）已知明文攻击（Known-plaintext Attack）。密码分析者不仅可得到一些消息的密文，而且也知道这些消息的明文。分析者的任务就是用加密信息推出用来加密的密钥或导出一个算法，此算法可以对用同一密钥加密的任何新的消息进行解密。密码分析者已知的东西是：①加密算法；②待破译的密文；③由密钥形成的一个或多个明文-密文对。

3）选择明文攻击（Chosen-plaintext Attack）。分析者不仅可得到一些消息的密文和相应的明文，而且他们也可选择被加密的明文。这比已知明文攻击更有效。因为密码分析者能选择特定的明文块去加密，那些块可能产生更多关于密钥的信息，分析者的任务是推出用来加密消息的密钥或导出一个算法，此算法可以对用同一密钥加密的任何新的消息进行解密。密码分析者已知的东西是：①加密算法；②待破译的密文；③由密码分析者选择的明文，连同它对应的由其密钥生成的密文。

4）选择密文攻击（Chosen-ciphertext Attack）。密码分析者已知的东西是：①加密算法；②待破译的密文；③由密码分析者选择的猜测性密文，连同它对应的由密钥生成的已破译的明文。

5）自适应选择明文攻击（Adaptive chosen-plaintext Attack）。这是选择明文攻击的特殊情况。密码分析者不仅能选择被加密的明文，而且也能基于以前加密的结果修正这个选择。在选择明文攻击中，密码分析者还可以选择一大块被加密的明文。而在自适应选择密文攻击中，可选取较小的明文块，然后再基于第一块的结果选择另一明文块，以此类推。密码分析者已知的东西是：①加密算法；②待破译的密文；③由密码分析者选择的明文，连同它对应的由密钥生成的密文；④由密码分析者选择的猜测性密文，连同它对应的由密钥生成的已破译的明文。

另外还有至少两类其他的密码分析攻击方法，包括选择密钥攻击和软磨硬泡攻击（Rubber-hose Cryptanalysis）。

上述攻击中，惟密文攻击是困难的攻击，因为密码分析者可利用的信息最少，有时甚至对明文是英语文本还是法语文本或是中文文本或是账本文件都需猜测。但是，在许多情况下，密码分析者有更多的信息，除了密文外，还能获取一段或多段明文，或者可能知道某种明文模式将出现在某个消息中，此时可以进行已知明文攻击。如果密码分析者能在加密源系统中插入由分析员选择的消息，则可进行选择明文攻击。其他两种类型的密码分析：选择密文攻击和自适应选择明文攻击较少使用，但无论如何是可能的攻击途径。

对密码设计者而言，被设计的加密算法一般要能经受得住已知明文攻击。如