计算机安全保密技术

谢冬青 编著

湖南大学出版社

内 容 简 介

本书从计算机安全保密的一般概念、原理、方法入手，介绍了计算机安全保密技术的基本知识。全书共10章，内容包括：计算机安全概论、密码学基础、数据加密标准、RSA体制、其它主要的公开密钥密码体制、公开密钥密码的安全性准则与破译技术、密码学应用新领域、计算机病毒、磁盘加密技术、INTERNET网络安全技术及防火墙产品等。

本书可作为大专院校计算机、通信工程、电子工程、应用数学各专业教材，也可供有关工程技术人员参考。

计算机安全保密技术

Jisuanji Anquan Baomi Jishu

谢冬青 编著

□责任编辑 陈灿华

□装帧设计 谭石山

□出版发行 湖南大学出版社

社址 长沙市岳麓山 邮码 410082

电话 0731-8821691 0731-8821315

□经 销 湖南省新华书店

□印 装 国防科技大学印刷厂

□开本 787×1092 16开 □印张 11.5 □字数 266千

□版次 1998年10月第1版 □1998年10月第1次印刷

□印数 1—3 500册

□书号 ISBN 7-81053-161-1/TP·16

□定价 14.80元

前 言

随着计算机在政治、经济、文化等许多领域的广泛应用，人们在公开场合逐步深入研究计算机安全保密技术。如今，Internet 迅猛发展，电子商务方兴未艾，对计算机安全保密技术提出了越来越高的要求。

20 世纪 70 年代中期，数据加密标准(美国)和公开密钥密码的提出树起了密码学历史上的两个里程碑。由于出现了强有力的基于加密的协议，并开辟了计算机安全保密技术新领域，计算机安全保密技术得到了飞速发展。80 年代末期出现的零知识证明反过来为计算机科学中一些悬而未决问题的解决提供了新的思路，它是一个非常活跃的科研领域，可以为众多的实际工作服务。

信息安全技术有自身的特殊性，一方面大量数据共享和互通要求有共同认可的使用方便的安全产品，小生产方式研制安全产品经济上不合算、安全性无法保证，也要求有相对标准化的产品；另一方面，如果某一标准在相当大范围甚至全世界使用，一旦找到一种可行的破译方法，不仅标准本身要修改，而且从前的大量数据也会暴露，损失将是巨大的；再者，尽管公开了算法，但是如果不公开高层的设计思想和设计原则，那么即使这种算法能经受世界范围的攻击，也难保没有设置“陷井”。因此有人强调密码算法的个性化、非标准化。国际标准化组织(ISO)已经决定放弃 DES 为国际标准，同时宣布不再将任何算法标准化，CCITT 也正式宣布今后不会推荐密码算法。我国的政策是：安全产品的关键技术应走一条纯中国化的道路，安全产品由国家密码管理委员会统一管理，由授权开发商统一研制，在国内销售的安全产品需经过统一注册、认证。涉及到国家政治、经济的重要信息安全系统应全部采用国内安全产品。

本书介绍了计算机安全保密技术的一些基本知识，重点是 20 世纪 70 年代以后的现代安全保密技术，并力图将读者的眼光引向最新成果。囿于篇幅，本书重点介绍算法而不是程序。

本书是在内部讲义的基础上经多次修改而成的，在编写过程中，硕士生綦科、冷健、戴正兵提出了许多修改意见，在此深表感谢。由于作者水平有限，书中缺点和不足在所难免，诚恳地期待读者们批评与指正。

谢冬青
于长沙岳麓山
1998 年 8 月

目　次

第一章　计算机安全概论

第一节　引　言

从狭义的保护角度来看，计算机安全包含了信息的保密性、信息的完整性、防止拒绝服务。信息的保密性是保护信息不为非授权用户掌握；信息的完整性是保护信息不致被非法篡改或破坏；拒绝服务包括临时降低系统性能、系统崩溃而需人工重新启动以及数据永久性丢失。历史上，政府、企业的投资、专业人员的兴趣主要在信息的保密性上。

20 世纪 70 年代以来，信息的保密技术被应用于数据完整性保护，取得了巨大的进展，而对拒绝服务的研究进展缓慢，因为它牵涉到结构化开发、诊断与容错、软件可靠性等许多方面。

广义的信息保护还包括信息设备的物理安全性，诸如场地环境保护、防火措施、防水措施、静电防护、电源保护、空调设备、计算机辐射和计算机病毒等。

尽管近年来计算机安全技术取得了巨大的进展，但计算机信息安全性比以往任何时候都更加脆弱。体现在：

(1) 计算机领域中任何大的技术进步都对安全性构成新的威胁。所有这些威胁都需要新的技术来消除，而且技术进步的速度要比克服方法进步的速度快得多。

(2) 网络的普及，使信息共享达到了一个新的层次，信息被暴露的机会大大增多。

(3) 尽管操作系统都是有缺陷的，但可以通过版本的不断升级来克服，现有的版本是可靠的，能完成基本设计功能。而计算机安全的每一个漏洞都会使系统的所有安全控制毫无价值。

(4) 安全性的地位总是列在计算机系统总体设计规划的最后面，它首先考虑的是系统的功能、价格、性能、兼容性、可靠性、用户界面。

(5) 计算机安全本身也带来了一些约束，例如，采取措施不规范，既干扰了诚实用户的工作，又使诚实用户对过程控制、安全措施不熟悉。

计算机安全的目的不在于系统百分之百安全，而应当使之达到相当高的水平，使入侵者的非法行为变得极为困难、危险、耗资巨大，获得的价值远不及付出的代价。

许多数据表明，现有的计算机非授权使用及欺骗行为大多数是非技术性的。计算机犯罪的突破口往往选择在过程控制和人员控制的薄弱点上，而不是在内部技术控制的薄弱点上。由于非技术性的偷窃行为相对容易得手，它已成为计算机犯罪的主要途径，但是计算机可以保护自身免受错误的过程控制的威胁，计算机内部的技术性控制可以减轻过程控制的负担，比如计算机的威胁来自被解雇的职工，这是很危险的。这类人事问题，计算机本身无法解决，但可以通过为系统配置必要的设备而顺利解决。在非技术性犯罪途径被有效控制以后，技术性犯罪将成为主要犯罪手段。

计算机安全有其自身的特殊性，其关键技术应该走一条纯中国化的道路。我国的密码将由

新成立的国家密码管理委员会统一管理，由授权开发商统一研制。在国内销售的信息安全产品需通过统一认证，涉及到国家政治、经济的重要信息安全系统应全部采用国内安全产品。

第二节　计算机系统硬件资源的安全与管理

一、计算机硬件设备的使用管理

计算机系统的硬件设备一般价格昂贵，一旦被损坏而不及时恢复，不仅造成设备上的经济损失，而且可能导致业务瘫痪，影响信誉，产生不良的社会影响。因此，首先要加强计算机硬件设备的使用管理，坚持做好日常维护和保养工作。

（一）计算机硬件设备的使用管理

（1）要根据硬件设备的具体配置情况，制定切实可行的硬件设备的使用操作规程，并严格按操作规程进行操作。

（2）建立设备使用情况日志，并严格登记使用过程的情况。

（3）建立硬件设备故障情况登记表，详细记录故障性质和修复情况。

（4）坚持对设备进行例行维护和保养，并指定专人负责。

（二）常用硬件设备的维护和保养

（1）主机的维护保养。包括：

- 严禁带电进行设备（包括打印机、显示器、键盘、鼠标、网络线等）的插拔。
- 严禁在运行过程中挪动主机。
- 定期打开机箱（一般半年一次）进行机内除尘。用干净毛刷将机内线路板上各元器件和导线上的灰尘轻轻刷掉。

（2）显示器的维护保养。包括：

- 定期打开显示器后盖（一般半年一次）进行机内除尘。用干净毛刷将机内线路板上各元器件和导线上的灰尘轻轻刷掉。
- 亮度不宜开得太大，以防显像管老化。
- 显示屏应每天用软布擦拭。

（3）键盘的维护保养。包括：

- 键盘上严禁放置大头针、回形针等物品，防止发生短路等故障。
- 按键力度要适中，不能用力太大。
- 键盘接触不良很可能是灰尘积累造成的，应定期拆开键盘板刷除灰尘，并用绸布蘸无水酒精细擦触点。

（4）软盘、软驱的维护保养。包括：

- 使用软盘时切忌用手触摸盘片上的读写窗口。当盘片使用完毕从驱动器中取出后应立即放入纸套中。在驱动器指示灯亮时，切勿取盘。
- 软盘不能弯曲、折叠、重压和靠近强磁场，并应垂直放置。
- 软盘标签纸应事先写好再贴到盘片上，切勿贴上后再用硬笔写字。
- 软盘驱动器长期使用后，磁头会变脏，应用清洗盘清洗。清洗时应严格掌握清洗时间。
- 软盘驱动器的机械部分不能加油，以防沾染灰尘，导致磁头定位错误。

(5) 打印机的维护保养。包括：

· 应在断电情况下连接打印机与主机或终端电缆，以防烧坏芯片。

· 严禁在通电情况下拨动打印头。

· 使用不同厚度的打印纸时，应调整打印头的位置，以免折断打印针。

· 应经常清洗打印头(用软质毛刷蘸上无水酒精清洗)。

· 经常检查色带，当发现色带有破损或打印字迹很淡时，应及时更换。

(6) 硬盘使用注意事项。包括：

· 主机电源关闭后，要间隔至少 30 s 以后才能再次开机。

· 硬盘指示灯亮或主机开机后处于自检状态时，不宜用热启动方式启动机器，以防划伤盘面。

(7) 稳压器、不间断电源(UPS)在使用时要注意散热，散热不良容易引起故障。还要对 UPS 定期进行切断市电的试验，确保供电不间断。

(8) 应经常检查清洗空调的过滤网，以保持制冷或制热效果。

(9) 要定期检查供电系统的各种保护装置及地线是否正常。

二、计算机机房的安全管理

众所周知，计算机主机及大部分外部设备是放在计算机机房中的，业务处理程序以及业务数据是存放在计算机磁盘上的。因此，加强机房的安全管理至关重要。一般地说，计算机机房的安全管理应包括下面几个方面的工作。

(一) 严格保持机房的环境条件参数值在规定的范围内

如温度保持在 15～30 ℃(开机)，5～30 ℃(关机)；相对湿度要求为 40%～70%(开机)，20%～80%(关机)；噪音小于 68 dB；清洁度要求机房尘埃颗粒直径小于 0.5 μm，平均每升空气含尘量小于 1 万颗。

温度过低会导致硬盘无法启动，过高会使元器件性能发生变化，耐压降低，导致不能工作。统计数据表明：温度超过规定范围时，每升高 10 ℃，机器可靠性下降 25%。

湿度过高，会加速金属器件的腐蚀，引起绝缘性能下降，灰尘的导电性增强，耐潮性能不良和器件失效的可能性增大；湿度过低、过于干燥会导致计算机中某些器件龟裂，印刷电路板变形，特别是静电感应增加，对计算机带来危害。

灰尘会造成接插件的接触不良、发热元件的散热效率降低、绝缘破坏，甚至造成击穿；灰尘还会增加机械磨损，尤其对驱动器和盘片，灰尘不仅会使读出、写入信息出现错误，而且会划伤盘片，甚至损坏磁头。

(二) 机房管理要贯彻双人制度

坚持双人开、关机，双人维护和进行数据备份。

(三) 建立健全机房管理规章制度，经常对有关人员进行安全教育，定期或不定期地进行安全检查

机房管理规章制度主要包括以下几个方面：

(1) 机房门卫管理。机房门卫要落实到人，任何人进入机房均要更换工作衣、鞋，严格进行机房出入登记；与机房管理无关人员未经许可不准进入机房；机房内不准会客，参观人员须经领导批准并由专人陪同参观；严禁将易燃、易爆、腐蚀性、强磁性的物品带入机房；严禁将与工作无关的物品带入机房，特别是外来软盘。

(2) 机房安全工作。开机前要认真检查电源和空调设备工作是否正常；严格值班制度，值

班人员要认真填写值班日记；机房应具有防火、防水、防潮、防盗、防鼠害、防破坏等设施；机房工作人员必须严格执行《保密法》的规定，严守保密纪律，凡机房内使用过的废纸杂物，必须按规定进行烧毁或坏碎。

（3）机房卫生工作。每天对机房地板进行吸尘打扫，定期对机房除尘；机房内严禁吸烟、喝水、吃东西；不准随便乱扔废纸、杂物。

（4）机房操作管理。机房要加双锁，双人开关机房；为每台机器建立档案记录，将每天机器运转情况如实登记；非操作人员不准上机操作和拨动机房内的各种开关；机器发生故障时，操作人员应认真记录故障现象和有关信息，及时报告领导，通知维护人员进行维护。

第三节　计算机信息资源的安全与管理

除硬件资源以外的资源一般都属于信息资源，信息资源的安全管理包括程序、数据、信息网络、信息存贮等的安全管理。

一、信息存储的安全管理

计算机处理的结果（信息）要存贮在具体的媒体上，常用的媒体有：磁盘、磁带、打印纸、光盘。信息存贮的管理实际上就是对存放有信息的具体媒体的管理。

（1）存放有业务数据或程序的磁盘、磁带或光盘，应视同文字记录妥善保管。必须注意防磁、防潮、防火、防盗，必须垂直放置。

（2）对硬盘上的数据，要建立有效的级别、权限，并严格管理，必要时要对数据进行加密，以确保硬盘数据的安全。

（3）存放业务数据或程序的磁盘、磁带或光盘，管理必须落实到人，并分类建立相应的登记簿，记录编号、名称、用途、规格、制作日期、有效期、使用者、批准者等。

（4）对存放有重要信息的磁盘、磁带、光盘，要备份两份并分两处保管。

（5）打印有业务数据或程序的打印纸，要视同档案进行管理。

（6）凡超过数据保存期的盘带、光盘，必须经过特殊的数据清除处理，否则不能视同空白盘带、光盘。

（7）凡不能正常记录数据的盘带、光盘，须经测试确认后由专人进行销毁，并做好登记工作。

（8）对需要长期保存的有效数据，应在盘带、光盘的质量保证期内进行转贮，转贮时应确保内容正确。

二、信息的使用管理

计算机中的信息是文字记录、数据在计算机中的表示形式，对它的安全控制关系到国家、集体、个人的安全利益。必须加强对信息的使用管理，防止非法使用。

（1）程序和数据的使用一般采用级别、权限来管理。系统管理员、运行管理员、操作员、软件开发人员、主管人员等各自均有自己的使用级别和权限。

（2）程序和数据必须严格保密，未经上级主管部门同意，一律不准对外提供任何数据和程序。

（3）程序和数据除按规定进行拷贝以外，任何人不得以任何借口和形式进行拷贝。

(4) 程序对操作要进行控制，特别是要对非法操作、出错操作进行控制。

(5) 对数据的修改不得用系统提供的工具直接进行，应在应用程序的控制下采用程序提供的功能进行必要的改动，并详细记录。

三、信息网络的安全管理

计算机应用已由单机使用过渡到计算机联网，随着网络的建设和运行，计算机网络安全已成为计算机安全的焦点之一，必须加强对信息网络的安全管理。

(1) 在网络建设时，要采用网络安全控制技术，确保计算机网络安全、可靠运行。

(2) 加强对整个网络系统的监控，及时产生错误报告，给出错误统计，根据操作情况，判断有无非法用户进入网络，以便随时采取措施，保护系统安全。

(3) 加强审计，特别是对数据库操作的审计，对数据库情况进行监督，对访问数据库进行跟踪，对删改操作进行记录，以便于查找事故原因，分析处理问题。

(4) 加强数据备份。对数据库文件和系统文件都要进行多种备份，以便一旦出事，可以迅速恢复。

(5) 采取必要的保密措施，防止信息在传输过程中泄密。主要措施有：数据加密，采用光纤作为主要通讯手段，验证和授权，入网检查等。

第四节　计算机应用系统的安全与管理

一、计算机应用系统的特点

将计算机用于各种不同的场合，从而形成各种不同的计算机应用系统，具有如下的特点：

(1) 综合性。计算机用于某种具体的应用，建立完善的满足应用要求的计算机应用系统，既要掌握计算机硬件方面的知识，又要精通计算机软件开发方面的技术，还要熟悉了解具体的应用业务。计算机应用系统的建设人员只有具备多方面的专业知识和经验，才能将各方面的知识和技术有机地结合起来，按照规范要求，采用科学的方法进行系统的建设。

(2) 过程性。计算机应用系统从提出设想、制定规划到项目实施并投入实际应用，要经过若干个相对独立的阶段(即系统规划阶段、系统分析阶段、系统设计阶段、系统实施阶段、系统运行和维护阶段)才能实现。这些阶段构成了计算机应用系统建设的一个完整的过程。

(3) 复杂性。计算机应用系统的建设常常需要几人、几十人甚至数百人、数千人工作1年，开发成百上千个程序模块。应用系统各部分之间的关系、系统调度与管理等是一个相当复杂的问题。

(4) 长期性。计算机应用系统研制周期少则1年，多则数年。耗资数万、数十万乃至数百万、数千万元。

计算机应用系统的上述特点，给管理提出了新的要求，具体包括：计算机应用系统的应用环境建设管理，计算机应用系统的应用过程管理及计算机应用后的组织管理。

二、计算机应用系统的应用环境建设管理

计算机应用系统的应用环境建设管理主要包括：计算机应用系统的硬件、软件支撑环境建设管理。

（一）硬件支撑环境建设管理

（1）供电系统的建设管理。包括：

· 采用UPS加蓄电池组保证不间断供电5～10 h，确保业务处理系统不会因电压不稳、掉电等原因而瘫痪。

· 地线的埋设应满足接地电阻小于4 Ω的指标，计算机地线应与避雷针地线、UPS地线等严格分开，交流地线和直流地线也要分开。良好的接地是计算机系统安全可靠运行的必要条件之一。

（2）通讯线路建设要确保质量，在装机使用前，要对通讯线路进行全面测试，确认所有技术指标在规定的范围内。

（3）机房建设。机房建设要讲究科学合理，防止片面追求装潢的豪华而忽视对机房的技术要求。一般地说，要考虑下面几方面因素：

· 机房选址。要便于应用网络系统的建立，主机房应建在业务集中、进行监督的地区。

· 机房面积。机房面积的确定除了要有足够的空间放置计算机系统和电源等辅助设备外，还要考虑将来的业务扩充需要及系统维护的要求等。

· 屏蔽措施。根据机房所处的环境，整个机房分别用导磁率高（如铁）和导电率高（如铜、铝）的金属板或框架包围起来，以屏蔽干扰磁场和干扰电场。

· 要采用合理的调温、隔音、湿度调节、防尘、防火系统。

（4）机型选择。机型选择要合理，验收要严格，安装调试要正确。

· 选择机器的基本原则。在调查研究的基础上，选择技术先进、后援可靠、软件丰富、结构简单、稳定性好、可靠性强、便于推广应用、扩充和维护的计算机系统。

· 作好机器的验收工作。一是资料验收，包括技术手册、安装指南、操作手册、维修手册、用户手册和随机的软件（盘、带、光盘）等资料；二是硬件设备验收（包括有无机器损坏），清点机器及附件数目，检查所配的插件种类是否齐全。通电就地进行抽检调试，运行软件及诊断程序，进行机器性能测试；三是签订保退保换及维修方式、付款方式方面的合同，一般应建立保修制度，并签定保退保换或免费维修协议。

· 作好机器设备的安装调试工作。机器设备的安装应在技术人员的精心安排下严格进行，安装前应拟定较为严格的安装步骤。

（二）软件支撑环境的建设管理

计算机软件分为系统软件和应用软件，软件支撑环境建设主要是系统软件的管理。

（1）所有软件（如操作系统、编译系统、开发系统等），都要采用正版软件，严禁使用盗版软件。

（2）选用的支撑软件要与硬件环境相匹配，并可较好地支持应用程序。

（3）操作系统的选择，要选用系统安全性好、运行效率高且符合国际规范的系统。

三、计算机应用系统的应用过程管理

计算机应用系统从规划到投入运行，要经历一个比较漫长的过程，在这个应用过程中，要加强管理，确保应用的顺利进行。

（一）采用科学的系统开发方法，加强对应用软件开发的管理

软件开发本身是一项复杂的工程，同其他工程一样，除了面临技术方面的问题外，还有许多管理方面的问题。

软件开发常用生命周期方法，其主要思想是从时间的角度，将一个庞大而又复杂的系统建

设项目，分解成若干个容易实现、容易控制的阶段，每阶段有相对独立的任务，然后逐步完成每个阶段的任务。通常前一阶段任务的完成是后一阶段工作开始的前提和基础，而后一阶段的任务则是使前一阶段提出的解法更进一步具体化。因此，按照这种工程方法，无论是多大的工程，或是多么复杂的系统，都可以有条不紊地分步骤、分阶段地去成功地建设。通常将软件开发过程分为可行性研究、需求分析、系统设计、系统实现(程序设计等)、系统测试和软件验收等 6 个阶段。

软件开发管理通常包括计划管理、任务管理、变更管理、进度管理、质量管理、资源管理和成本管理等 7 个方面。

(1) 计划管理。它是保证一项工程顺利完成的有力措施，在工程开始之前，必须制定一套周密而又完整的计划。计划管理主要包括计划制定和计划调整两个方面。

计划制定主要涉及时间、资源、成本 3 个方面。时间计划将工程中每个任务规定起止时间，按时间顺序把各项任务排列起来，得到一个工程施工时间表；资源计划是指根据时间计划表，确定各个任务所需资源的情况，即所需的人力、设备等方面的情况。在资源计划中，人力资源是最重要的部分。因人力是工程中最昂贵、最活跃的资源，人力资源的合理使用是工程成功的决定因素之一，这就要求主管人员对人力资源的安排和分配要尽可能地准确、合理。也就是说要做到人尽其才；成本计划是指在工程的资源计划基础上，根据各个阶段的资源需求，做出该工程项目开发的成本预算。

计划调整主要指在每个开发阶段完成之后，对该工程项目的计划执行情况进行检查，根据工程实际进展情况，对工程以后各阶段的计划、资源和成本预算等进行适当调整，使工程计划更加符合工程实际。

(2) 任务管理。它是对软件开发工程中的各个任务进行具体的分配和调度，以保证每个任务的顺利进行。任务的分配是把工程计划中的各项任务，按照工程进展的需要，分配给开发人员。分配时，可视任务的工作量、工作进度、工作方式，将一项任务分配给一个人或几个人共同完成。任务被分配后，项目的负责人要将该任务的资料输入计算机，进行任务的监督统计，在工程进行过程中，如发现进度不理想，可随时进行任务的再调度，以保证工程的进度要求。

(3) 变更管理。它是指对方案实施过程中的任何变动进行控制和管理。变更管理的方法是指划定变更管理的范围，设立变更管理小组，建立变更管理制度。变更管理范围是指在工程实施过程中，凡是对经过批准或决定的工程项目的全部或部分产生影响的变更，均须通过变更管理小组讨论，提出建议后，才能由开发部门签批付诸实施。变更管理小组是决定各种变更是否执行的权力机构。建立变更管理制度是指履行变更应遵循的审批和执行步骤，这一步骤通常由变更发起者填写“变更需求书”，交变更管理小组。对于紧急变更，应立即召集会议讨论；对可缓变更，可到例会时再提出讨论。通过这一整套的制度，使工程中的变更能得到有序的控制。

(4) 进度管理。其目的是使工程管理人员能及时了解工程进展情况，同时，根据工程的实际情况对工程中的任务、资源和成本等计划做出适当的调整，使工程能按预期的目标顺利进行。

(5) 质量管理。它是软件工程管理中最重要的一项管理，是保证工程项目能否达到预期目标的重要措施。质量管理的方法较多，但最重要的方法是产品审批制度，也就是软件工程中采用的技术审查和管理复审制度。这一制度要求，在软件开发的每个阶段都采用科学的管理技术和方法，在每个阶段结束之前都从技术和管理两个角度进行严格的审查，只有合格才能开始下一阶段的工作。这就使软件开发工程的全过程以一种有条不紊的方式进行，保证了软件的质

量。

(6) 资源管理。在软件开发过程中，必须有计划、持续地对软件开发所需要的各种资源进行管理。只有通过管理，才能保证有限的资源得到充分的利用，促使工程顺利完成。

(7) 成本管理。软件工程的成本管理主要包括成本预算和成本核算两个方面。成本预算是指在工程开始制定计划时，对该工程中使用的人力、计算机资源等方面的消耗进行估计，并根据该项工程对这些资源的使用情况和收费标准做出成本预算，供工程管理人员参考。成本核算是指在工程结束时，全面地核算工程开支，准确计算出工程使用经费即最终成本。

(二) 系统建设要满足标准化的要求

标准化问题是计算机应用中的一个重要课题，在计算机应用系统的建设过程中应引起特别重视，使所建设的系统符合国际、国内标准，提高系统的通用性，实现系统之间的信息交换，以满足各种业务活动的要求，增强应用系统的生命力。

(三) 要按计划，有步骤地进行应用系统的开发、推广使用和维护

应用软件开发完成后，并不意味着应用系统建设已经完成，要将开发的应用系统成功地应用于实际，还有很多工作要做，丝毫不能放松管理。一般来说，应用系统真正投入应用要经历人员培训、环境建设、数据移植、人机并行和使用维护等 5 个阶段。

(1) 人员培训。它 是计算机应用的首要工作，没有合格的人才，就谈不上计算机应用。因此，在计算机应用系统推广使用之前，首先要搞好人员培训工作。人员培训一般可分 3 个层次：领导层的计算机应用管理培训，软件、硬件技术人员和应用系统管理人员的技术培训，计算机操作员的上岗培训。

人员培训工作可以采用各种不同方式：

· 对领导层的计算机应用管理知识培训，内容应包括：计算机的基本知识，计算机应用的基本情况，计算机应用管理基本办法等，着重点放在作为领导如何面对计算机应用进行科学的管理。

· 对软件、硬件技术人员和应用系统管理人员的培训，要求经过较长时间的专业培训，能熟悉计算机的一般原理，熟练地掌握计算机操作系统，了解应用系统的内部流程并能准确使用，能给操作人员以正确的指导。对计算机应用过程中出现的故障，应能迅速判断原因，并进行力所能及的维护。对于这一层次的人员，可以分批选送到有关院校进行一个月以上的专门培训。

· 对计算机操作员的培训，应在应用系统的现场集中进行培训，培训时间根据应用系统的复杂程度决定，一般要求操作员能熟悉计算机应用系统的整个操作过程，并能独立操作。

(2) 环境建设。应用系统的环境建设，应与应用系统开发同时进行。但当一个应用系统要应用于多个单位或部门时，在进行人员培训的同时，要开始进行环境建设。环境建设主要包括机房建设、主机及附属设施的安装、应用软件的安装等工作。

(3) 数据移植。它是指将手工处理或旧系统中的数据，整理转换成新系统中的数据形式，并输入新系统的过程。为数据移植需要，必须进行充分的事前准备工作，包括组织专门的数据移植班子，有专人负责管理，编制数据移植程序，以及做一些其他必须的辅助工作等。在数据移植过程中，加强管理非常重要，管理水平的高低会影响移植的速度、正确性。因此，数据移植工作应由业务骨干负责，进行全面调度和统筹安排。

(4) 人机并行。它是由手工处理到计算机处理必须经过的一个过渡阶段。对已经成熟的应用系统，人机并行的主要目的是使业务部门人员有一段熟悉、适应的过程。对首次使用的、刚开

发好或修改完成的应用系统进行试点时，人机并行是通过计算机处理和手工处理同步运行的方法，用业务处理的真实数据进一步对应用系统进行测试，以发现应用系统错误的一种有效手段。测试内容主要包括计算机处理方法是否符合业务部门有关规定，移植数据是否正确，处理输出结果是否符合要求等。人机并行阶段还包括对应用系统的可靠性和适应性的评价。

(5) 使用维护。在经过了以上几个步骤，并通过最终审查确认后，计算机应用系统便可正式投入实际应用。必须指出的是，对于任何一个复杂的计算机应用系统，不管经过多么严格的测试，总难免有这样那样的错误存在。因此，在应用过程中，要加强日常的维护、保养，建立健全故障登记和维护制度，确保应用系统正常运行。

第二章　密码学基础

第一节　基本概念

一、基本术语

密码学(cryptology)是研究秘密书写的原理和破译密码的方法的一门科学。它包括密切相关的两方面内容：其一是密码编码学(cryptography)，研究书写出好的密码体制的方法，保护信息不被侦察；其二是密码分析学(cryptanalysis)，研究攻破一个系统的途径，恢复被隐蔽起来的信息的本来面目。

一个密码系统包括明文(cleartext 或 plaintext)字母空间、密文(ciphertext)字母空间、密钥(key)空间和算法(algorithm)，密码系统的两个基本单元是算法和密钥。算法是一些公式、法则或程序，规定明文和密文之间的变换方法。密钥可以看成是算法中的参数。在一个密码系统中，算法是相对稳定的。不能设想在一个系统中经常改变算法，在这种意义下可以把算法视作常量，而密钥则视作变量。可以根据事先约定好的安排，或者每逢一个新信息改变一个密钥，或者每天更换一次密钥。为了密码系统的安全，频繁地更换密钥是必要的。由于种种原因，算法是不能保密的，因此，我们常认定算法是公开的，真正需要保密的是密钥。可见，在分发密钥时要特别小心。

从明文到密文的变换过程称为加密(encryption)，这个变换过程实质上就是一个算法，记为 E；用密文、密钥来恢复明文的过程称为解密(decryption)，也叫脱密，相应的算法叫解密算法，记为 D。从截获的密文推断出原来的明文的过程称为密码分析。这样一个保密通信系统模型可以用图 2.1 表示。

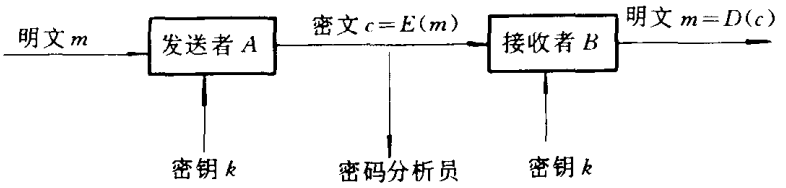

图 2.1　保密通信系统模型

为了便于理解，举一个具体的密码体制作为例子，这是一个已知最古老的密码体制。

polybios 密码体制：明文空间 $M=\{a,b,c,\cdots,x,y,z\}$ 其中字母 j 被略去。密文空间 $C=\{a,b,\cdots,y,z\}$，加密算法(规则)是明文中每个字母都用该字母所在的行和列的字母代替，见表 2.1，如 $D=AD$，$T=DD$，$X=EC$，

表 2.1　Polybios 方案

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

明文 DIGITAL COMMUNICATION 加密为 ADBDBBBDDDAACAACCDCBCBDECC BDACAADD BDCDCC。解密算法(规则)是两个字母一组,按第一个字母所在的行和第二个字母所在的列找到该字母。这里密钥是表 2.1 给出的方表,可以改变成其它的排列方式。

传统密码体制按对明文加密方式不同而分为两大类:将明文消息字符串分为多个字符的组,逐组进行加密者称分组密码(block cipher),其一个重要特征是加密变换 E_k 随密钥 k 的取定而完全确定,即加密变换是非时变的,DES 是这类体制的典型代表;另一类是流密码(stream cipher),也称序列密码,它将明文消息字符串逐位地加密成密文字符,即加密变换是时变的,它既依赖于种子密钥,又依赖于加密器中记忆元件在该时刻的状态。移位寄存器序列是这类体制的典型代表。

很显然,对一个密码系统的基本要求是:

(1) 知道 k 时,E 容易计算;

(2) 知道 k 时,D 容易计算;

(3) 不知道 k 时,由 $c=E(m)$不易推导出 m。

总而言之,一个密码系统对于合法的通信双方来讲,加解密变换容易进行,而对于密码分析员来说,由密文推导出明文是困难的。

二、密码攻击

在保密通信系统中,信道中传输的是加密后的消息,即密文。采用截获密文进行分析的攻击称作被动攻击(passive attack),采用删除、更改、增填、重放、伪造等手段向系统注入假消息并进行分析的攻击,称为主动攻击(active attack)。密码分析员要破译密码首先要搜集密文,通常有以下几种不同的搜集方法:

(1) 搭线窃听。即利用硬线连接,对通信线路中的各种传输进行截收(包括网络非法接收)。

(2) 电磁窃听。即对无线电传输进行截收。例如,对无线电和微波传输,或对从电子设备辐射出的带有信息的电磁能等进行截收。可以在 1 km 以外通过接收显示器辐射出的电磁能完整恢复显示器显示的内容。现在基本上禁止采用微波传送机密信息,而是采用光缆传送。

(3) 声音窃听。即对由人的语言或者由打印机、穿孔和发送设备产生的声波进行截收(这里例举的这种窃听方法仅供参考,几乎在所有情况下,单用物理安全措施而不采用密码技术就可以有效地防止这种窃听)。

衡量一个密码系统的保密性能是很困难的,其中涉及的因素很多。例如密码分析员掌握的关于密码系统的知识越多,则对密码系统的威胁也就越大。一般都假定密码分析者知道明文的统计特性、加密体制、密钥空间及其统计特性,密码的安全性必须完全寓于密钥之中。密码分析员对密码系统的攻击能力大体上可以分为:

(1) 密码分析员只掌握密码系统的加—解密算法。即使密码分析者试用几种密码体制,其过程的复杂度同一种体制的复杂度完全相同,因此,总是假设密码分析者知道所用的密码体制。

(2) "仅知道密文的攻击",分析员能够搜集到密文信息。

(3) "已知明文的攻击",分析员能够搜集到某些明文和与之对应的密文信息。运用明密对有助于分析欲破译的密文。

(4) "选择明文的攻击",密码分析员可以有选择地搜集到某些明文和与之对应的密文信息。

(5) 密码分析员可以象合法用户那样发送加密的信息。

(6) 密码分析员可以改变、截取和重新发送信息。

上述分级是按照密码分析员的能力由低到高排列的，在设计密码系统时，至少应该使它经受(1)、(2)级攻击的考验。

三、序列密码与分组密码

序列密码亦称为流密码，它是由明文序列与密钥序列经模 2 加来得到密文序列的。这种体制的加、解密算法都非常简单(如图 2.2 所示)。

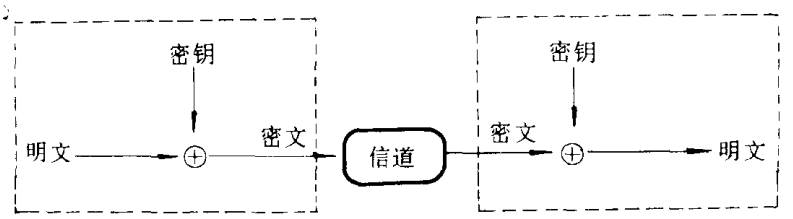

图 2.2　序列密码体制

在已知明文攻击下，要求密码分析者在知道一部分明、密文对之后不能解开其它密文，即在已知部分密钥条件下，不能知道其余的密钥，这就要求密钥序列有一定的随机性。完全随机的序列保密性最好，但是接收者(receiver)必须与发送者(sender)拥有相同的密钥序列才能解密，这又要求密钥序列必须按一定规则产生。我们把这种按某种固定规则产生的具有一定随机性的序列叫做伪随机序列。

怎样衡量一个序列的随机性？若二元序列(a_t)，由一个固定机器按某种规则产生，则从某一位后输出的序列一定是一个周期序列，即存在正整数 p 使得 $a_{k+p}=a_k$。最短的重复序列称为一个圈，圈的长度就是这个序列的周期。相同的一串序列元素称为一个游程，元素全为 0 的游程称为 0-游程，全为 1 的游程称为 1-游程，游程中字符的个数称为游程长度。设序列 $a_1,a_2,\cdots,a_n,\cdots$ 的周期为 p，并习惯地用(a_t)记这个序列。称$(a_{t+\tau})$为(a_t)的平移序列，其中 τ 为某一整数。定义序列(a_t)的自相关函数为：

$$C(\tau)=\frac{1}{p}\sum_{t=1}^{p}(-1)^{a_t+a_{\tau+t}} \tag{3.1}$$

显然，对所有 τ，$C(\tau+p)=C(\tau)$。故只需研究 $0\leqslant\tau<p$ 的那些 τ 就行了。当 $\tau=0$ 时，称同相自相关；当 $\tau\neq0$ 时，称异相自相关。

对于周期为 p 的二元序列，Golomb 提出了以下 3 条随机性公设：

(1) 如果 p 是偶数，则长为 p 的圈中应含相同数目的 0 与 1；如果 p 是奇数，则 0 的数目应当比 1 的数目多一个或少一个。

(2) 在长度为 p 的圈中，游程数目的 1/2 是长度为 1 的游程，1/4 是长度为 2 的游程，1/8 是长度为 3 的游程。一般来说，对于一个以上的游程的每个长度 i 而言，长度为 i 的游程占游程总数的$\frac{1}{2^i}$。此外，对每一种长度，0-游程与 1-游程各占一半。

(3) 异相自相关是一个常数。

上述 3 条公设作为衡量随机性的准则，它们各反映了哪些问题呢？粗略地说，公设 1 反映了字符的均等性这一特征；公设 2 反映了连续字符出现的情况，有点象英语中的双字母组、三字母组等，但不完全一样；公设 3 则说明通过密文与其平移的比较，得不到额外信息。

衡量序列随机性的另一个重要准则是下一位不可预测性：即从已知的 $a_1,a_2,\cdots,a_n$ 来猜测 a_{n+1} 不会比瞎猜更好。