“十三五”国家重点出版物出版规划项目
高等教育规划教材

计算机网络安全教程

第3版

梁亚声　汪永益　刘京菊　汪 生　王永杰 编著

机 械 工 业 出 版 社

本书系统地介绍了计算机网络安全的体系结构、基础理论、技术原理和实现方法。主要内容包括计算机网络的物理安全、信息加密与 PKI 技术、防火墙技术、入侵检测技术、操作系统与数据库安全技术、网络安全检测与评估技术、计算机病毒与恶意代码防范技术、数据备份技术、无线网络安全、云计算安全及网络安全解决方案。本书涵盖了计算机网络安全的技术和管理，在内容安排上将理论知识和工程技术应用有机结合，并介绍了许多计算机网络安全技术的典型应用方案。

本书可作为计算机、网络工程和信息安全等专业本科生的教科书，也可作为网络工程技术人员、网络管理人员和信息安全管理人员的技术参考书。

本书配有授课电子课件，需要的教师可登录 www.cmpedu.com 免费注册，审核通过后下载，或联系编辑索取（QQ：2850823885，电话：010-88379739）。

图书在版编目（CIP）数据

计算机网络安全教程 / 梁亚声等编著. —3 版. —北京：机械工业出版社，2016.4
高等教育规划教材
ISBN 978-7-111-53752-6

Ⅰ. ①计… Ⅱ. ①梁… Ⅲ. ①计算机网络－安全技术－高等学校－教材
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2016）第 103913 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
责任编辑：郝建伟 责任校对：张艳霞
责任印制：
印刷（ 装订）

2016 年 8 月第 3 版 • 第 1 次印刷
184mm×260mm • 22 印张 • 540 千字
0001－3000 册
标准书号：ISBN 978-7-111-53752-6
定价：49.90 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
服务咨询热线：（010）88379833
读者购书热线：（010）88379649

网络服务
机 工 官 网：www.cmpbook.com
机 工 官 博：weibo.com/cmp1952
教育服务网：www.cmpedu.com
金 书 网：www.golden-book.com

出 版 说 明

当前，我国正处在加快转变经济发展方式、推动产业转型升级的关键时期。为经济转型升级提供高层次人才，是高等院校最重要的历史使命和战略任务之一。高等教育要培养基础性、学术型人才，但更重要的是加大力度培养多规格、多样化的应用型、复合型人才。

为顺应高等教育迅猛发展的趋势，配合高等院校的教学改革，满足高质量高校教材的迫切需求，机械工业出版社邀请了全国多所高等院校的专家、一线教师及教务部门，通过充分的调研和讨论，针对相关课程的特点，总结教学中的实践经验，组织出版了这套“高等教育规划教材”。

本套教材具有以下特点：

1）符合高等院校各专业人才的培养目标及课程体系的设置，注重培养学生的应用能力，加大案例篇幅或实训内容，强调知识、能力与素质的综合训练。

2）针对多数学生的学习特点，采用通俗易懂的方法讲解知识，逻辑性强、层次分明、叙述准确而精炼、图文并茂，使学生可以快速掌握，学以致用。

3）凝结一线骨干教师的课程改革和教学研究成果，融合先进的教学理念，在教学内容和方法上做出创新。

4）为了体现建设“立体化”精品教材的宗旨，本套教材为主干课程配备了电子教案、学习与上机指导、习题解答、源代码或源程序、教学大纲、课程设计和毕业设计指导等资源。

5）注重教材的实用性、通用性，适合各类高等院校、高等职业学校及相关院校的教学，也可作为各类培训班的教材和自学用书。

欢迎教育界的专家和老师提出宝贵的意见和建议。衷心感谢广大教育工作者和读者的支持与帮助！

机械工业出版社

前　言

随着计算机网络的广泛应用，人类面临着信息安全的巨大挑战。如何保证个人、企业及国家的机密信息不被黑客和间谍窃取，如何保证计算机网络不间断地工作，是国家和企业信息化建设必须考虑的重要问题。然而，计算机网络安全问题错综复杂，涉及面非常广，有技术因素，也有管理因素；有自然因素，也有人为因素；有外部的安全威胁，还有内部的安全隐患。

本书紧密结合计算机网络安全技术的最新发展，不断更新内容，在操作系统、无线网络和云计算等方面，对《计算机网络安全教程》（第 2 版）进行了调整、补充和完善。

本书共 12 章，第 1 章主要介绍计算机网络的相关概念和计算机网络的安全体系结构。第 2 章主要介绍计算机网络的物理安全，从计算机机房、通信线路、设备和电源等方面介绍计算机网络物理层的安全技术。第 3 章主要介绍信息加密与 PKI 技术，包括密码学基础、加密体制、古典密码/单钥加密/双钥加密/同态加密等加密算法、信息加密技术应用、数字签名技术和身份认证技术，以及公开密钥基础设施（PKI）。第 4 章主要介绍防火墙技术，包括防火墙体系结构、包过滤、应用代理、状态检测、NAT 等防火墙技术，以及防火墙的应用和个人防火墙。第 5 章主要介绍入侵检测技术，包括入侵检测的基本原理、系统结构、系统分类、技术实现、分布式入侵检测、入侵检测系统的标准、入侵防护系统和入侵检测系统的应用。第 6 章主要介绍操作系统和数据库安全技术，包括访问控制技术、操作系统的安全技术、UNIX/Linux/Windows 7 系统安全技术、数据库安全机制及安全技术。第 7 章主要介绍网络安全检测与评估技术，包括网络安全漏洞的分类和检测技术、网络安全评估标准和方法，以及网络安全评估系统。第 8 章主要介绍计算机病毒与恶意代码防范技术，包括计算机病毒的工作原理和分类、计算机病毒的检测和防范技术，以及恶意代码的防范技术。第 9 章主要介绍数据备份技术，包括磁盘备份、双机备份、网络备份技术、数据备份方案、数据备份与恢复策略，以及备份软件。第 10 章主要介绍无线网络的安全技术，包括 Wi-Fi 和无线局域网安全、移动终端安全、无线安全技术及应用。第 11 章主要介绍云计算安全，包括云安全威胁和安全需求、云计算安全架构和云计算安全技术。第 12 章主要介绍网络安全解决方案，包括网络安全体系结构，以及企业和单机用户网络安全解决方案。

本书具有以下主要特点。

1）在内容安排上具有全面性和系统性，本书从计算机网络安全的体系结构、软硬件安全、安全设计和管理等方面，系统地介绍了计算机网络完全的基础理论、技术原理和实现方法，使读者对计算机网络安全有一个系统、全面的了解。

2）在介绍技术时注重理论性和实用性，对于每种网络安全技术，首先介绍技术的理论基础和原理，再通过具体的实例介绍安全技术的应用和操作方法。

3）在章节编排上具有独立性和完整性，虽然本书涉及的内容十分广泛，但通过合理安排章节，使各章节内容相对独立，在实施教学时可结合教学对象和实际情况，进行适当的选取和编排。

本书由梁亚声编写第 1 章并统稿，汪永益编写第 4、8、9 章，刘京菊编写第 2、7、12 章，汪生编写第 3、5、6 章，王永杰编写第 10、11 章。

由于作者水平有限，书中难免存在不妥之处，敬请广大读者批评指正。

编　者

目　录

第1章 绪 论

在信息化时代，互联网在全球范围掀起一场影响人类所有层面的深刻变革，实现了基于企业内部网（Intranet）、企业外部网（Extranet）、全球互联网（Internet）的世界范围内的信息共享和业务处理。随着政府上网、企业上网、教育上网、家庭上网等的普及，计算机网络在经济、军事和文教等诸多领域得到广泛应用。

计算机网络在为人们提供便利、带来效益的同时，也使人类面临着信息安全的巨大挑战。计算机网络存储、传输和处理着政府宏观调控决策、商业经济、银行资金转账、股票证券、能源资源、国防和科研等大量关系国计民生的重要信息，许多重要信息直接关系到国家的安全。如何保护个人、企业和国家的机密信息不受黑客和间谍的入侵，如何保证网络系统安全地、不间断地工作，是国家和单位信息化建设必须考虑的重要问题。

有关计算机安全技术的研究始于 20 世纪 60 年代。当时，计算机系统的脆弱性已日益为美国政府和一些私营机构所认识。但是，由于当时计算机的速度和性能还比较落后，使用的范围也不广，再加上美国政府把它当作敏感问题而施加控制。因此，有关计算机安全的研究一直局限在比较小的范围内。

进入 20 世纪 80 年代后，计算机的性能得到了成百上千倍的提高，应用的范围也在不断扩大，计算机几乎遍及世界各个角落。并且，人们利用通信网络把孤立的单机系统连接起来相互通信和共享资源，随之而来的计算机网络的安全问题就日益严峻，成为信息技术中最重要的问题之一。

1.1 计算机网络面临的主要威胁

计算机网络是颇具诱惑力的攻击目标，无论是个人、企业，还是政府机构，只要使用计算机网络，都会感受到网络安全问题带来的威胁。无论是局域网还是广域网，都存在着自然和人为等诸多脆弱性和潜在威胁。

1.1.1 计算机网络实体面临的威胁

实体是指计算机网络中的关键设备，包括各类计算机（服务器、工作站等）、网络和通信设备（路由器、交换机、集线器、调制解调器和加密机等）、存放数据的媒体（磁带、磁盘和光盘等）、传输线路、供配电系统，以及防雷系统和抗电磁干扰系统等。这些设备不管哪一个环节出现问题，都会影响网络的正常运行，甚至给整个网络带来灾难性的后果。

1.1.2 计算机网络系统面临的威胁

1986～1989 年，原西德黑客团伙“汉诺威集团”试图进入美国军事计算机网络刺探机密，这一事件于 1989 年 3 月 2 日在德国电视上曝光。1990 年 1 月 15 日又发生了 AT＆T“一·一五”大瘫痪事件。从而使美国意识到黑客对计算机网络系统的严重威胁，1990 年在

美国全国范围内掀起了一场“扫黑大行动”。2014 年 4 月爆出了 Heartbleed（心脏出血）漏洞，涉及各大网银、门户网站等，该漏洞可被用于窃取服务器敏感信息，实时抓取用户的账号密码。在漏洞被公开后到系统被修复前这段时间内，该漏洞已经被利用，有些网站用户信息或许已经被黑客非法获取。2014 年 12 月，索尼影业公司被黑客攻击，摄制计划、明星隐私及未发表的剧本等敏感数据都被黑客窃取，并逐步公布在网络上，预计索尼影业损失高达 1 亿美元。

计算机网络系统的安全威胁主要表现在主机可能会受到非法入侵者的攻击，网络中的敏感数据有可能泄露或被修改，从内部网向公共网传送的信息可能被他人窃听或篡改等。表 1-1 所示为典型的网络安全威胁。

表 1-1　典型的网络安全威胁

威　胁	描　述
窃听	网络中传输的敏感信息被窃听
重传	攻击者事先获得部分或全部信息，以后将此信息发送给接收者
伪造	攻击者将伪造的信息发送给接收者
篡改	攻击者对合法用户之间的通信信息进行修改、删除或插入后，再发送给接收者
非授权访问	通过假冒、身份攻击或系统漏洞等手段，获取系统访问权，从而使非法用户进入网络系统读取、删除、修改或插入信息等
拒绝服务攻击	攻击者通过某种方法使系统响应减慢甚至瘫痪，阻止合法用户获得服务
行为否认	通信实体否认已经发生的行为
旁路控制	攻击者发掘系统的缺陷或安全脆弱性
电磁/射频截获	攻击者从电子或机电设备所发出的无线射频或其他电磁辐射中提取信息
APT（Advanced Persistent Threat，高级持续性威胁）攻击	利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。 APT 在发动攻击之前对攻击对象的业务流程和目标系统进行精确的收集，挖掘被攻击对象受信系统和应用程序的漏洞，利用 0day 漏洞进行攻击
人员疏忽	授权的人为了利益或由于粗心将信息泄漏给未授权人

1.1.3　恶意程序的威胁

以计算机病毒、网络蠕虫、间谍软件和木马程序等为代表的恶意程序时刻都威胁着计算机网络的安全。

1988 年 11 月发生了互联网络蠕虫（worm）事件，也称莫里斯蠕虫案。22 岁的罗伯特·泰潘·莫里斯是美国康奈尔大学计算机系研究生，其父鲍勃·莫里斯是美国安全局的首席安全专家。罗伯特从小喜爱计算机，非常熟悉 UNIX 系统。在恶作剧心态的操纵下，罗伯特利用 UNIX 系统中 Sendmail、Finger 和 FTP 的安全漏洞，编写了一个蠕虫病毒程序。11 月 2 日晚，罗伯特将病毒程序安放在与 ARPANET（国际互联网 Internet 的前身）联网的麻省理工学院的网络上。由于病毒程序中一个参数设置错误，该病毒迅速在与 ARPANET 联网的几乎所有计算机中扩散，并被疯狂复制，大量侵蚀计算机资源，使得美国成千上万台计算机一夜之间陷入瘫痪。

1999 年 4 月 26 日，CIH 病毒爆发，俄罗斯 10 多万台计算机瘫痪，韩国 24 万多台计算机受影响，马来西亚 12 个股票交易所受到侵害。

计算机病毒可以严重破坏程序和数据，使网络的效率和作用大大降低，使许多功能无法正常使用，导致计算机系统的瘫痪。据统计，计算机病毒所造成的损失占网络经济损失的76%，仅“爱虫”发作在全球所造成的损失就高达 96 亿美元。虽然至今尚未出现灾难性的后果，但各种各样的计算机病毒层出不穷，并活跃在各个角落。

1.1.4 计算机网络威胁的潜在对手和动机

对网络进行攻击的潜在对手有怀有恶意的，也有非恶意的。网络威胁的潜在对手举例如表 1-2 所示。

表 1-2 潜在的对手举例

对手		描述
恶意攻击	国家	国家经营，组织精良，并得到很好的财政资助，收集别国的机密或关键信息
	黑客	寻找网络系统的脆弱性及其缺陷，进而攻击网络
	恐怖分子/计算机恐怖分子	各种恐怖分子或极端势力的个人或团体，以强迫、恐吓政府或社会以满足其需要为目的
	有组织的计算机犯罪	有组织和财政资助的协同犯罪
	其他犯罪成员	犯罪群体的其他部分，通常由少量成员构成，或是单独行动的个人
	国际新闻社	收集和发布消息（有时是非法的），并将其服务出售给出版社和娱乐媒体的组织。其行为包括在任何指定时间收集关于任何人和事的情报
	工业竞争	在竞争市场中营运的国内或外国公司，它们经常以商业间谍的形式，从竞争对手或外国政府那里非法收集情报
	不满的雇员	具有访问系统的条件，能够对系统实施内部威胁
非恶意	粗心或未受良好训练的工作人员	缺乏训练，或者粗心大意导致信息系统损坏

对计算机网络进行恶意破坏的目的多种多样，主要是为了获取商业、军事或个人情报，影响计算机系统正常运行。

通常，从事这些行为的人被称为黑客。黑客的范围很广，从没有经验的职员、大学生或新手到具有高技术能力的人员。大多数黑客以他们的技术为荣，寻求简单方法获得对系统的访问权（而非破坏）。

黑客刺探特定目标的通常动机如下。

- 获取机密或敏感数据的访问权。
- 跟踪或监视目标系统的运行（跟踪分析）。
- 扰乱目标系统的正常运行。
- 窃取钱物或服务。
- 免费使用资源（如计算机资源或用网络）。
- 向安全机制进行技术挑战。

从信息系统方面看，这些动机具有以下 3 个基本目标。

- 访问信息。
- 修改或破坏信息或系统。
- 使系统拒绝服务。

在攻击信息处理系统时，面临着一定风险，这些风险包括以下几个。

- 暴露其攻击能力。
- 打草惊蛇，使对手有所防范，从而增加未来进一步成功攻击的难度。
- 遭受惩罚（如罚款或入狱等）。
- 危及生命安全。

1.2 计算机网络的不安全因素

一般来说，计算机网络本身的脆弱性和通信设施脆弱性共同构成了计算机网络的潜在威胁。一方面，计算机网络的硬件和通信设施极易受到自然环境的影响（如温度、湿度、灰尘度和电磁场等），以及自然灾害（如洪水，地震等）和人为（故意破坏和非故意破坏）的物理破坏；另一方面，计算机网络的软件资源和数据信息易受到非法的窃取、复制、篡改和毁坏；再有，计算机网络硬件的自然损耗和自然失效，以及软件的逻辑错误，同样会影响系统的正常工作，造成计算机网络系统内信息的损坏、丢失和安全事故。

1.2.1 不安全的主要因素

对计算机网络安全构成威胁的因素很多，综合起来包括以下三个方面。

- **偶发因素**：如电源故障、设备的机能失常、软件开发过程中留下的漏洞或逻辑错误等。
- **自然灾害**：各种自然灾害（如地震、风暴、泥石流和建筑物破坏等）对计算机系统构成严重的威胁。此外，火灾、水灾和空气污染也对计算机网络构成严重威胁。
- **人为因素**：不法之徒利用计算机网络或潜入计算机房，篡改系统数据、窃用系统资源、非法获取机密数据和信息、破坏硬件设备或编制计算机病毒等。此外，管理不好、规章制度不健全、有章不循、安全管理水平低、人员素质差、操作失误，以及渎职行为等都会对计算机网络造成威胁。

人为因素对计算机网络的破坏也称为人对计算机网络的攻击，可分为下列几个方面。

1．被动攻击

这类攻击主要是监视公共媒体（如无线电、卫星、微波和公共交换网）上传送的信息，典型的被动攻击如表 1-3 所示。抵抗这类攻击的对策主要包括：使用虚拟专用网 VPN、加密被保护网络，以及使用加保护的分布式网络。

表 1-3 典型被动攻击举例

攻　击	描　述
监视明文	监视网络，获取未加密的信息
解密通信数据	通过密码分析，破解网络中传输的加密数据
口令嗅探	使用协议分析工具，捕获用于各类系统访问的口令
通信量分析	不对加密数据进行解密，而是通过对外部通信模式的观察获取关键信息。例如，通信模式的改变可以暗示紧急行动

2．主动攻击

主动攻击主要是避开或突破安全防护、引入恶意代码（如计算机病毒），以及破坏数据和

系统的完整性，典型的主动攻击如表 1-4 所示。抵抗这类攻击的对策主要包括：增强内部网络的保护（如防火墙和边界护卫）、采用基于身份认证的访问控制、远程访问保护、质量安全管理、自动病毒检测、审计和入侵检测等技术。

表 1-4　典型主动攻击举例

攻　击	描　述
修改传输中的数据	截获并修改网络中传输的数据，例如修改电子交易数据，从而改变交易的数量或者将交易转移到别的账户
重放	将旧的消息重新反复发送，造成网络效率降低
会话拦截	未授权使用一个已经建立的会话
伪装成授权的用户或服务器	这类攻击者将自己伪装成他人，从而未授权访问资源和信息。一般过程是，先利用嗅探或其他手段获得用户/管理员信息，然后作为一个授权用户登录。这类攻击也包括用于获取敏感数据的欺骗服务器，通过与未产生怀疑的用户建立信任服务关系来实施攻击
利用系统软件的漏洞	攻击者探求以系统权限运行的软件中存在的脆弱性。几乎每天都能发现软件和硬件平台中新的脆弱性
利用主机或网络信任	攻击者通过操纵文件，使虚拟/远方主机提供服务，从而获得信任。典型的攻击有 rhost 和 rlogin
利用恶意代码	攻击者通过系统的脆弱性进入用户系统，并向系统内植入恶意代码；或者是，将恶意代码植入看起来无害的供下载的软件或电子邮件中，从而使用户去执行恶意代码
利用协议或基础设施的系统缺陷	攻击者利用协议中的缺陷来欺骗用户或重定向通信量。这类攻击包括：哄骗域名服务器以进行未授权远程登录，使用 ICMP 炸弹使某个机器离线，源路由伪装成信任主机源，TCP 序列号猜测获得访问权，为截获合法连接而进行 TCP 组合等
拒绝服务	攻击者有很多实施拒绝服务的攻击方法，包括：有效地将一个路由器从网络中脱离的 ICMP 炸弹，在网络中扩散垃圾包，以及向邮件中心发送垃圾邮件等

3．邻近攻击

邻近攻击是指未授权者可物理上接近网络、系统或设备，从而可以修改、收集信息，或使系统拒绝访问，典型的临近攻击如表 1-5 所示。接近网络可以是秘密进入或公开，也可以是两者都有。

表 1-5　邻近攻击举例

攻　击	描　述
修改数据或收集信息	攻击者获取系统管理权，从而修改或窃取信息，如 IP 地址、登录的用户名和口令等
系统干涉	攻击者获取系统访问权，从而干涉系统的正常运行
物理破坏	该攻击获取系统物理设备访问权，从而对设备进行物理破坏

4．内部人员攻击

内部工作人员具有对系统的直接访问权，可轻易地对系统实施攻击。内部人员攻击分为恶意和非恶意（不小心或无知行为）两种。非恶意行为也会导致安全事件，因此，非恶意破坏也被认为是一种攻击，典型的内部人员攻击如表 1-6 所示。

1）内部人员的恶意攻击：根据美国联邦调查局的评估，80%的攻击和入侵来自内部。内部人员知道系统的布局、有价值的数据在何处，以及系统所采用的安全防范措施。而且，内部人员的攻击通常是最难以检测和防范的。

2）内部人员的非恶意攻击：这类攻击并非故意破坏信息或信息处理系统，而是由于无意的行为对系统产生了破坏，这些破坏一般是由于缺乏知识或不小心所致。

典型对策包括：加强安全意识和技术培训，对系统的关键数据和服务采取特殊的访问控

制机制，采用审计、入侵检测等技术。

表 1-6　内部人员攻击举例

攻　击		描　述
恶意	修改数据或安全机制	内部人员直接使用网络，具有系统的访问权。因此，内部人员攻击者比较容易实施未授权操作或破坏数据
	擅自连接网络	对涉密网络具有物理访问能力的人员，擅自将机密网络与密级较低的网络或公共网络连接，违背涉密网络的安全策略和保密规定
	隐通道	隐通道是未授权的通信路径，用于从本地网向远程站点传输盗取的信息
	物理损坏或破坏	对系统具有物理访问权限的工作人员对系统故意破坏或损坏
非恶意	修改数据	由于缺乏知识或粗心大意，修改或破坏数据或系统信息
	物理损坏或破坏	由于渎职或违反操作规程，对系统的物理设备造成意外损坏或破坏

5．分发攻击

分发攻击是指在软件和硬件开发出来后和安装之前，当它从一个地方送到另一个地方时，攻击者恶意地修改软件或硬件，典型的分发攻击如表 1-7 所示。可以通过受控分发，以及由最终用户检验软件签名和访问控制来消除分发攻击威胁。

表 1-7　分发攻击举例

攻　击	描　述
在设备生产时修改软、硬件	当软件和硬件在生产线上时，通过修改软、硬件配置来实施这类攻击
在产品分发时修改软、硬件	在产品分发期内修改软、硬件配置（如安装窃听设备）

1.2.2　不安全的主要原因

计算机网络系统安全的脆弱性是伴随计算机网络一同产生的，换句话说，安全脆弱是计算机网络与生俱来的致命弱点。在网络建设中，网络特性决定了不可能无条件、无限制地提高其安全性能。既要使网络方便快捷，又要保证网络安全，这是一个非常棘手的“两难选择”，而网络安全只能在“两难选择”所允许的范围内寻找平衡点。因此，可以说任何一个计算机网络都不是绝对安全的。

1．互联网具有不安全性

最初，互联网用于科研和学术目的，它的技术基础存在不安全性。互联网是对全世界所有国家开放的网络，任何团体或个人都可以在网上方便地传送和获取各种各样的信息，具有开放性、国际性和自由性，这就对安全提出了更高的要求，主要表现在以下三个方面。

- **开放性的网络**：导致网络的技术全开放，使得网络所面临的破坏和攻击来自多方面。可能来自物理传输线路的攻击，也可能来自对网络通信协议的攻击，以及对软件和硬件实施的攻击。
- **国际性的网络**：意味着网络的攻击不仅来自本地网络的用户，而且可以来自互联网上的任何一台计算机，也就是说，网络安全面临的是国际化的挑战。
- **自由性的网络**：意味着网络最初对用户的使用并没有提供任何技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。

另外，互联网使用的 TCP/IP（传输控制协议/网际协议），以及 FTP（文件传输协议）、

E-mail（电子邮件）、RPC（远程程序通信规则）和 NFS（网络文件系统）等都包含许多不安全的因素，存在许多安全漏洞。

2．操作系统存在的安全问题

操作系统软件自身的不安全性，以及系统设计时的疏忽或考虑不周而留下的“破绽”，都给危害网络安全的人留下了许多“后门”。

操作系统体系结构造成的不安全隐患是计算机系统不安全的根本原因之一。操作系统的程序是可以动态连接的，如 I/O 的驱动程序和系统服务，这些程序和服务可以通过打“补丁”的方式进行动态连接。许多 UNIX 操作系统的版本升级和开发都是采用打补丁的方式进行的。这种动态连接的方法容易被黑客利用，而且还是计算机病毒产生的好环境。另外，操作系统的一些功能也带来不安全因素，例如，支持在网络上传输可以执行的文件映像，以及网络加载程序的功能等。

操作系统不安全的另一原因在于它可以创建进程，支持进程的远程创建与激活，支持被创建的进程继承创建进程的权利，这些机制提供了在远端服务器上安装间谍软件的条件。若将间谍软件以打补丁的方式“打”在一个合法的用户上，尤其“打”在一个特权用户上，黑客或间谍软件就可以使系统进程与作业的监视程序都监测不到它的存在。

操作系统的无口令入口及隐蔽通道（原是为系统开发人员提供的便捷入口），也都成为黑客入侵的通道。

3．数据的安全问题

在网络中，数据存放在数据库中，供不同的用户共享。然而，数据库存在着许多不安全性，例如，授权用户超出了访问权限进行数据的更改活动；非法用户绕过安全内核，窃取信息资源等。对于数据库的安全而言，要保证数据的安全可靠和正确有效，即确保数据的安全性、完整性和并发控制。数据的安全性就是防止数据库被故意破坏和非法存取；数据的完整性是防止数据库中存在不符合语义的数据，以及防止由于错误信息的输入、输出而造成无效操作和错误结果；并发控制就是在多个用户程序并行地存取数据库时，保证数据库的一致性。

4．传输线路安全问题

尽管在光缆、同轴电缆、微波和卫星通信中窃听其中指定一路的信息是很困难的，但是从安全的角度来说，没有绝对安全的通信线路。

5．网络应用存在的安全问题

伴随着互联网更加开放，用户开展的业务也更加丰富多彩，终端智能普遍使用，数据中心和各种云的建设应用，网络的安全问题也出现了新的形式及特点，应用安全问题已经成为移动互联网网络推广的主要问题。

6．网络安全管理问题

网络系统缺少安全管理人员，缺少安全管理的技术规范，缺少定期的安全测试与检查，缺少安全监控，是网络最大的安全问题之一。

1.3 计算机网络安全的概念

计算机网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论和信息论等多种学科的综合性学科。

1.3.1 计算机网络安全的定义

计算机网络安全是指利用管理控制和技术措施，保证在一个网络环境里，信息数据的机密性、完整性及可使用性受到保护。要做到这一点，必须保证网络的系统软件、应用软件和数据库系统具有一定的安全保护功能，并保证网络部件（如终端、调制解调器和数据链路等）的功能只能被授权的人们访问。网络的安全问题实际上包括两方面的内容，一是网络的系统安全，二是网络的信息安全，而保护网络的信息安全是最终目的。

从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、不可否认性和可控性的相关技术和理论都是网络安全的研究领域。

网络安全的具体含义会随着“角度”的变化而变化。从用户（个人、企业等）的角度来说，希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和不可否认性的保护，避免其他人或对手利用窃听、冒充、篡改和抵赖等手段侵犯，即用户的利益和隐私不被非法窃取和破坏。从网络运行和管理者角度来说，希望其网络的访问、读写等操作受到保护和控制，避免出现“后门”、病毒、非法存取、拒绝服务，以及网络资源被非法占用和非法控制等威胁，制止和防御黑客的攻击。对安全保密部门来说，希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会造成危害，避免给国家造成巨大损失。从社会教育和意识形态角度来讲，网络上不健康的内容会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

1.3.2 计算机网络安全的目标

从计算机网络安全定义中可以看出，计算机网络安全应达到以下几个目标。

1．保密性

保密性是指网络中的保密信息只能供经过允许的人员，以经过允许的方式使用，信息不泄露给非授权用户、实体或过程，或供其利用。从技术上说，任何传输线路，包括电缆（双绞或同轴）、光缆、微波和卫星，都是可能被窃听的。提供保密性安全服务取决以下若干因素。

- **需保护数据的位置**：数据可能存放在 PC 或服务器、局域网的线路上，或其他流通机制（如磁带、U 盘和光盘等）上，也可能流经一个完全公开的媒体（如经过互联网或通信卫星）。
- **需保护数据的类型**：数据元素可以是本地文件（如口令或密钥）、网络协议所携带的数据和网络协议的信息交换（如一个协议数据单元）。
- **需保护数据的数量或部分**：保护整个数据元素、部分数据单元或协议数据单元。
- **需保护数据的价值**：被保护数据的敏感性，以及数据对用户的价值。

保密性的要素如下。

- **数据保护**：防止信息内容的泄露。
- **数据隔离**：提供隔离路径或采用过程隔离。
- **通信流保护**：数据的特征，包括：频率、数量和通信流的目的地等，通信流保护是指对通信的特征信息及推断信息（如命令结构等）进行保护。

2．完整性

完整性是指网络中的信息安全、精确与有效，不因种种不安全因素而改变信息原有的内容、形式与流向，确保信息在存储或传输过程中不被修改、不被破坏和不丢失。

破坏信息的完整性既有人为因素，也有非人为因素。非人为因素是指通信传输中的干扰噪声、系统硬件或软件的差错等。人为因素包括有意和无意两种，有意危害是指非法分子对计算机的侵入、合法用户越权对数据进行处理，以及隐藏破坏性程序（如计算机病毒、时间炸弹和逻辑陷阱等）等；无意危害是指操作失误或使用不当。完整性被破坏是计算机网络安全的主要威胁。另外，信息完整性是一个很广泛的问题。例如，分布式数据库中并发性操作或者对多个数据副本的更新所引起的数据一致性问题；又如，由于系统的设计不完善造成使用不当或操作失误所引起的数据完整性问题等。

提供完整性服务的要求与保密性服务的要求相似，包括需要保护数据的位置、类型、数量及内容。

3．可用性

可用性是指网络资源在需要时即可使用，不因系统故障或误操作等使资源丢失或妨碍对资源的使用，是被授权实体按需求访问的特性。在网络环境下，拒绝服务、破坏网络和系统的正常运行等都属于对可用性的攻击。

网络可用性还包括在某些不正常条件下继续运行的能力。对网络可用性的破坏，包括合法用户不能正常访问网络资源和有严格时间要求的服务不能得到及时响应。影响网络可用性的因素包括人为与非人为两种。前者是指非法占用网络资源、切断或阻塞网络通信、降低网络性能、甚至使网络瘫痪等；后者是指灾害事故（如火、水和雷击等）、系统死锁和系统故障等。

保证可用性的最有效的方法是提供一个具有普遍安全服务的安全网络环境。通过使用访问控制阻止未授权资源访问，利用完整性和保密性服务来防止可用性攻击。访问控制、完整性和保密性成为协助支持可用性安全服务的机制。

- **避免受到攻击**：一些基于网络的攻击旨在破坏、降级或摧毁网络资源。解决办法是加强这些资源的安全防护，使其不受攻击。免受攻击的方法包括：关闭操作系统和网络配置中的安全漏洞，控制授权实体对资源的访问，以及防止路由表等敏感网络数据的泄露。
- **避免未授权使用**：当资源被使用、占用和过载时，其可用性就会受到限制。如果未授权用户占用了有限的资源（如处理能力、网络带宽和调制解调器连接等），则这些资源对授权用户就是不可用的，通过访问控制可以限制未授权使用。
- **防止进程失败**：操作失误和设备故障也会导致系统可用性降低。解决方法是使用高可靠性设备、提供设备冗余和提供多路径的网络连接等。

4．不可否认性

“否认”是指参与通信的实体拒绝承认它参加了通信，不可否认是保证信息行为人不能否认其信息行为。不可否认性安全服务提供了向第三方证明该实体确实参与了通信的能力。

- 数据的接收者提供数据发送者身份及原始发送时间的证据。
- 数据的发送者提供数据已交付接收者（某些情况下还包括接收时间）的证据。
- 审计服务提供信息交换中各涉及方的可审计性，这种可审计性记录了可用来跟踪某些人的相关事件，这些人应对其行为负责。

不可否认性服务主要由应用层提供。通常用户最关心的是应用程序数据（如电子邮件和文件）的不可否认性。在低层提供不可否认性功能，仅能证明产生过的连接，而无法将流经该连接的数据同特定的实体相绑定。

5．可控性

可控性是指对信息的传播及内容具有控制能力，保证信息和信息系统的授权认证和监控

管理，确保某个实体（人或系统）身份的真实性，也可以确保执法者对社会的执法管理行为。

1.3.3 计算机网络安全的层次

根据网络安全措施作用位置的不同，可以将网络安全划分为 4 个层次，分别为物理安全、逻辑安全、操作系统安全和联网安全。

1．物理安全

物理安全主要包括防盗、防火、防静电、防雷击、防电磁泄漏和物理隔离等方面。关于物理安全的具体内容将在第 2 章中详细介绍。

2．逻辑安全

计算机系统的逻辑安全主要通过口令密码、权限控制等方法来实现。例如，可以限制连续登录的次数或限制连续登录的时间间隔；可以用加密软件保护存储在计算机系统中的信息；通过身份验证技术限制对存储于计算机系统中文件的访问。此外，可以通过一些安全软件跟踪可疑、未授权的访问企图。

3．操作系统安全

操作系统是计算机中最基本、最重要的软件，是计算机系统安全的基础。操作系统安全主要包括用户权限控制、安全漏洞修复等内容。

4．联网安全

联网安全主要通过以下安全措施来实现。

- 访问控制：用来保护计算机和网络资源不被非授权使用。
- 通信安全：用来保证数据的保密性和完整性，以及各通信方的可信赖性。

1.3.4 计算机网络安全所涉及的内容

网络安全研究的主要内容包括以下几个方面。

- 网络安全体系结构。
- 网络攻击手段与防范措施。
- 网络安全设计。
- 网络安全标准、安全评测及认证。
- 网络安全检测技术。
- 网络安全设备。
- 网络安全管理和安全审计。
- 网络犯罪侦查。
- 网络安全理论与政策。
- 网络安全教育。
- 网络安全法律。

概括起来，网络安全包括下列 3 个重要部分。

- **先进的技术**：先进的安全技术是网络安全的根本保障，用户通过风险评估来决定所需的安全服务种类，选择相应的安全机制，集成先进的安全技术。
- **严格的管理**：使用网络的机构、企业和单位建立相宜的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。
- **威严的法律**：安全的基石是社会法律、法规与手段，通过建立与信息安全相关的法

律、法规，使非法分子慑于法律，不敢轻举妄动。

1.4 计算机网络安全体系结构

研究计算机网络安全的体系结构，就是研究如何从管理和技术上保证网络的安全得以完整、准确的实现，网络安全需求得以全面准确的满足。

1.4.1 网络安全模型

网络安全的基本模型如图 1-1 所示。通信双方在网络上传输信息时，首先需要在收、发方之间建立一条逻辑通道。为此，就要先确定从发送方到接收方的路由，并选择该路由上使用的通信协议，如 TCP/IP 等。

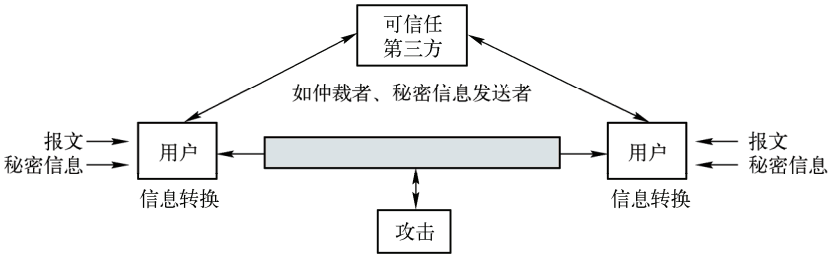


图 1-1　网络安全模型

为了在开放式的网络环境中安全地传输信息，需要为信息提供安全机制和安全服务。信息的安全传输包含两个方面的内容：一是对发送的信息进行安全转换，如进行加密，以实现信息的保密性，或附加一些特征码，以实现对发送方身份的验证等；二是收、发方共享的某些秘密信息，如加密密钥等，除了对可信任的第三方外，对其他用户都是保密的。

为了使信息安全地进行传输，通常需要一个可信任的第三方，其作用是负责向通信双方分发秘密信息，以及在双方发生争执时进行仲裁。

一个安全的网络通信方案必须考虑以下内容。

- 实现与安全相关的信息转换的规则或算法。
- 用于信息转换的秘密信息（如密钥）。
- 秘密信息的分发和共享。
- 利用信息转换算法和秘密信息获取安全服务所需的协议。

1.4.2 OSI 安全体系结构

OSI 安全体系结构的研究始于 1982 年，当时 OSI 基本参考模型刚刚确立。这项工作由 ISO/IEC JTCl/SC21 完成，于 1988 年结束，其成果标志是 ISO 发布了 ISO 7498—2 标准，作为 OSI 基本参考模型的新补充。1990 年，ITU 决定采用 ISO7498—2 作为它的 X.800 推荐标准，我国的国标 GB/T 9387.2—1995《信息处理系统 开放系统互连 基本参考模型　第 2 部分：安全体系结构》等同于 ISO/IEC 7498—2。

OSI 安全体系结构不是能实现的标准，而是如何设计标准的标准。因此，具体产品不应声称自己遵从这一标准。OSI 安全体系结构定义了许多术语和概念，还建立了一些重要

的结构性准则。它们中有一部分已经过时，仍然有用的部分主要是术语、安全服务和安全机制的定义。

1．术语

OSI 安全体系结构给出了标准族中的部分术语的正式定义，其所定义的术语只限于 OSI 体系结构，在其他标准中对某些术语采用了更广的定义。

2．安全服务

OSI 安全体系结构中定义了五大类安全服务，也称为安全防护措施。

- **鉴别服务**：提供对通信中对等实体和数据来源的鉴别。对等实体鉴别提供对实体本身的身份进行鉴别；数据源鉴别提供对数据项是否来自某个特定实体进行鉴别。
- **访问控制服务**：对资源提供保护，以对抗非授权使用和操纵。
- **数据机密性服务**：保护信息不被泄漏或暴露给未授权的实体。机密性服务又分为数据机密性服务和业务流机密性服务。数据机密性服务包括：连接机密性服务，对某个连接上传输的所有数据进行加密；无连接机密性服务，对构成一个无连接数据单元的所有数据进行加密；选择字段机密性服务，仅对某个数据单元中所指定的字段进行加密。业务流机密性服务使攻击者很难通过网络的业务流来获得敏感信息。
- **数据完整性服务**：对数据提供保护，以对抗未授权的改变、删除或替代。完整性服务有 3 种类型：连接完整性服务，对连接上传输的所有数据进行完整性保护，确保收到的数据没有被插入、篡改、重排序或延迟；无连接完整性服务，对无连接数据单元的数据进行完整性保护；选择字段完整性服务，对数据单元中所指定的字段进行完整性保护。

  完整性服务还分为具有恢复功能和不具有恢复功能两种类型。仅能检测和报告信息的完整性是否被破坏，而不采取进一步措施的服务为不具有恢复功能的完整性服务；能检测到信息的完整性是否被破坏，并能将信息正确恢复的服务为具有恢复功能的完整性服务。
- **抗抵赖性服务**：防止参与通信的任何一方事后否认本次通信或通信内容。抗抵赖服务可分为两种形式：数据原发证明的抗抵赖，使发送者不承认曾经发送过这些数据或否认其内容的企图不能得逞；交付证明的抗抵赖，使接收者不承认曾收到这些数据或否认其内容的企图不能得逞。

表 1-8 给出了对付典型网络威胁的安全服务，表 1-9 给出了网络各层提供的安全服务。

表 1-8　对付典型网络威胁的安全服务

安全威胁	安全服务
假冒攻击	鉴别服务
非授权侵犯	访问控制服务
窃听攻击	数据机密性服务
完整性破坏	数据完整性服务
服务否认	抗抵赖服务
拒绝服务	鉴别服务、访问控制服务和数据完整性服务等

表 1-9　网络各层提供的安全服务

安全服务 \ 网络层次		物理层	数据链路层	网络层	传输层	会话层	表示层	应用层
鉴别	对等实体鉴别			√	√			√
	数据原发鉴别			√	√			√
访问控制				√	√			√
数据机密性	连接机密性	√	√	√	√		√	√
	无连接机密性		√	√	√		√	√
	选择字段机密性						√	√
	业务机密性	√		√				√
数据完整性	可恢复的连接完整性				√			√
	不可恢复的连接完整性			√	√			√
	选择字段的连接完整性							√
	无连接完整性			√	√			√
	选择字段的无连接完整性							√
抗抵赖性	数据原发证明的抗抵赖							√
	交付证明的抗抵赖							√

3．安全机制

OSI 安全体系结构没有详细说明安全服务应该如何来实现。作为指南，它给出了一系列可用来实现这些安全服务的安全机制，基本的机制如图 1-2 所示，包括加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、通信业务流填充机制、路由控制和公证机制（把数据向可信第三方注册，以便使人相信数据的内容、来源、时间和传递过程）。

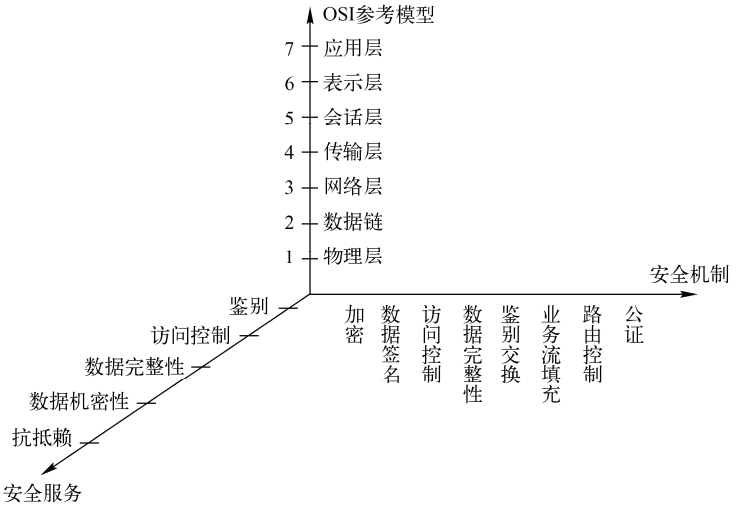


图 1-2　计算机网络安全体系结构三维图

安全服务与安全机制的关系如表 1-10 所示。

表 1-10　安全服务与安全机制的关系

安全服务 \ 协议层		加密	数字签名	访问控制	数据完整性	认证交换	业务流填充	公证
鉴别	对等实体鉴别	√	√			√		
	数据原发鉴别	√	√					
访问控制				√				
数据机密性	连接机密性	√					√	
	无连接机密性	√					√	
	选择字段机密性	√						
	业务机密性	√				√	√	
数据完整性	可恢复的连接完整性	√			√			
	不可恢复的连接完整性	√			√			
	选择字段的连接完整性	√			√			
	无连接完整性	√	√		√			
	选择字段的无连接完整性	√	√		√			
抗抵赖性	数据原发证明的抗抵赖	√	√		√			√
	交付证明的抗抵赖	√	√		√			√

1.4.3　P2DR 模型

P2DR 模型是一种常用的网络安全模型，如图 1-3 所示。P2DR 模型包含 4 个主要部分：Policy（安全策略）、Protection（防护）、Detection（检测）和 Response（响应）。防护、检测和响应组成了一个完整的、动态的安全循环。在整体安全策略的控制和指导下，在综合运用防护工具（如防火墙、身份认证和加密等手段）的同时，利用检测工具（如网络安全评估、入侵检测等系统）掌握系统的安全状态，然后通过适当的响应将网络系统调整到“最安全”或“风险最低”的状态。该模型认为：安全技术措施是围绕安全策略的具体需求而有序地组织在一起，构成一个动态的安全防范体系。

图 1-3　P2DR 模型示意图

- Protection：防护通常是通过采用一些传统的静态安全技术及方法来实现的，主要有防火墙、加密和认证等方法。
- Detection：在 P2DR 模型，检测是非常重要的一个环节，检测是动态响应和加强防护的依据，也是强制落实安全策略的有力工具，通过不断地检测和监控网络和系统，来发现新的威胁和弱点，通过循环反馈来及时做出有效的响应。
- Response：响应在安全系统中占有最重要的地位，是解决潜在安全问题的最有效办

法。从某种意义上讲，安全问题就是要解决响应和异常处理问题。要解决好响应问题，就要制定好响应的方案，做好响应方案中的一切准备工作。

- Policy：安全策略是整个网络安全的依据。不同的网络需要不同的策略，在制定策略以前，需要全面考虑局域网中如何在网络层实现安全性，如何控制远程用户访问的安全性，在广域网上的数据传输实现安全加密传输和用户的认证等问题。对这些问题做出详细回答，并确定相应的防护手段和实施办法，就是针对网络系统的一份完整的安全策略。策略一旦制定，就应当作为整个网络系统安全行为的准则。

P2DR 模型有一套完整的理论体系，以数学模型作为其论述基础——基于时间的安全理论（time based security）。该理论的基本思想是认为与信息安全有关的所有活动，包括攻击行为、防护行为、检测行为和响应行为等都要消耗时间，可以用时间来衡量一个体系的安全性和安全能力。

作为一个防护体系，当入侵者要发起攻击时，每一步都需要花费时间。攻击成功花费的时间就是安全体系提供的防护时间 Pt。在入侵发生的同时，检测系统也在发挥作用，检测到入侵行为所要花费的时间就是检测时间 Dt；在检测到入侵后，系统会做出应有的响应动作，该过程所要花费的时间就是响应时间 Rt。

P2DR 模型通过一些典型的数学公式来表达安全的要求。

$$Pt>Dt+Rt \tag{1-1}$$

Pt：系统为了保护安全目标设置各种保护后的防护时间；或者理解为在这样的保护方式下，黑客（入侵者）攻击安全目标所花费的时间。

Dt：从入侵者开始发动入侵开始，系统能够检测到入侵行为所花费的时间。

Rt：从发现入侵行为开始，系统能够做出足够的响应，将系统调整到正常状态的时间。

那么，针对需要保护的安全目标，如果上述数学公式满足，防护时间大于检测时间加上响应时间，则在入侵者危害安全目标之前就能够检测到并及时处理。

$$Et=Dt+Rt \tag{1-2}$$

如果 Pt=0，公式的前提是假设防护时间为 0。这种假设对 Web Server 这样的系统可以成立。

Dt：从入侵者破坏了安全目标系统开始，系统能够检测到破坏行为所花费的时间。

Rt：从发现遭到破坏开始，系统能够做出足够的响应，将系统调整到正常状态的时间。比如，对 Web Server 被破坏的页面进行恢复。

那么，Dt 与 Rt 的和就是该安全目标系统的暴露时间 Et。针对需要保护的安全目标，Et 越小，系统就越安全。

通过上面两个公式的描述，实际上对安全给出了一个全新的定义：“及时的检测和响应就是安全”和“及时的检测和恢复就是安全”。

而且，这样的定义为安全问题的解决给出了明确的方向：提高系统的防护时间 Pt，降低检测时间 Dt 和响应时间 Rt。

P2DR 理论给人们提出了新的安全概念，安全不能依靠单纯的静态防护，也不能依靠单纯的技术手段来解决。网络安全理论和技术还将随着网络技术和应用技术的发展而发展。未来的网络安全具有以下趋势。

一方面，高度灵活和自动化的网络安全管理辅助工具将成为企业信息安全主管的首选，

它能帮助管理相当庞大的网络，通过对安全数据进行自动的多维分析和汇总，使人从海量的安全数据中解脱出来，根据它提交的决策报告进行安全策略的制定和安全决策。

另一方面，由于网络安全问题的复杂性，网络安全管理将与较成熟的网络管理集成，在统一的平台上实现网络管理和安全管理。

另外，检测技术将更加细化，针对各种新的应用程序的漏洞评估和入侵监控技术将会产生，还将有攻击追踪技术应用到网络安全管理的环节当中。

P2DR 安全模型也存在一个明显的弱点，就是忽略了内在的变化因素，如人员的流动、人员素质的差异和安全策略贯彻执行的不完全等。实际上，安全问题牵涉的面非常广，不仅包括防护、检测和响应，还包括系统本身安全能力的增强、系统结构的优化和人员素质的提升等，而这些方面都是 P2DR 安全模型没有考虑到的。

1.4.4 网络安全技术

本节将分析网络安全的典型技术。

1．物理安全措施

物理安全是保护计算机网络设备、设施，以及其他媒体免遭地震、水灾、火灾等环境因素，人为操作失误，以及各种计算机犯罪行为导致的破坏过程。它主要包括 3 个方面。

- **环境安全**：对系统所在环境的安全保护措施，如区域保护和灾难保护。
- **设备安全**：设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护技术和措施等。
- **媒体安全**：媒体数据的安全，以及媒体本身的安全技术和措施。

为保证计算机网络的物理安全，除了网络规划和场地、环境等要求之外，还要防止信息在空间的扩散。因为，计算机网络辐射的电磁信号可在几百甚至上千米以外截获，重要的政府、军队和金融机构在建信息中心时都要考虑电磁信息泄漏。

2．数据传输安全技术

为保障数据传输的安全，通常采用数据传输加密技术、数据完整性鉴别技术及防抵赖技术。数据传输加密技术就是对传输中的数据流进行加密，以防止通信线路上的窃听、泄漏、篡改和破坏。如果以加密实现的通信层次来区分，加密可以在通信的 3 个不同层次来实现，即链路加密（位于 OSI 网络层以下的加密）、结点加密和端到端加密（传输前对文件加密，位于 OSI 网络层以上的加密）。一般常用的是链路加密和端到端加密这两种方式。链路加密侧重于在通信链路上而不考虑信源和信宿，对保密信息通过各链路采用不同的加密密钥提供安全保护。链路加密是面向结点的，对于网络高层主体是透明的，对高层的协议信息（地址、检错、帧头帧尾）都加密，数据在传输中是密文，但在中央结点必须解密得到路由信息。端到端加密是指信息由发送端进行加密，打入 TCP/IP 数据包封装，然后作为不可阅读和不可识别的数据穿过网络，这些信息一旦到达目的地后，将自动重组、解密，成为可读数据。端到端加密是面向网络高层主体，不对下层协议进行信息加密，协议信息以明文形式传输，用户数据在交换结点无须解密。

防抵赖技术包括对数据源和目的地双方的证明，常用的方法是数字签名，数字签名采用一定的数据交换协议，使得通信双方能够满足两个条件：接收方能够鉴别发送方所宣称的身份；发送方不能否认发送过数据的事实。比如，通信的双方采用公钥体制，发送方使用接收方的公钥和自己的私钥加密信息，只有接收方凭借自己的私钥和发送方的公钥解密之后才能读

懂，而对于接收方的回执也是同样道理。

3．内外网隔离技术

采用防火墙技术可以将内部网络与外部网络进行隔离，对内部网络进行保护。并且，还可以防止影响一个网段的问题在整个网络传播。防火墙技术是实现内外网的隔离与访问控制，保护内部网安全的最主要、最有效、最经济的措施。

4．入侵检测技术

利用防火墙技术，通常能够在内外网之间提供安全的网络保护，降低网络的安全风险。但是，仅利用防火墙，网络安全还远远不够，例如，入侵者会寻找防火墙背后可能敞开的后门、入侵者可能就在防火墙内等。

入侵检测的目的就是提供实时的检测及采取相应的防护手段，以便对进出各级局域网的常见操作进行实时检查、监控、报警和阻断，从而防止针对网络的攻击与犯罪行为，阻止黑客的入侵。

5．访问控制技术

访问控制是维护计算机网络系统安全、保护计算机资源的重要手段，是保证网络安全最重要的核心策略之一。访问控制就是给用户和用户组赋予一定的权限，控制用户和用户组对目录、子目录、文件和其他资源的访问，以及指定用户对这些文件、目录及设备能够执行的操作。受托者指派和继承权限屏蔽是实现访问控制的两种方式。受托者指派控制用户和用户组如何使用网络服务器的目录、文件和设备；继承权限屏蔽相当于一个过滤器，可以限制子目录从父目录那里继承哪些权限。根据访问权限将用户分为以下几类：①特殊用户，即系统管理员；②一般用户，系统管理员根据用户的实际需要为他们分配操作权限；③审计用户，负责网络的安全控制与资源使用情况的审计。用户对网络资源的访问权限可以用访问控制表来描述。

6．审计技术

审计技术是记录用户使用计算机网络系统进行所有活动的过程，记录系统产生的各类事件。审计技术是提高安全性的重要方法，它不仅能够识别谁访问了系统，还能指出系统正被怎样使用。对系统事件进行记录，能够更迅速和系统地识别系统出现的问题，为事故处理提供重要依据。另外，通过对安全事件的不断收集与积累，并且加以分析，以及有选择地对其中的某些用户进行审计跟踪，可以发现并为证明其破坏性行为提供有力的证据。

7．安全性检测技术

网络系统的安全性取决于网络系统中最薄弱的环节。如何及时发现网络系统中最薄弱的环节？如何最大限度地保证网络系统的安全？最有效的方法是定期对网络系统进行安全分析，及时发现并修正存在的弱点和漏洞。

网络安全检测（漏洞检测）是对网络的安全性进行评估分析，通过实践性的方法扫描分析网络系统，检查系统存在的弱点和漏洞，提出补救措施和安全策略的建议，达到增强网络安全性的目的。

8．防病毒技术

在网络环境下，计算机病毒有不可估量的威胁和破坏力，计算机病毒的防范是网络安全建设中重要的一环。网络反病毒技术包括预防病毒、检测病毒和消除病毒 3 种。

9．备份技术

采用备份技术可以尽可能快地全面恢复运行计算机网络所需的数据和系统信息。根据系统安全需求可选择的备份机制有：场地内高速度、大容量自动的数据存储、备份与恢复；场地外的数

据存储、备份与恢复。备份不仅能在网络系统硬件故障或人为失误时起到保护作用，而且，在入侵者非授权访问，数据完整性面临破坏时起到保护作用，同时是系统灾难恢复的前提之一。

10．终端安全技术

终端安全技术主要解决终端的安全保护问题，一般的安全功能有：基于口令或（和）密码算法的身份验证，防止非法使用终端；自主和强制存取控制，防止非法访问文件；多级权限管理，防止越权操作；存储设备安全管理，防止非法 U 盘复制和硬盘启动；数据和程序代码加密存储，防止信息被窃；预防病毒，防止病毒侵袭；严格的审计跟踪，便于追查责任事故。苹果发布了 iOS 系统安全技术指南，提供一个针对病毒、恶意软件，以及其他一些漏洞的安全防护。Android 保留和继承了 Linux 操作系统的安全机制，而且其系统架构的各个层次都有独特的安全特性。

1.5 计算机网络安全管理

面对网络安全的脆弱性，除了采用各种网络安全技术和完善系统的安全保密措施外，还必须加强网络的安全管理，诸多的不安全因素恰恰存在于组织管理方面。据权威机构统计表明：信息安全大约 60%以上的问题是由管理造成的，也就是说，解决信息安全问题不应仅从技术方面着手，同时更应加强信息安全的管理工作。

1.5.1 网络安全管理的法律法规

网络（信息）安全标准是信息安全保障体系的重要组成部分，是政府进行宏观管理的重要依据。信息安全标准不仅关系到国家安全，同时也是保护国家利益的一种重要手段，并且，有利于保证网络安全产品的可信性、实现产品的互联和互操作性，以支持计算机网络系统的互联、更新和可扩展性，支持系统安全的测评与评估，保障计算机网络系统的安全可靠。

英国标准协会（BSI）于 1995 年制定了信息安全管理体系标准——BS 7799。目前，我国有章可循的国际国内信息安全标准有 100 多个，如《信息处理 64bit 分组密码算法的工作方式》《计算站场地技术条件》和《计算机机房用活动地板技术条件》等。

1.5.2 计算机网络安全评价标准

计算机网络安全评价标准是一种技术性法规。在信息安全这一特殊领域，如果没有这一标准，与此相关的立法和执法就会有失偏颇，最终会给国家的信息安全带来严重后果。由于信息安全产品和系统的安全评价事关国家的安全利益，因此，许多国家都在充分借鉴国际标准的前提下，积极制定本国的计算机安全评价认证标准。

1.6 计算机网络安全技术发展趋势

随着网络的普及，以及越来越多的人掌握了网络知识，网上攻击事件也越来越多，网络受到的安全威胁也越发严重，网络用户为了保护自己的信息安全开始关注各类网络防护措施。据调查，企业局域网用户最关心网络安全的占了 66%。

1.6.1 网络安全威胁发展趋势

美国基础设施保护中心（NIPC）做了一个统计，近几年，平均每个月出现 10 个以上新的攻击手段。CNNS 特地组织安全专家对近 3 年的信息安全威胁，尤其是最近出现的新攻击手段进行分析，发现基于各种攻击机制的各种现成攻击工具越来越智能化，也越来越傻瓜化。虽然大多数的攻击手法都非常相似，无非是蠕虫、后门、rootkits、DoS 和 sniffer 等，但这些手段都体现了惊人的威力。攻击手段的新变种，与以前出现的相比，更加智能化，攻击目标直指互联网基础协议和操作系统层次。同时，黑客工具应用起来也越来越简单，很多新手也能轻易使用。

病毒技术与黑客技术的结合对信息安全造成更大的威胁。近年来，流行的计算机病毒无一例外地与网络结合，并具有多种传播方法和攻击手段，一经爆发即在网络上快速传播，难以遏制，加之与黑客技术的融合，潜在的威胁和损失更巨大。从发展趋势来看，现在的病毒已经由从前的单一传播、单种行为，变成依赖互联网传播，集电子邮件、文件传染等多种传播方式，融黑客、木马等多种攻击手段为一身的广义的“新病毒”。今后恶意代码、网络安全威胁和攻击机制的发展将具有以下特点。

1）与 Internet 更加紧密地结合，利用一切可以利用的方式（如邮件、局域网、远程管理和即时通信工具等）进行传播。

2）所有的病毒都具有混合型特征，集文件传染、蠕虫、木马和黑客程序的特点于一身，破坏性大大增强。

3）扩散极快，且更加注重欺骗性。

4）利用系统漏洞将成为病毒有力的传播方式。

5）无线网络技术的发展使远程网络攻击的可能性加大。

6）各种境外情报和谍报人员将越来越多地通过信息网络渠道收集情报和窃取资料。

7）各种病毒、蠕虫和后门技术越来越智能化，并出现整合趋势，形成混合性威胁。

8）各种攻击技术的隐秘性增强，常规防范手段难以识别。

9）分布式计算技术用于攻击的趋势增强，威胁高强度密码的安全性。

10）一些政府部门的超级计算机资源将成为攻击者利用的跳板。

11）网络管理安全问题日益突出。

1.6.2 网络安全主要实用技术的发展

网络安全技术的发展是多维的、全方面的，主要有以下几种。

1．物理隔离

物理隔离的思想是不安全就不联网，要绝对保证安全。在物理隔离的条件下，如果需要进行数据交换，就如同两台完全不相连的计算机，必须通过移动硬盘、U 盘等媒介，从一台计算机向另一台计算机复制数据，这也被形象地称为“数据摆渡”。由于两台计算机没有直接连接，就不会有基于网络的攻击威胁。

2．逻辑隔离

在技术上，实现逻辑隔离的方式多种多样，但主要还是采用防火墙。防火墙在体系结构上有不同的类型：双网口、多网口、DMZ 和 SSN。不同类型的防火墙在 OSI 的 7 层模型上的工作机理有明显的不同。防火墙的发展主要是提高性能、安全性和功能。实际上，这三者是相互矛盾、相互制约的。功能多、安全性好的技术往往性能受影响；功能多也影响到系统的安全。

3．防御来自网络的攻击

主要是抗击 DoS 等拒绝服务攻击，其技术是识别正常服务的包，将攻击包分离出来。目前 DDoS（分布式 DoS）的攻击能力可达到 10 万以上的并发攻击，因此，抗攻击网关的防御能力必须达到抗击 10 万以上并发的分布式 DoS 攻击。

4．防御网络上的病毒

传统的病毒检测和杀病毒是在客户端完成的。但是这种方式存在致命的缺点，如果某台计算机发现病毒，说明病毒已经感染了单位内部几乎所有的计算机。在单位内部的计算机网络和互联网的连接处放置防病毒网关，一旦出现新病毒，更新防病毒网关就可清除每个终端的病毒。

5．身份认证

一般认为，鉴别、授权和管理（AAA）系统是一个非常庞大的安全体系，主要用于大的网络运营商。实际上单位内部网同样需要一套强大的 AAA 系统。根据 IDC 的报告，单位内部的 AAA 系统是目前网络安全应用增长最快的部分。

6．加密通信和虚拟专用网

移动办公、单位和合作伙伴之间、分支机构之间通过公用的互联网通信是必不可少的。加密通信和虚拟专用网（VPN）有很大的需求。IPSec 已成为主流和标准，VPN 的另外一个方向是向轻量级方向发展。

7．入侵检测和主动防卫（IDS）

互联网的发展已经暴露出易被攻击的弱点。针对黑客的攻击，有必要采用入侵检测和主动防卫（IDS），实时交互监测和主动防卫的手段。

8．网管、审计和取证

网络安全越完善，体系架构就越复杂，最好的方式是采用集中网管技术。审计和取证功能变得越来越重要。审计功能不仅可以检查安全问题，而且还可以对数据进行系统的挖掘，从而了解内部人员使用网络的情况，了解用户的兴趣和需求等。

9．网络行为安全监管技术

网络行为监控是网络安全的重要方面，研究的范围包括网络事件分析、网络流量分析、网络内容分析，以及相应的响应策略与响应方式。

10．容灾与应急处理技术

容灾与应急响应是一个非常复杂的网络安全技术领域，涉及众多网络安全关键技术，需要多个技术产品的支持。主要技术包含应急响应体系的整体架构、应急响应体系的标准制定和应急响应的工具开发。

11．可信计算技术

通过增强现有的 PC 终端体系结构的安全性来保证整个计算机网络的安全，在计算机网络中搭建一个诚信体系，每个终端都具有合法的网络身份，并能够被认可；而且终端对恶意代码，如病毒、木马等有免疫能力。在这样的可信计算环境中，任何终端出现问题，都能保证合理取证，方便监控和管理。

1.7 小结

随着计算机网络广泛应用于经济、军事和教育等各领域，计算机网络安全成为涉及个人、单位、社会和国家信息安全的重大问题。计算机网络实体和软件系统面临的不安全因素

有：偶然发生的故障、自然灾害，以及人为破坏。人为对计算机网络的破坏可分为被动攻击、主动攻击、邻近攻击、内部人员攻击和分发攻击等 5 种形式。

造成计算机网络不安全的主要原因首先来自互联网本身，由于互联网的开放性、国际性和自由性，使其不可避免地会受到黑客的攻击。操作系统和数据库存在的安全缺陷是造成网络系统安全受到威胁的最重要原因。另外，传输线路的安全，以及网络的安全管理不当都直接影响着网络的安全性。

计算机网络安全要达到的目标就是确保信息系统的保密性、完整性、可用性、不可否认性和可控性。要确保计算机网络的安全，就必须依靠先进的技术、严格的管理和配套的法律。OSI 安全体系结构中定义了鉴别、访问控制、数据机密性、数据完整性和抗抵赖 5 种网络安全服务，以及加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、通信业务流填充机制、路由控制和公证机制 8 种基本的安全机制。

1.8 习题

1．计算机网络面临的典型安全威胁有哪些？
2．分析计算机网络的脆弱性和安全缺陷。
3．分析计算机网络的安全需求。
4．计算机网络安全的内涵和外延分别是什么？
5．论述 OSI 安全体系结构。
6．简述 P2DR 安全模型的结构。
7．简述计算机网络安全技术及其应用。
8．简述网络安全管理的意义和主要内容。

第2章 物 理 安 全

物理安全是整个计算机网络系统安全的前提。物理安全是保护计算机网络设备、设施及其他媒体免遭地震、水灾、火灾等环境事故、人为操作失误或各种计算机犯罪行为导致的破坏过程。物理安全主要考虑的问题是环境、场地和设备的安全，以及物理访问控制和应急处置计划等。物理安全技术主要是指对计算机及网络系统的环境、场地、设备和人员等采取的安全技术措施。物理安全在整个计算机网络信息系统安全中占有重要地位。它主要包括以下几个方面。

- 机房环境安全：计算机网络系统机房环境的安全特点是：可控性强，损失也大。对计算机网络系统所在环境的安全保护，如区域保护和灾难保护的相关标准，可参见有关国家标准。机房环境安全主要包括机房防火与防盗、防雷与接地、防尘与防静电、防地震等自然灾害等。
- 通信线路安全：通信线路安全主要包含通信线路的防窃听技术。
- 设备安全：设备安全主要包括防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。硬盘损坏、设备使用寿命到期等的物理损坏，停电、电磁干扰和意外事故等引起的设备故障，也是保障设备安全的重要内容。
- 电源安全：电源是机房内所有电子设备正常工作的能量源泉，在机房安全中占有重要地位。电源安全主要包括电力能源供应、输电线路安全和保持电源的稳定性等。

对于任何计算机网络系统，物理安全都是必须考虑的重要问题，物理安全措施包括安全制度、数据备份、辐射防护、屏幕口令保护、隐藏销毁、状态检测、报警确认、应急恢复、加强机房管理、运行管理、安全组织和人事管理等手段。物理安全是相对的，在设计物理安全方案时，要综合考虑需要保护的硬件、软件及其信息价值，从而采用适当的物理保护措施。

2.1 机房安全

机房安全技术涵盖的范围非常广泛，机房从里到外，从设备设施到管理制度都属于机房安全技术研究的范围。从这个意义上讲，下面几节的内容都是机房安全技术在某些方面的具体实现。

计算机机房的安全保卫技术是机房安全技术的重要一环，主要的安全技术措施包括防盗报警、实时监控和安全门禁等。计算机机房的温度、湿度等环境条件保持技术可以通过加装通风设备、排烟设备和专业空调设备来实现。计算机机房的用电安全技术也是机房安全技术的重要环节，主要包括不同用途电源分离技术、电源和设备有效接地技术、电源过载保护技术，以及防雷击技术等。计算机机房安全管理技术是指制定严格的计算机机房工作管理制度，并要求所有进入机房的人员严格遵守管理制度，将制度落到实处。

机房的安全等级分为 A 类、B 类和 C 类 3 个基本类别。

- A 类：对计算机机房的安全有严格的要求，有完善的计算机机房安全措施。

● B 类：对计算机机房的安全有较严格的要求，有较完善的计算机机房安全措施。

● C 类：对计算机机房的安全有基本的要求，有基本的计算机机房安全措施。

计算机机房的安全要求的详细情况如表 2-1 所示。

表 2-1　计算机机房安全要求

安全类别 / 安全项目	A 类机房	B 类机房	C 类机房
场地选择	—	—	
防火	—	—	—
内部装修	+	—	
供配电系统	+	—	—
空调系统	+	—	—
火灾报警和消防设施	+	—	—
防水	+	—	
防静电	+	—	
防雷击	+	—	
防鼠害	+	—	
防电磁泄漏	—	—	

表中符号说明：+表示要求，—表示有要求或增加要求。

1．机房的安全要求

如何减少无关人员进入机房的机会是计算机机房设计时首先要考虑的问题。为此，计算机机房在选址时应避免靠近公共区域，避免窗户直接临街，此外在机房布局上应使工作区在内，生活辅助区域在外。在一个大的建筑内，计算机机房最好不要安排在底层或顶层，这是因为底层一般较潮湿，而顶层有漏雨、穿窗而入的危险。在较大的楼层内，计算机机房应靠近楼层的一边安排布局。这样既便于安全警卫，又利于发生火灾险情时及时转移撤离。

应当保证所有进出计算机机房的人都必须在管理人员的监控之下。外来人员一般不允许进入机房内部，特殊需要进入机房内部的，应办理相关手续，并对来访者的随身物品进行相应的检查。

计算机机房所在建筑物的结构从安全的角度还应该考虑以下几个问题。

1）电梯和楼梯不能直接进入机房。

2）建筑物周围应有足够亮度的照明设施和防止非法进入的设施。

3）外部容易接近的进出口，如风道口、排风口、窗户和应急门等应有栅栏或监控措施，而周边应有物理屏障（隔墙、带刺铁丝网等）和监视报警系统，窗口应采取防范措施，必要时安装自动报警设备。

4）机房进出口必须设置应急电话。

5）机房供电系统应将动力照明用电与计算机系统供电线路分开，机房及疏散通道要安装应急照明装置。

6）机房建筑物方圆 100m 内不能有危险建筑物。危险建筑物主要指易燃、易爆或有害气体等的存放场所，如加油站、煤气站、天然气煤气管道和散发强烈腐蚀气体的设施、工厂等。

7）机房内应设置更衣室和换鞋处，机房的门窗要具有良好的封闭性能。

8）机房内的照明应达到规定标准。

2．机房的防盗要求

众所周知，计算机网络系统的大部分设备都是放置在计算机机房中的，重要的应用软件和业务数据也都是存放在服务器计算机系统的磁盘或光盘上的。此外，机房内的某些设备可能是用来进行机密信息处理的，这类设备本身及其内部存储的信息都非常重要，一旦丢失或被盗，将产生极其严重的后果。因此，对重要的设备和存储媒体（磁盘等）应采取严格的防盗措施。

早期主要采取增加质量和胶粘的防盗措施，即将重要的计算机网络设备永久地固定或粘接在某个位置上。虽然该方法增强了设备的防盗能力，但给设备的移动或调整位置带来了不便。随后，又出现了将设备与固定底盘用锁连接的防盗方法，只有将锁打开才可移动设备。现在某些笔记本计算机还在采用机壳加锁扣的防盗方法。

国外一家公司发明了一种通过光纤电缆保护重要设备的方法。该方法是将每台重要的设备通过光纤电缆串接起来，并使光束沿光纤传输，如果光束传输受阻，则自动报警。该保护装置比较简便，一套装置可保护机房内的所有重要设备，并且不影响设备的可移动性。

一种更方便的防护措施类似于图书馆和超市使用的防盗系统。首先在需要保护的重要设备、存储媒体和硬件上贴上特殊标签（如磁性标签），当非法携带这些重要设备或物品外出时，检测器就会发出报警信号。

视频监视系统是一种更为可靠的防盗设备，能实时地对计算机网络系统的外围环境和操作环境进行全程监控。对重要的机房，还应采取特别的防盗措施，如值班守卫、出入口安装金属探测装置等。

3．机房的三度要求

温度、湿度和洁净度并称为三度，为保证计算机网络系统的正常运行，对机房内的三度都有明确的要求。为使机房内的三度达到规定的要求，空调系统、去湿机和除尘器是必不可少的设备。重要的计算机系统安放处还应配备专用的空调系统，它比公用的空调系统在加湿、除尘等方面有更高的要求。

（1）温度

计算机系统内有许多元器件，不仅发热量大而且对环境温度敏感。温度过低会导致硬盘无法启动，温度过高会使元器件性能发生变化，耐压性降低，导致工作不正常。总之，环境温度过高或过低都容易引起硬件损坏。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%。机房温度一般应控制在 18℃～22℃。

（2）湿度

湿度也是影响计算机网络系统正常运转的重要因素，机房内相对湿度过高会加速金属器件的腐蚀，引起电气部分绝缘性能下降，耐潮性能不良，同时湿度过大还会使灰尘的导电性能增强，电子器件失效的可能性也随之增大；而相对湿度过低则会导致计算机网络设备中的某些器件龟裂，印制电路板变形，特别是静电感应增加，会使计算机内存储的信息丢失或异常，严重时还会导致芯片损坏，严重危害计算机系统。机房内的相对湿度一般控制在 40%～60%为宜。湿度控制与温度控制最好都与空调联系在一起，由空调系统集中控制。机房内应安装温、湿度显示仪，随时观察和监测。

（3）洁净度

洁净度要求机房尘埃颗粒直径小于 0.5μm，平均每升空气含尘量小于 1 万颗。

灰尘会造成接插件的接触不良、发热元件的散热效率降低、电气元件的绝缘性能下降；

灰尘还会增加机械磨损，尤其对驱动器和盘片，灰尘不仅会使磁盘数据的读写出现错误，而且可能划伤盘片，甚至导致磁头损坏。因此，计算机机房必须有除尘、防尘的设备和措施，保持清洁卫生，以保证设备的正常工作。

4．防静电措施

不同物体间的相互摩擦或接触就会产生静电。如果静电不能及时释放而保留在物体内，就会产生能量不大但非常高的电位，而且静电在放电时还可能发生火花，容易造成火灾或损坏芯片等意外事故。计算机系统的 CPU、ROM 和 RAM 等关键部件大都是采用 MOS 工艺的大规模集成电路，对静电极为敏感，容易因静电而损坏。

静电对电子设备的损害具有如下特点。

- **隐蔽性**：人体不能直接感知静电，除非发生静电放电，但是发生静电放电人体也不一定能有电击的感觉，这是因为人体感知的静电放电电压为 2～3kV，所以静电具有隐蔽性。
- **潜在性**：有些电子元器件受到静电损伤后的性能没有明显的下降，但多次累加放电会给器件造成内伤而形成隐患。因此静电对器件的损伤具有潜在性。
- **随机性**：从一个电子元件生产出来以后，一直到它损坏以前，时刻都受到静电的威胁，而这些静电的产生也具有随机性，其损坏过程也具有随机性。
- **复杂性**：静电放电损伤的失效分析工作，因电子产品的精、细、微小的结构特点而费时、费事、费钱，要求较高的技术并往往需要使用扫描电镜等高精密仪器。即使如此，有些静电损伤现象也难以与其他原因造成的损伤加以区别，使人误把静电损伤失效当做其他失效。这在对静电放电损害未充分认识之前，常常归因于早期失效或情况不明的失效，从而不自觉地掩盖了失效的真正原因。所以静电对电子器件损伤的分析具有复杂性。

机房的内装修材料一般应避免使用挂毯、地毯等吸尘、容易产生静电的材料，而应采用乙烯材料。为了防静电，机房一般要安装防静电地板，并将地板和设备接地以便将设备内积聚的静电迅速释放到大地。机房内的专用工作台或重要的操作台应有接地平板。此外，工作人员的服装和鞋最好用低阻值的材料制作，机房内应保持一定的湿度，特别是在干燥季节应适当增加空气湿度，以免因干燥而产生静电。

5．接地与防雷要求

接地与防雷是保护计算机网络系统和工作场所安全的重要安全措施。接地是指整个计算机网络系统中各处电位均以大地电位为零参考电位。接地可以为计算机系统的数字电路提供一个稳定的 0V 参考电位，从而可以保证设备和人身的安全，同时也是防止电磁信息泄漏的有效手段。

（1）地线种类

1）保护地。计算机系统内的所有电气设备，包括辅助设备，外壳均应接地。如果电子设备的电源线绝缘层损坏而漏电时，设备的外壳可能带电，将造成人身和设备事故。因而必须将外壳接地，以使外壳上积聚的电荷迅速释放到大地。

要求良好接地的设备有：各种计算机外围设备、多相位变压器的中性线、电缆外套管、电子报警系统、隔离变压器、电源和信号滤波器，以及通信设备等。

配电室的变压器中点要求接大地。但从配电室到计算机机房如果有较长的输电距离，则应在计算机机房附近将中性线重复接地，这是因为零线上过高的电势会影响设备的正常工作。

保护地一般是为大电流泄放而接地。我国规定，机房内保护地的接地电阻≤4Ω。保护地在插头上有专门的一条芯线，由电缆线连接到设备外壳，插座上对应的芯线（地）引出与大地相连。

保护地线应连接可靠，一般不用焊接，而采用机械压紧连接。地线导线应足够粗，至少

应为 4 号 AWG 铜线，或为金属带线。

2）直流地。直流地又称逻辑地，是计算机系统的逻辑参考地，即计算机中数字电路的低电位参考地。数字电路只有 1 和 0 两种状态，其电位差一般为 3V～5V。随着超大规模集成电路技术的发展，电位差越来越小，对逻辑地的接地要求也越来越高。因为逻辑地（0）的电位变化直接影响到数据的准确性。直流地的接地电阻一般要求≤2Ω。

3）屏蔽地。为避免计算机网络系统各种设备间的电磁干扰，防止电磁信息泄漏，重要的设备和重要的机房都要采取适当的屏蔽措施，即用金属体来屏蔽设备或整个机房。金属体称为屏蔽机柜或屏蔽室。屏蔽体需与大地相连，形成电气通路，为屏蔽体上的电荷提供一条低阻抗的泄放通路。屏蔽效果的好坏与屏蔽体的接地密切相关，一般屏蔽地的接地电阻要求≤4Ω。

4）静电地。机房内人体本身、人体在机房内的运动，以及设备的运行等均可能产生静电。人体静电有时可达上千伏，人体与设备或元器件导电部分直接接触极易造成设备损坏。而设备运行中产生的静电干扰则会引起设备的运行故障。为消除静电可能带来的不良影响，除采取如测试人体静电、接触设备前先触摸地线、泄放电荷、保持室内一定的温度和湿度等管理方面的措施外，还应采取防静电地板等措施，即将地板金属基体与地线相连，以使设备运行中产生的静电随时释放掉。

5）雷击地。雷电具有很大的能量，雷击产生的瞬时电压可高达 l0MV 以上。单独建设的机房或机房所在的建筑物必须设置专门的雷击保护地（简称雷击地），以防止雷击产生的巨大能量和高压对设备和人身带来的危害。应将具有良好导电性能和一定机械强度的避雷针安置在建筑物的最高处，引下导线接到地网或地桩上，形成一条最短的、牢固的对地通路，即雷击地线。防雷击地线地网和接地桩应与其他地线系统保持一定的距离，至少应在 10m 以上。

（2）接地系统

计算机机房的接地系统是指计算机系统本身和场地的各种地线系统的设计和具体实施。

1）各自独立的接地系统。这种接地系统主要考虑直流地、交流地、保护地、屏蔽地和雷击地等的各自作用，为避免相互干扰，分别单独通过地网或接地桩接到大地。这种方案虽然理论上可行，但实施起来难度很大。

2）交、直流分开的接地系统。这种接地系统将计算机的逻辑地和雷击地单独接地，其他地共地。这既可使计算机工作可靠，又可减少一些地线。但这样仍需 3 个单独的接地体，无论从接地体的埋设场地考虑，还是从投资和施工难度考虑，都是很难承受的。

3）共地接地系统。共地接地系统的出发点是除雷击地外，另建一个接地体，此接地体的地阻要小，以保证泄放电荷迅速排放到大地。而计算机系统的直流地、保护地和屏蔽地等在机房内单独接到各自的接地母线，自成系统，再分别接到室外的接地体上。

这种接地系统的优点是减少了接地体的建设，各地之间独立，不会产生相互干扰。缺点是直流地（逻辑地）与其他地线共用，易受其他信号干扰影响。

4）直流地、保护地共用地线系统。这种接地系统的直流地和保护地共用接地体，屏蔽地、交流地和雷击地单独埋没。该接地方案的出发点是许多计算机系统内部已将直流地和保护地连在一起，对外只有一条引线，在此情况下，直流地与保护地分开已无实际意义。由于直流地与交流地分开，使计算机系统仍具有较好的抗干扰能力。

5）建筑物内共地系统。随着城市高层建筑群的不断增多，建筑物内各种设备、供电系统和通信系统的接地问题越来越突出。一方面，建筑高层化、密集化，接地设备多、要求高；另一方面高层建筑附近又不可能有足够的场地构造地线接地体。高层建筑目前基础施工都是光打

桩，整栋建筑从下到上都有钢筋基础。由于这些钢筋很多，且连成一体，深入到地下漏水层，同时各楼层钢筋均与地下钢筋相连，作为地线地阻很小（经实际测量可小于0.2Ω）。由于地阻很小，可将计算机机房及各种设备的地线共用建筑地，从理论上讲不会产生相互干扰，从实际应用看也是可行的。它具有投资少、占地少、阻值稳定等特点，符合城市建筑的发展趋势。

（3）接地体

接地体的埋设是接地系统好坏的关键。通常使用的接地体有地桩、水平栅网、金属接地板和建筑物基础钢筋等。

1）地桩。垂直打入地下的接地金属棒或金属管，是常用的接地体。它用在土壤层超过3m 厚的地方。金属棒的材料为钢或铜，直径一般应为 15mm 以上。为防止腐蚀、增大接触面积并承受打击力，地桩通常采用较粗的镀锌钢管。

金属棒做地桩形成的地阻主要与金属棒的长度和土壤情况有关，受直径的影响不大。金属棒的长度一般选择 3m 以上。由于单根接地桩地阻较大，在实际使用中常将多根接地桩连成环形或网格形，每两根地桩间的距离一般要大于地桩长度的两倍。

土壤的含水率和含盐量的多少决定了土壤的电阻率，而土壤电阻率是决定地线地阻的重要因素。为降低大地电阻率，常需采取水分保持和化学盐化措施。

在地网表层土壤适当种植草类或豆类植物，可保持土壤中的水分，又不致出现盐分流失的现象。此外，在接地桩周围土壤中要添加一些产生离子的化学物品，以提高土壤的电导率。这些化学物品有硫酸镁、硝酸钾和氯化钠等。其中硫酸镁是一种较好的降阻材料，它成本低，电导率高，对接地电极和附近的金属物体腐蚀作用弱。在土壤中添加硫酸镁时，可在地桩周围挖一条 0.3m 深的沟，在沟内填满硫酸镁，用土覆盖。这样硫酸镁不与地桩直接接触，以使其分布最佳而腐蚀作用又最小。另一种方法是用一个 0.6m 长的套管套在地桩外面，套管内填充硫酸镁至距地面 0.3m，套管与地面持平并用木盖盖住管口。这样，套管内的硫酸镁会随着雨水均匀地潜入到地桩周围。

化学盐化并不能永久地改变接地电阻。化学材料会随着雨水逐渐流失，一般有效期为 3 年，随着时间的延长应适当补充化学材料。

2）水平栅网。在土质情况较差，特别是岩层接近地表面无法打桩的情况下，可采用水平埋设金属条带和电缆的方法。金属条带应埋在地下 0.5～1m 深处，水平方向构成星形或栅格网形，在每个交叉处，条带应焊接在一起，且带间距离大于 1m。

水平铺设金属条带的方法同样要求采取保持水平和增加化学盐分的方法，使土壤的电阻率降低。

3）金属接地板。这种方法是将金属板与地面垂直埋在地下，与土壤形成至少 $0.2m^2$ 的双面接触。深度要求在永久性潮土壤以下 30cm，一般至少在地下埋 1.5m 深。金属板的材料通常为铜板，也可为铁板或钢板。

这种方法占地面积小，但为获得较好的效果，必须埋设多个金属板，使埋设难度和造价增高。因此，除特殊情况外，近年来已逐渐为地桩所代替。

4）建筑物基础钢筋。如前所述，现代高层建筑的基础桩深入地下几十米，基础钢筋在地下形成很大的地网并从地下延伸至顶层，每层均可接地线。这种接地体节省场地，经济、适用，是城市建设机房地线的发展方向。

（4）防雷措施

机房的外部防雷应使用接闪器、引下线和接地装置吸引雷电流，并为其泄放提供一条低

阻值通道。

机器设备应有专用地线，机房本身应有避雷设施，包括通信设备和电源设备有防雷击的技术设施，机房的内部防雷主要采取屏蔽、等电位连接、合理布线或防闪器、过电压保护等技术措施，以及拦截、屏蔽、均压、分流和接地等方法，从而达到防雷的目的。机房的设备本身也应有避雷装置和设施。

6．机房的防火、防水措施

计算机机房的火灾一般是由电气原因、人为事故或外部火灾蔓延引起的。电气原因主要是指电气设备和线路的短路、过载、接触不良、绝缘层破损或静电等原因导致电打火而引起的火灾。人为事故是指由于操作人员不慎、吸烟或乱扔烟头等，使充满易燃物质（如纸片、磁带和胶片等）的机房起火。外部火灾蔓延是因外部房间或其他建筑物起火而蔓延到机房，从而引起机房起火。

计算机机房的水灾一般是由于机房内有渗水、漏水等原因引起的。

机房内应有防火、防水措施。如机房内应有火灾、水灾自动报警系统，如果机房上层有用水设施，需加防水层；机房内应放置适用于计算机机房的灭火器，并建立应急计划和防火制度等。

为避免火灾和水灾，应采取如下具体措施。

（1）隔离

建筑物内的计算机机房四周应设计一个隔离带，以便外部的火灾至少可隔离一个小时。系统中特别重要的设备，应尽量与人员频繁出入的地区和堆积易燃物（如打印纸）的区域隔离。所有机房门应为防火门，外层应有金属蒙皮。计算机机房内部应用阻燃材料装修。

机房内应有排水装置，机房上部应有防水层，下部应有防漏层，以避免出现渗水、漏水现象。

（2）火灾报警系统

火灾报警系统的作用是在火灾初期就能检测到并及时发出警报。

火灾报警系统按传感器的不同，分为烟报警和温度报警两种类型。烟报警器可在火灾开始的发烟阶段就检测出，并发出警报。它的动作快，可使火灾及时被发觉。而热敏式温度报警器是在火焰发生、温度升高后发出报警信号。近年来还开发出一种新型的 CO 探测报警器，它可在发烟初期即可探测到火灾的发生，避免损失，且可避免人员因缺氧而死亡。

为安全起见，机房应配备多种火灾自动报警系统，并保证在断电后 24 小时之内仍可发出警报。报警器可采用音响或灯光报警，一般安放在值班室或人员集中处，以便工作人员及时发现并向消防部门报告，组织人员疏散等。

（3）灭火设施

机房应配置适用于计算机机房的灭火器材，机房所在楼层应有防火栓，以及必要的灭火器材和工具，这些设施应具有明显的标记，且需定期检查。主要的消防器材和工具包括以下两类。

1）灭火器。虽然机房建筑内要求有自动喷水、供水系统和各种灭火器，但并不是任何机房火灾都要自动喷水，因为有时对设备的二次破坏比火灾本身造成的损坏更为严重。因此，灭火器材最好使用气体灭火器，推荐使用不会造成二次污染的卤代烷 1211 或 1301 灭火器，如无条件，也可使用 CO_2 灭火器。一般每 $4m^2$ 至少应配置一个灭火器，还应有手持式灭火器，用于大设备灭火。

2）灭火工具及辅助设备。如液压千斤顶、手提式锯、铁锹、镐、榔头和应急灯等。

（4）管理措施

机房应制订完善的应急计划和相关制度，并严格执行计算机机房环境和设备维护的各项规章制度。加强对火灾隐患部位的检查，如电源线路要经常检查是否有短路处，防止出现火花引起火灾。要制订灭火的应急计划并对所属人员进行培训。此外，还应定期对防火设施和工作人员的掌握情况进行测试。

2.2 通信线路安全

如果所有的计算机系统都锁在室内，并且所有连接计算机系统的网络设备和接到计算机系统上的终端设备也都锁在同一室内，则通信与计算机系统一样安全（假定不存在对外连接的Modem）。但是当有计算机网络系统的通信线路连接到室外时，问题就产生了。

尽管从网络通信线路上提取信息所需要的技术比直接从通信终端获取数据的技术要高几个数量级，以目前的技术水平也是完全有可能实现的。

用一种简单（但很昂贵）的高技术加压电缆可以获得通信线路上的物理安全，这一技术是若干年前为美国国家电话系统而开发的。通信电缆密封在塑料套管中，并在线缆的两端充气加压。线上连接了带有报警器的监视器，用来测量压力。如果压力下降，则意味着电缆可能被破坏了，技术人员还可以进一步检测出破坏点的位置，以便及时进行修复。

电缆加压技术提供了安全的通信线。将加压电缆架设于整座楼中，每寸电缆都将暴露在外。如果任何人企图割电缆，监视器会启动报警器，通知安全保卫人员电缆已被破坏。假设任何人成功地在电缆上接了自己的通信线，在安全人员定期检查电缆的总长度时，就可以发现电缆拼接处。加压电缆是包裹在波纹铝钢丝网中的，几乎没有电磁发射，从而大大增强了通过通信线路窃听的难度。

光纤通信线曾被认为是不可搭线窃听的，其断破处立即就会被检测到，拼接处的传输速度会非常缓慢，令人难以忍耐。光纤没有电磁辐射，所以也不能用电磁感应窃密。不幸的是光纤的最大长度有限制，目前网络覆盖范围半径约 100km，长于这一长度的光纤系统必须定期地放大（复制）信号。这就需要将信号转换成电脉冲，然后再恢复成光脉冲，继续通过另一条线传送。完成这一操作的设备（复制器）是光纤通信系统的安全薄弱环节，因为信号可能在这一环节被搭线窃听。有两个办法可解决这一问题：距离大于最大长度限制的系统之间，不采用光纤通信；或加强复制器的安全，如用加压电缆、警报系统和加强警卫等措施。

对于任何可以直接存取而不加安全防护措施的系统，通信是特别严重的安全薄弱环节。当允许用户通过拨号连接到 Modem 访问计算机网络系统时，则计算机网络系统的安全程度将被大大削弱，因为有电话和 Modem 的任何人就可能非法进入该系统。因此，应当避免这一情况的发生，要确保 Modem 的电话号码不被列于电话簿上，并且最好将电话号码放在不同于本单位普通电话号码所在的交换机上。总之，不要假设没人知道自己的拨入号码，大多数攻击者都能使用自动拨号软件通过一个 Modem 整天依次调用拨号码，记录下连接上的 Modem 的号码。如果可能，安装一个局域 PBX，使得对外界的拨号产生 1 秒钟的拨号蜂音，并且必须输入一个与 Modem 相关联的扩展号码，就可有效提高系统的安全性。

2.3 设备安全

设备安全是一个比较宽泛的概念，包括设备的维护与管理、设备的电磁兼容和电磁辐射防护，以及信息存储媒体的安全管理等内容。

2.3.1 硬件设备的维护和管理

计算机网络系统的硬件设备一般价格昂贵，一旦损坏而又不能及时修复，不仅会造成经济损失，而且可能导致整个网络系统瘫痪，产生严重的不良影响。因此，必须加强对计算机网络系统硬件设备的使用管理，坚持做好硬件设备的日常维护和保养工作。

1．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操作使用规程，并严格按照操作规程进行操作。

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。

2．常用硬件设备的维护和保养

常用硬件设备的维护和保养包括主机、显示器、打印机和硬盘的维护保养；网络设备如HUB、交换机、路由器、MODEM、RJ-45 接头和网络线缆等的维护保养；还要定期检查供电系统的各种保护装置及地线是否正常。

所有的计算机网络设备都应当置于上锁且有空调的房间里。同时还要注意，电源插座附近清扫的工作人员或粗心的使用人员都可能使设备掉电。同时还要将对设备的物理访问权限限制在最小。

2.3.2 电磁兼容和电磁辐射的防护

1．电磁兼容和电磁辐射

计算机网络系统的各种设备都属于电子设备，在工作时都不可避免地会向外辐射电磁波，同时也会受到其他电子设备的电磁波干扰，当电磁干扰达到一定的程度时就会影响设备的正常工作。

电磁干扰可通过电磁辐射和传导两条途径影响电子设备的工作。一条是电子设备辐射的电磁波通过电路耦合到另一台电子设备中引起干扰；另一条是通过连接的导线、电源线和信号线等耦合而引起相互之间的干扰。

电子设备及其元器件都不是孤立存在的，而是在一定的电磁干扰环境下工作。电磁兼容性就是电子设备或系统在一定的电磁环境下互相兼顾、相容的能力。

电磁兼容问题由来已久。1831 年法拉第发现电磁感应现象，总结出电磁感应定律；1881 年英国科学家希维思德发表了“论干扰”的文章；1888 年赫兹通过试验演示了电磁干扰现象。20 世纪以来，特别是在第二次世界大战中，电磁兼容理论进一步发展，逐步形成了一门独立的学科。电磁兼容设计已成为军用武器装备和电子设备研制中必须严格遵守的原则，电磁兼容性成为产品可靠性保证的重要组成部分。如果设备的电磁兼容性很差，在电磁干扰的环境中就不能正常工作。我国已将电磁兼容性作为强制性的标准来执行。

1985 年在法国举办的“计算机与通信安全”国际会议上，荷兰的一位工程师现场演示了

用一套稍加改装的黑白电视机还原 1km 以外机房内计算机显示屏上的信息。这说明计算机的电磁辐射造成信息泄漏的危险是真实存在的。尤其是在微电子技术和卫星通信技术飞速发展的今天，各种信息窃取手段日趋先进，电磁辐射泄密的危险也越来越大。

美国、俄罗斯等发达国家已对电磁辐射泄密问题进行了多年研究，并逐渐形成了一种专门的技术——抑制信息处理设备的噪声泄漏技术，简称信息泄漏防护技术（Tempest 技术）。

Tempest 技术是一项综合性非常强的技术，包括泄漏信息的分析、预测、接收、识别、复原、防护、测试和安全评估等技术，涉及多个学科领域。Tempest 技术基本上是在传统的电磁兼容理论的基础上发展起来的，但比传统的抑制电磁干扰的要求要高得多，在技术实现上也更复杂。一般认为显示器的视频信号、打印机打印头的驱动信号、磁头读/写信号、键盘输入信号，以及信号线上的输入/输出信号等为需要重点防护的对象。美国政府规定，凡属高度机密部门所使用的计算机等信息处理设备，其电磁泄漏发射必须达到 Tempest 标准规定的要求。

2．电磁辐射防护的措施

为保证计算机网络系统的物理安全，除在网络规划、场地和环境等方面进行防护之外，还要防止数据信息在空间中的扩散。计算机系统通过电磁辐射使信息被截获而失密的案例已经很多，在理论和技术支持下的验证工作也证实这种截取距离在几百米甚至可达千米的复原显示给计算机系统信息的保密工作带来了极大的威胁。为了防止计算机系统中的数据信息在空间中的扩散，通常是在物理上采取一定的防护措施，以减少或干扰扩散到空间中的电磁信号。这对政府、军队及金融机构在构建信息中心时都将成为首先要解决的问题。

目前防护措施主要有两类：一类是对传导发射的防护，主要是对电源线和信号线加装性能良好的滤波器，减小传输阻抗和导线间的交叉耦合；另一类是对辐射的防护，这类防护措施又可分为以下两种：一种是采用各种电磁屏蔽措施，如对设备的金属屏蔽和各种接插件的屏蔽，同时对机房的下水管、暖气管和金属门窗进行屏蔽和隔离；另一种是干扰的防护措施，即在计算机系统工作的同时，利用干扰装置产生一种与计算机系统辐射相关的伪噪声向空间辐射来掩盖计算机系统的工作频率和信息特征。

为提高电子设备的抗干扰能力，除在芯片和部件上提高抗干扰能力外，主要的措施有屏蔽、隔离、滤波、吸波和接地等，其中屏蔽是应用最多的方法。

（1）屏蔽

电磁波经封闭的金属板之后，大部分能量被吸收、反射和再反射，再传到板内的能量已很小，从而保护内部的设备或电路免受强电磁干扰。

（2）滤波

滤波是另一种重要的方法。滤波电路是一种无源网络，它可让一定频率范围内的电信号通过而阻止其他频率的电信号，从而起到滤波作用。在有导线连接或阻抗耦合的情况下，进出线采用滤波器可使强干扰被阻止。

还有一种吸波作用，是采用铁氧体等吸波材料，在空间很小的情况下起到类似滤波器的作用。

（3）隔离

隔离是将系统内的电路采用隔离的方法分别处理，将强辐射源、信号处理单元等隔离开，单独处理，从而减弱系统内部和系统向外的电磁辐射。

（4）接地

接地对电磁兼容来说十分重要，它不仅可起到保护作用，而且可使屏蔽体、滤波器等集

聚的电荷迅速排放到大地，从而减小干扰。用于电磁兼容的地线最好单独埋放，对其地阻、接地点等均有很高的要求。

电磁防护层主要是通过上述种种措施，提高计算机的电磁兼容性，提高设备的抗干扰能力。使计算机能抵抗强电磁干扰；同时将计算机的电磁泄漏发射降到最低，使之不致将有用的信息泄漏出去。

2.3.3 信息存储媒体的安全管理

计算机网络系统的信息要存储在某种媒体上，常用的存储媒体有硬盘、磁盘、磁带、打印纸和光盘等。对存储媒体的安全管理主要包括以下几个方面。

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，要建立有效的级别和权限，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，并分类建立登记簿，记录编号、名称、用途、规格、制作日期、有效期、使用者和批准者等信息。

4）对存放有重要信息的磁盘、磁带和光盘，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磁盘、磁带和光盘，必须经过特殊的数据清除处理。

7）凡不能正常记录数据的磁盘、磁带和光盘，必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，应在磁盘、磁带和光盘的质量保证期内进行转储，转储时应确保内容正确。

2.4 电源系统安全

电源是计算机网络系统的命脉，电源系统的稳定可靠是计算机网络系统正常运行的先决条件，电源系统电压的波动、浪涌电流和突然断电等意外情况的发生还可能引起计算机系统存储信息的丢失、存储设备的损坏等情况的发生。电源系统的安全是计算机网络系统物理安全的一个重要组成部分。国内外关于电源的相关标准主要有以下两个。

- **直流电源的相关标准**。国际电工委员会（IEC）制定了直流稳定电源标准：IEC478.1－1974《直流输出稳定电源术语》；IEC478.2－1986《直流输出稳定电源额定值和性能》；IEC478.3－1989《直流输出稳定电源传导电磁干扰的基准电平和测量》；IEC478.4－1976《直流输出稳定电源除射频干扰外的试验方法》；IEC478.5－1993《直流输出稳定电源电抗性近场磁场分量的测量》。这一套标准颁布实施的时间较早，而国内相应的国家标准尚未颁布。国内颁布的有关直流稳定电源的电子行业标准有 SJ2811.1－87《通用直流稳定电源术语及定义、性能与额定值》和 SJ2811.2－87《通用直流稳定电源测试方法》。
- **交流电源的相关标准**。国际电工委员会（IEC）于 1980 年颁布了 IEC686－80《交流输出稳定电源》。1994 年，原电子工业部颁布了电子行业标准 SJ/T10541－94《抗干扰型交流稳压电源通用技术条件》和 SJ/T10542－94《抗干扰型交流稳压电源测试方法》。

在国标 GB2887－2011 和 GB9361－2011 中也对机房安全供电做了明确的要求。国标

GB2887－2011 将供电方式分为了 3 类。

- **一类供电**：需建立不间断供电系统。
- **二类供电**：需建立带备用的供电系统。
- **三类供电**：按一般用户供电考虑。

GB9361－2011 中也提出 A、B 类安全机房应符合如下要求。

- 计算站应设专用可靠的供电线路。
- 计算机系统的电源设备应提供稳定可靠的电源。
- 供电电源设备的容量应具有一定的余量。
- 计算机系统的供电电源技术指标应按 GB2887－2011《计算站场地技术要求》 中的第 9 章的规定执行。
- 计算机系统独立配电时，宜采用干式变压器。安装油浸式变压器时应符合 GBJ232－82《电气装置安装工程规范》中的规定。
- 从电源室到计算机电源系统的分电盘使用的电缆，除应符合 GB232－2010 中配线工程中的规定外，载流量应减少 50%。
- 计算机系统用的分电盘应设置在计算机机房内，并应采取防触电措施。
- 从分电盘到计算机系统的各种设备的电缆应为耐燃铜芯屏蔽的电缆。
- 计算机系统的各设备走线不得与空调设备、电源设备的无电磁屏蔽的走线平行。交叉时，应尽量以接近于垂直的角度交叉，并采取防延燃措施。
- 计算机系统应选用铜芯电缆，严禁铜、铝混用，若不能避免时，应采用铜、铝过渡头连接。
- 计算机电源系统的所有接点均应进行镀铅锡处理，冷压连接。
- 在计算机机房出入口处或值班室，应设置应急电话和应急断电装置。
- 计算站场地宜采用封闭式蓄电池。
- 使用半封闭式或开启式蓄电池时，应设专用房间。房间墙壁和地板表面应做防腐蚀处理，并设置防爆灯、防爆开关和排风装置。
- 计算机系统接地应采用专用地线。专用地线的引线应和大楼的钢筋网及各种金属管道绝缘。
- 计算机系统的几种接地技术要求及诸地之间的相互关系应符合 GB2887－2011 中的规定。
- 计算机机房应设置应急照明和安全口的指示灯。

C 类安全机房应满足 GB2887－2011 中规定的三类供电要求。

电源系统安全不仅包括外部供电线路的安全，更重要的是指室内电源设备的安全。下面将从电力能源的可靠供应和影响电源设备安全的潜在威胁等方面展开论述。

1. 电力能源的可靠供应

为了确保电力能源的可靠供应，以防外部供电线路发生意外故障，必须有详细的应急预案和可靠的应急设备。应急设备主要包括备用发电机、大容量蓄电池和 UPS 等。除了要求这些应急电源设备具有高可靠性外，还要求它们具有较高的自动化程度和良好的可管理性，以便在意外情况发生时保证电源的可靠供应。

2. 电源对用电设备安全的潜在威胁

（1）脉动与噪声

理想的直流电源应提供纯净的直流，然而总有一些干扰存在，比如在开关电源（SMPS）输出端口叠加的脉动电流和高频振荡。这两种干扰再加上电源本身产生的尖峰噪声，使电源出

现断续和随意的漂移（PARD）。

（2）电磁干扰

电磁干扰会产生电磁兼容性问题，目前这方面的标准有美国的 FCC 标准，FCC 分为 A 和 B 两个级别。国内相应的标准为 China Compulsory Certification 认证标准，即 3C 认证。FCC-A 级指工业标准，FCC-B 级指家用电器标准，只有达到 B 级的电源才被认为是安全无害的。当电源的电磁干扰比较强时，其产生的电磁场就会影响到硬盘等磁性存储介质，久而久之就会使存储的数据受到损害。

在电磁兼容性方面，国标 GB9254—2008：《信息技术设备的无线电干扰极限值和测量方法》对电磁干扰的极限值和测量方法都做了明确的规定。

GB9254—2008 将信息设备按安全性分为两级，即 A 级和 B 级，具体要求如下。

- A 级设备保护距离为 30m，通常用于工业环境中。
- B 级设备的保护距离为 10m，可用于住宅区、商业区、商务区、公共娱乐场所、户外场所和轻工业区等。

电磁骚扰可以通过设备的电源端子传导发射，造成电网的污染。因此，电磁兼容标准中对电源端子的传导骚扰发射进行了限制，这就是电源端子传导发射限值。表 2-2 给出了 A 级和 B 级电源端子的传导骚扰限值。

表 2-2　电源端子的传导骚扰限值

A 级			B 级		
频率范围/MHz	限值/dBμV		频率范围/MHz	限值/dBμV	
	准峰值	平均值		准峰值	平均值
0.15～0.50	79	66	0.15～0.50	66 ～ 56	56 ～ 46
0.50～50	78	60	0.50～5	56	46
			5～30	60	50

电缆上的共模电流会产生很强的电磁辐射，大部分设备在不连接电信电缆时能够顺利通过有关的标准，而连接上电缆后就不再满足标准的要求，这就是由于电缆中共模电流产生了共模辐射。因此本项对电信端口的共模传导发射提出了限制。表 2-3 给出了 A 级和 B 级电信端口的共模传导骚扰限值。

表 2-3　电信端口的共模传导骚扰限值

频率范围/MHz	A 级				B 级			
	电压限值/dBμV		电流限值/dBμA		电压限值/dBμV		电流限值/dBμA	
	准峰值	平均值	准峰值	平均值	准峰值	平均值	准峰值	平均值
0.15～0.5	97～87	84～74	53～43	40～30	84～74	74～64	40～30	30～20
0.5～30	87	74	43	30	74	64	30	20

信息设备在工作时会向空间辐射电磁波，这构成了对其他设备的骚扰，特别是对无线接收设备的影响很大。因此，本项对设备辐射的电磁波强度提出了限制。表 2-4 给出了 A 级和 B 级辐射骚扰限值。

表 2-4　辐射骚扰限值

频率范围/MHz	准峰值/（dBμV/m）	
	A 级	B 级
30～230	40	30
230～1000	47	37

此外，当电源纹波系数过大时，电源所输出的直流电压中掺杂了过多的交流成分，就会使主板、内存和显卡等半导体器件不能正常工作，而且当市电有较大波动时，电源输出电压产生大的变化，还有可能导致计算机和网络设备重新启动或不能正常工作。

2.5　小结

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，也是其他安全措施得以实施并发挥正常作用的基础和前提条件。计算机网络系统物理安全的内涵是保护计算机网络设备、设施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。主要内容为机房安全技术、通信线路安全技术和计算机网络系统设备安全技术等。机房安全主要是从机房场地、机房防盗、机房三度、防静电和防雷击等方面进行讨论。通信线路安全主要着重介绍加压电缆和光纤等通信线路的防窃听技术。计算机网络系统设备安全应采取的主要手段有计算机网络系统设备的安全管理和维护、信息存储媒体的管理和计算机网络系统设备的电磁兼容技术。电源系统安全应该注意电源电流或电压的波动可能会对计算机网络系统造成的危害。

2.6　习题

1．简述物理安全在计算机网络信息系统安全中的意义。
2．物理安全主要包含哪些方面的内容？
3．计算机机房安全等级的划分标准是什么？
4．计算机机房安全技术主要包含哪些方面的内容？
5．保障通信线路安全的主要技术措施有哪些？
6．电磁辐射对网络通信安全的影响主要体现在哪些方面，防护措施有哪些？
7．保障信息存储安全的主要措施有哪些？
8．简述各类计算机机房对电源系统的要求。

第 3 章　信息加密与 PKI

加密技术是保障信息安全的基石，它以很小的代价，对信息提供一种强有力的安全保护。长期以来，密码技术广泛应用于政治、经济、军事、外交和情报等重要部门。近年来随着计算机网络和通信技术的发展，密码学得到了前所未有的重视并迅速普及，同时其应用领域也广为拓展，如今密码技术不仅服务于信息的加密和解密，还是身份认证、访问控制和数字签名等多种安全机制的基础。

在理论上，信息加密是利用密码学的原理与方法对传输数据提供保护，它以数学计算为基础，信息论和复杂性理论是其两个重要组成部分。其中，信息论主要包括 Shannon 关于保密系统的信息理论和 Simmoms 关于认证系统的信息理论。密码学复杂性理论主要讨论算法复杂性和问题复杂性两方面的内容。在构成上，密码技术主要由密码编码技术和密码分析技术两个既相互对立又相互依存的分支组成，密码编码技术主要解决产生安全有效的密码算法问题，实现对信息的加密或认证；密码分析技术主要解决破译密码或伪造认证码问题，从而窃取保密信息或进行破坏活动。

3.1　密码学概述

为方便学习本章后续内容，先对密码学的发展历程、一些基本概念，以及单钥密码体制和双钥密码体制的原理进行概要性介绍。

3.1.1　密码学的发展

密码学是一门古老而深奥的科学，它以认识密码变换为本质，以加密与解密的基本规律为研究对象。密码学的发展历程大致经历了 3 个阶段：古代加密方法、古典密码和近代密码。

1．古代加密方法

应用需求是催生古代加密方法起源和进步的直接动力。据石刻及有关史料记载，许多古代文明，如埃及人、希伯来人等都是在实践中逐步发明并使用了密码系统。从某种意义上说，战争是科学技术进步的催化剂，自从有了战争，人类就面临着安全通信需求。研究表明，古代加密方法大约起源于公元前 440 年出现在古希腊战争中的隐写术。当时为了安全传送军事情报，奴隶主将奴隶的头发剃光，把情报写在奴隶的光头上，待头发长长后将奴隶送到另一个部落，再次剃光头发，原有的信息复现出来，从而实现两个部落间的秘密通信。

另一个将密码学用于通信的记录是，斯巴达人于公元前 400 年将 Scytale 加密工具用于军官间传递秘密信息。Scytale 实际上是一个锥形指挥棒，周围环绕一张羊皮纸，将要保密的信息写在羊皮纸上。解下羊皮纸，上面的消息杂乱无章、无法理解，但将它绕在另一个同等尺寸的棒子上后，就能看到原始的消息。

我国古代也早就出现以藏头诗、藏尾诗、漏格诗及绘画等形式，将需表达的消息或“密语”隐藏在诗文或画卷中特定位置的记载，若只注意诗或画的表面意境，则很难发现其中隐藏的“话外之音”。

总而言之，虽然这些古代加密方法只能限定在局部范围内使用，但其体现了密码学的若干典型特征。

2．古典密码

相比于古代加密方法，古典密码系统已变得较为复杂，并初步显现出近代密码系统的雏形，文字置换是其主要加密思想，一般通过手工或借助机械变换方式实现加密。古典密码的密码体制主要有单表代替密码、多表代替密码及转轮密码。例如，Caesar 密码就是一种典型的单表加密体制，多表代替密码有 Vigenere 密码、Hill 密码等。20 世纪 20 年代，随着机械和机电技术的逐步成熟，以及电报和无线电应用的出现，引起了密码设备方面的一场革命——发明了转轮密码机（简称转轮机，Rotor）。转轮机的出现是密码学发展的重要标志之一，由此传统密码学有了长足的进展，利用机械转轮人们开发出了许多极其复杂的加密系统，密码加密速度也大大提高。在第二次世界大战中，盟军破获的德军 Enigma 密码就是转轮密码的著名实例。由于转轮机的密钥量有限，二战中后期曾引发了一场加密与破译的对抗。

二战结束后，电子学开始被引入到密码机之中，第一个电子密码机也仅仅是一个转轮机，只是转轮被电子器件取代而已。这些电子转轮机的唯一优势在于其操作速度，但它们仍受制于机械式转轮密码机固有弱点（如密码周期有限、制造费用高等）的影响。

3．近代密码

20 世纪 70 年代，由于计算机科学的蓬勃发展，快速电子计算机和现代数学方法为加密技术提供了新的概念和工具，当然也给破译者提供了有力的武器。新技术的到来给密码设计者带来了前所未有的自由，他们可以轻易地摆脱原先用铅笔和纸张进行手工设计时易犯的错误，也不用为机械方式实现密码机的高额费用而发愁，从而可以设计出更为复杂的密码系统。

1949 年 Claude Shannon 发表了《保密系统的通信理论》（The Communication Theory of Secrecy Systems），这篇论文作为近代密码学的理论基础之一，直至 30 年之后才显示出它的价值。1976 年 Diffie 和 Hellman 发表了《密码学的新方向》（New Directions in Cryptography）一文，提出了适用于网络保密通信的公钥密码思想，开辟了公开密钥密码学的新领域，掀起了公钥密码研究的序幕。在这些思想的启迪下，各种公钥密码体制相继被提出，特别是 RSA 公钥密码体制的提出，是密码学史上的一个重要里程碑。可以说，没有公钥密码的研究就没有近代密码学。与此同时，美国国家标准局（NBS，即现在的国家标准与技术研究所 NIST）正式公布实施了美国的数据加密标准（Data Encryption Standard，DES）及其加密算法，并将之用于政府等非机密单位及商业领域的保密通信。上述两篇重要论文和美国数据加密标准 DES 的实施，标志着密码学理论与技术的划时代变革，宣布了近代密码学的开始。

近代密码学与计算机技术、电子通信技术紧密相关。在这一阶段，密码理论蓬勃发展，密码算法设计与分析互相促进，出现了大量的密码算法和各种攻击方法。另外，密码使用的范围也在不断扩大，而且出现了许多通用的加密标准。当然，密码学在飞速发展的同时，也出现了一些新的课题和方向。例如，在分组密码领域，由于 DES 已经无法满足高保密性的要求，美国于 1997 年开始征集新一代数据加密标准，即高级数据加密标准（Advanced Encryption Standard，AES），AES 征集活动使国际密码学界掀起了分组密码研究的新高潮。2006 年，高级数据加密标准已成为对称密钥加密中最流行的算法之一。

在公开密钥密码领域，椭圆曲线密码体制由于其安全性高、计算速度快等优点引起了人们的普遍关注。此外，由于嵌入式系统的发展和智能卡的应用，这些设备上所使用的密码算法由于系统本身资源的限制，要求密码算法以较小的资源快速实现，这样，公开密钥密码的快速实

现就成为一个新的研究热点。随着相关技术的发展，一些具有潜在密码应用价值的技术也得到了密码学家的高度重视，一些新的密码技术如混沌密码、量子密码等，正在逐步走向实用化。

3.1.2 密码学基本概念

密码学（cryptology）：密码学作为数学的一个分支，是研究信息系统安全保密的科学，是密码编码学和密码分析学的统称。

密码编码学（cryptography）：是使消息保密的技术和科学。密码编码学是密码体制的设计学，即怎样编码，采用什么样的密码体制保证信息被安全地加密。从事此行业的人员称为密码编码者（cryptographer）。

密码分析学（cryptanalysis）：是与密码编码学对应的技术和科学，即研究如何破译密文的科学和技术。密码分析学是在未知密钥的情况下从密文推演出明文或密钥的技术。密码分析者（cryptanalyst）是从事密码分析的专业人员。

在密码学中，有一个五元组：{明文，密文，密钥，加密算法，解密算法}，对应的加密方案称为密码体制（或密码）。

明文（Plaintext）：是作为加密输入的原始信息，即消息的原始形式，通常用 m 或 p 表示。所有可能明文的有限集称为明文空间，通常用 M 或 P 来表示。

密文（Ciphertext）：是明文经加密变换后的结果，即消息被加密处理后的形式，通常用 c 表示。所有可能密文的有限集称为密文空间，通常用 C 来表示。

密钥（Key）：是参与密码变换的参数，通常用 k 表示。一切可能的密钥构成的有限集称为密钥空间，通常用 K 表示。

加密算法（Encryption Algorithm）：是将明文变换为密文的变换函数，相应的变换过程称为加密，即编码的过程（通常用 E 表示，即 $c=E_k(p)$）。

解密算法（Decryption Algorithm）：是将密文恢复为明文的变换函数，相应的变换过程称为解密，即解码的过程（通常用 D 表示，即 $p=D_k(c)$）。

对于有实用意义的密码体制而言，总是要求它满足：$p=D_k(E_k(p))$，即用加密算法得到的密文总是能用一定的解密算法恢复出原始的明文来。而密文消息的获取同时依赖于初始明文和密钥的值。

一般地，密码系统的模型可用图 3-1 表示。

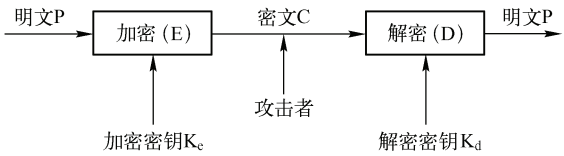


图 3-1　一般密码系统示意图

3.1.3 密码体制分类

密码体制从原理上可分为两大类，即单钥或对称密码体制（One-Key or Symmetric Cryptosystem）、双钥或非对称密码体制（Two-Key or Asymmetric Cryptosystem）。

1．单钥密码体制

单钥密码体制的本质特征是所用的加密密钥和解密密钥相同，或实质上等同，从一个可以推出另外一个。单钥体制不仅可用于数据加密，也可用于消息的认证，最有影响的单钥密码

是 1977 年美国国家标准局颁布的 DES 算法。系统的保密性主要取决于密钥的安全性，因此必须通过安全可靠的途径（如信使递送）将密钥送至收端。这种如何将密钥安全、可靠地分配给通信对方，包括密钥产生、分配、存储和销毁等多方面的问题统称为密钥管理（Key Management），是影响系统安全的关键因素。古典密码作为密码学的源头，其多种方法充分体现了单钥加密的思想，典型方法如代码加密、代替加密、变位加密和一次性密码簿加密等。

单钥密码体制的基本元素包括原始的明文、加密算法、密钥、密文及攻击者。单钥系统对数据进行加解密的过程如图 3-2 所示。

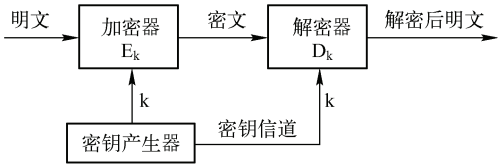


图 3-2　单钥密钥体制示意图

发送方的明文消息 $P=[P_1,P_2,\cdots,P_M]$，P 的 M 个元素是某个语言集中的字母，如 26 个英文字母，现在最常见的是二进制字母表{0,1}中元素组成的二进制串。加密之前先产生一个形如 $K=[K_1,K_2,\cdots,K_J]$ 的密钥作为密码变换的输入参数之一。该密钥或者由消息发送方生成，然后通过安全的渠道送到接收方；或者由可信的第三方生成，然后通过安全渠道分发给发送方和接收方。

发送方通过加密算法根据输入的消息 *P* 和密钥 K 生成密文 $C=[C_1,C_2,\cdots,C_N]$，即：

$$C=E_K(P) \tag{3-1}$$

接收方通过解密算法根据输入的密文 C 和密钥 K 恢复明文 $P=[P_1,P_2,\cdots,P_M]$，即：

$$P=D_K(C) \tag{3-2}$$

一个攻击者（密码分析者）能够基于不安全的公开信道观察密文 C，但不能接触到明文 P 或密钥 K，他可以试图恢复明文 P 或密钥 K。假定他知道加密算法 E 和解密算法 D，只对当前这个特定的消息感兴趣，则努力的焦点是通过产生一个明文的估计值 P' 来恢复明文 P。如果他也对读取未来的消息感兴趣，他就需要试图通过产生一个密钥的估计值 K' 来恢复密钥 K，这是一个密码分析的过程。

单钥密码体制的安全性主要取决于两个因素：①加密算法必须足够安全，使得不必为算法保密，仅根据密文就能破译出消息是不可行的；②密钥的安全性，密钥必须保密并保证有足够大的密钥空间，单钥密码体制要求基于密文和加密/解密算法的知识能破译出消息的做法是不可行的。

单钥密码算法的优点主要体现在其加密、解密处理速度快、保密度高等，其缺点主要体现在以下几个方面。

1）密钥是保密通信安全的关键，发信方必须安全、妥善地把密钥护送到收信方，不能泄露其内容。如何才能把密钥安全地送到收信方，是单钥密码算法的突出问题。单钥密码算法的密钥分发过程十分复杂，所花代价高。

2）多人通信时密钥组合的数量会出现爆炸性膨胀，使密钥分发更加复杂化，N 个人进行两两通信，总共需要的密钥数为 N(N−1)/2 个。

3）通信双方必须统一密钥，才能发送保密的信息。如果发信者与收信人素不相识，这就无法向对方发送秘密信息了。

4）除了密钥管理与分发问题，单钥密码算法还存在数字签名困难问题（通信双方拥有同样的消息，接收方可以伪造签名，发送方也可以否认发送过某消息）。

2．双钥密码体制

双钥体制是由 Diffie 和 Hellman 于 1976 年提出的，采用双钥密码体制（又称为公钥密码体制或非对称密码体制）的主要特点是将加密和解密能力分开，因而可以实现多个用户加密的消息只能由一个用户解读，或只能由一个用户加密消息而使多个用户可以解读。

双钥密码体制的原理是加密密钥与解密密钥不同，而且从一个难以推出另一个。两个密钥形成一个密钥对，用其中一个密钥加密的结果，可以用另一个密钥来解密。双钥密码体制的发展是整个密码学发展史上最伟大的一次革命，它与以前的密码体制完全不同。这是因为双钥密码算法基于数学问题求解的困难性，而不再是基于代替和换位方法；另外，双钥密码体制是非对称的，它使用两个独立的密钥，一个可以公开，称为公钥，另一个不能公开，称为私钥。

双钥密码体制的产生主要基于以下两个原因：一是为了解决常规密钥密码体制的密钥管理与分配的问题；二是为了满足对数字签名的需求。因此，双钥密码体制在消息的保密性、密钥分配和认证领域有着重要的意义。

在双钥密码体制中，公开密钥是可以公开的信息，而私有密钥是需要保密的。加密算法 E 和解密算法 D 也都是公开的。用公开密钥对明文加密后，仅能用与之对应的私有密钥解密才能恢复出明文，反之亦然。

在使用双钥体制时，每个用户都有一对选定的密钥：一个是可以公开的，用 k_1 表示，另一个则是秘密的，用 k_2 表示，公开的密钥 k_1 可以像电话号码一样进行注册公布，因此双钥体制又称为公钥体制（Public Key System）。双钥密码体制既可用于实现公共通信网的保密通信，也可用于认证系统中对消息进行数字签名。为了同时实现保密性和对消息进行确认，且加密、解密运算次序可换，即 $E_{k1}(D_{k2}(m)) = D_{k2}(E_{k1}(m)) = m$ 时，可采用双钥密码体制实现双重加、解密功能，如图 3-3 所示。例如，用户 A 要向用户 B 传送具有认证性的机密消息 m，可按图 3-3 的顺序进行变换。这样，A 发送给 B 的密文为 $c = E_{kB1}(D_{kA2}(m))$，B 恢复明文的运算过程如下。

$$m = E_{kA1}(D_{kB2}(c)) = E_{kA1}(D_{kB2}(E_{kB1}(D_{kA2}(m)))) = E_{kA1}(D_{kA2}(m))。$$

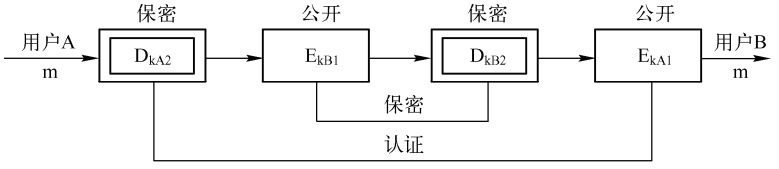


图 3-3　双钥保密和认证体制示意图

双钥密码体制的优点是可以公开加密密钥，适应网络的开放性要求，且仅需保密解密密钥，所以密钥管理问题比较简单。此外，双钥密码可以用于数字签名等新功能。最有名的双钥密码体系是 1977 年由 Rivest、Shamir 和 Adleman 等人提出的 RSA 密码体制。双钥密码的缺点是双钥密码算法一般比较复杂，加解密速度慢。因此，实际网络中的加密多采用双钥和单钥密码相结合的混合加密体制，即加解密时采用单钥密码，密钥传送时则采用双钥密码。这样既

解决了密钥管理的困难问题，又解决了加解密速度的问题。

3.2 加密算法

加密算法就其发展而言，共经历了古典密码、对称密钥密码（单钥密码体制）和公开密钥密码（双钥密码体制）3 个发展阶段。其中，古典密码是基于字符替换的密码，现在已很少使用，但其代表了密码的起源，仍在使用的有对位进行变换的密码算法。按密钥管理方式来区分，上述加密算法可以分为两大类，即对称密钥算法与公开密钥算法。这里，对称密钥算法的加密和解密密钥相同，也称单钥算法。按加密模式来分，对称算法还可分为序列密码和分组密码两大类。序列密码每次加密一位或一字节的明文，也称为流密码，序列密码是手工和机械密码时代的主流方式；分组密码将明文分成固定长度的组，用同一密钥和算法对每一块加密，输出也是固定长度的密文。公开密钥算法也称双钥加密算法，它使用完全不同但又是完全匹配的一对钥匙——公钥和私钥；在公开密钥算法加密文件时，只有使用匹配的一对公钥和私钥，才能完成对明文的加密和解密过程。

此外，随着云计算、电子商务等迅速发展，近年来，人们越来越重视同态加密的研究与应用。

3.2.1 古典密码算法

古典密码大都比较简单，可用手工或机械操作实现加解密，虽然现在很少采用，但研究这些密码算法的原理，对于理解、构造和分析现代密码是十分有益的。古典密码算法主要有代码加密、代替加密、变位加密和一次性密码簿加密等几种算法。代码加密是一种比较简单的加密方法，它使用通信双方预先设定的一组有确切含义的代码，如日常词汇、专有名词或特殊用语等来发送消息，一般只能用于传送一组预先约定的消息。代替加密是将明文中的每个字母或每组字母替换成另一个或一组字母，这种方法可用来传送任何信息，但安全性不及代码加密。变位加密不隐藏明文的字符，即明文的字母保持相同，但其顺序被打乱重新排列成另一种不同的格式，由于密文字符与明文字符相同，密文中字母的出现频率与明文中字母的出现频率相同，密码分析者可以很容易地由此进行判别。虽然许多现代密码也使用换位，但由于它对存储要求很大，有时还要求消息为某个特定的长度，因而比较少用。一次性密码簿加密具有代码加密的可靠性，又保持了代替加密的灵活性，密码簿的每一页都是不同的代码表，可用一页上的代码来加密一些词，用后销毁，再用另一页加密另一些词，直到全部明文完成加密。破译的唯一方法就是获取一份相同的密码簿。该方法可操作性不强，因此也很少使用。下面，介绍代替加密的几种算法实现。

1．简单代替密码或单字母密码

简单代替密码就是将明文字母表 M 中的每个字母用密文字母表 C 中的相应字母来代替。这一类密码包括移位密码、替换密码、仿射密码、乘数密码、多项式代替密码和密钥短语密码等。

1）移位密码是最简单的一类代替密码，将字母表的字母右移 k 个位置，并对字母表长度做模运算，其形式为：$e_k(m)=(k+m)=c \bmod q$，解密变换为：$d_k(c)=(c-k)=m \bmod q$。其中，q 为字母表 M 的长度，m 既代表字母表 *M* 中的位置，也代表该字母在 M 中的位置。c 既代表字母表 C 中的位置，也代表该字母在 C 中的位置。凯撒（Caesar）密码是对英文 26 个字母进行移位代替的密码，其 q=26。这种密码之所以称为凯撒密码，是因为凯撒使用过 k=3 的这种密码。使用凯撒密码，若明文为：

M=Caesar cipher is a shift substitution

则密文为：

C=Fdvhvdu flskhu lv d vkliw vxevwlwxwlrq。

2）在替换密码中，可对明文字母表进行 q 个字符的所有可能置换得到密文字母表。移位密码是替换密码算法的一个特例。

3）乘数密码也是一种替换密码，它将每个字母乘以一个密钥 k，即 $e_k(m)=km \bmod q$，其中，k 和 q 互素，这样字母表中的字母会产生一个复杂的剩余集合；若 k 和 q 不互素，则会有一些明文字母被加密成相同的密文字母，且不是所有的字母都会出现在密文字母表中。

4）替换密码的另一个特例就是仿射密码，其加密的形式为 $e_k(m)=(k_1m+k_2)=c \bmod q$，其中，$k_1$ 和 q 互素。

简单代替密码由于使用从明文到密文的单一映射，所以明文字母的单字母出现频率分布与密文中相同，可以很容易地通过使用字母频率分析法进行唯密文攻击。

2．多名或同音代替

该方法与简单代替密码类似，区别在于映射为一对多关系，每个明文字母可以加密成多个密文字母。同音代替密码比简单代替密码更难破译，尤其是当对字母的赋值个数与字母出现频率成比例时，这是因为密文符号的相关分布会近似于平的，可以挫败频率分析。若明文字母的其他统计信息在密文中仍很明显，同音代替密码仍然是可破译的。

3．多表代替

由于单字母出现的频率分布与密文中相同，因此多表代替密码使用从明文字母到密文字母的多个映射来隐藏单字母出现的频率分布，每个映射是简单代替密码中的一对一映射。

维吉尼亚（Vigenere）密码和博福特（Beaufort）密码均是多表代替密码的实例。多表代替密码有多个单字母密钥，每一个密钥被用来加密一个明文字母。第一个密钥加密明文的第一个字母，第二个密钥加密明文的第二个字母……所有密钥用完后，密钥再循环使用。维吉尼亚密码是 1858 年法国密码学家 Blaise de Vegenere 所发明，其算法可简述为：设密钥为 k，明文为 m，加密为 c，则有加密变换 $e_k(m)=c_1c_2\cdots c_n$，其中，$c_i= m_i+k_i \bmod q$。密钥 k 可以通过周期性地延长，反复进行以至无穷。博福特密码是按 mod q 减法运算的一种周期代替密码，它的加密变换与维吉尼亚密码类似，只是密文字母表为英文字母表（若 q=26）逆序排列进行循环右移 k_i+1 次而成。

4．多字母或多码代替

不同于前面介绍的代替密码都是每次加密一个明文字母，多字母代替密码将明文字符划分为长度相同的消息单元，称为明文组，对字符块成组进行代替，这样一来使密码分析更加困难。多字母代替的优点是容易将字母的自然频度隐蔽或均匀化，从而有利于抗击统计分析。Playfair 密码、Hill 密码等都是这一类型的密码。

3.2.2 单钥加密算法

单钥密钥体制的加密密钥与解密密钥相同或等价，其加密模式主要有序列密码（也称流密码）和分组密码两种方式。流密码（Stream Cipher）是将明文划分成字符（如单个字母）或其编码的基本单元（如 0、1 数字），字符分别与密钥流作用进行加密，解密时以同步产生的同样的密钥流解密。流密码的强度完全依赖于密钥流序列的随机性和不可预测性，其核心问题是密钥流生成器的设计，流密码主要应用于政府和军事等要害部门。根据密钥流是否依赖于明文流，可将流密码分为同步流密码和自同步流密码，目前，同步流密码较为多见。由于自同步流密码系统一般需要密文反馈，因而使得分析工作复杂化，但其具有抵抗密文搜索攻击和认证功

能等优点，所以这种流密码也是值得关注的方式。流密码的设计方法有信息论方法、系统论方法、复杂性理论方法及随机化方法等。

分组密码（Block Cipher）是将明文消息编码表示后的数字序列 $x_1, x_2, \cdots, x_i, \cdots$，划分为长为 m 的组 $x=(x_0, x_1, \cdots, x_{m-1})$，各组（长为 m 的矢量）分别在密钥 $k=(k_0, k_1, \cdots, k_{l-1})$控制下变换成等长的输出数字序列 $y=(y_0, y_1, \cdots, y_{n-1})$（长为 n 的矢量），其加密函数 E：$V_n \times K \rightarrow V_n$，$V_n$ 是 n 维矢量空间，K 为密钥空间，如图 3-4 所示。在相同密钥条件下，分组密码对长为 m 的输入明文组所实施的变换是等同的，所以只需关注对任一组明文数字的变换规则。这种密码实质上是字长为 m 的数字序列的代替密码。通常取 $n = m$，若 $n > m$，则为有数据扩展的分组密码；若 $n < m$，则为有数据压缩的分组密码。

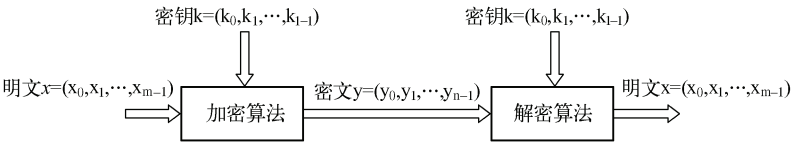


图 3-4　分组密码原理框图

围绕单钥密钥体制，密码学工作者已经开发了众多行之有效的单钥加密算法，并且对基于这些算法的软硬件实现进行了大量的工作，下面介绍其中的典型代表算法 DES 和 IDEA。

1．数据加密标准 DES

DES 即数据加密标准（Data Encryption Standard），它于 1977 年由美国国家标准局公布，是 IBM 公司研制的一种对二元数据进行加密的分组密码，数据分组长度为 64bit（8B），密文分组长度也是 64bit，没有数据扩展。密钥长度为 64bit，其中有效密钥长度为 56bit，其余 8bit 为奇偶校验。DES 的整个体制是公开的，系统的安全性主要依赖于密钥的保密，其算法主要由初始置换 IP、16 轮迭代的乘积变换、逆初始置换 IP^{-1}，以及 16 个子密钥产生器构成，如图 3-5 所示。

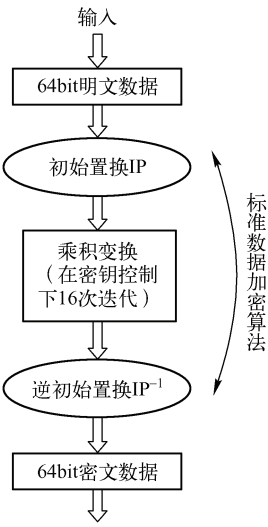


图 3-5　DES 算法框图

下面介绍各个组成部分的功能。设明文 m 是 0 和 1 组成的长度为 64bit 的符号串，$\tilde{m}$ 为经初始置换的置换码组，密钥 k 也为 64bit 长度的 0、1 字符串。令 $m=m_1m_2\cdots m_{64}$，$k=k_1k_2\cdots k_{64}$，其中 $m_i, k_i=0$ 或 1，$i=1, 2, \cdots, 64$。这里，密钥 k 中第 8、16、24、32、40、48、56、64 共 8 位是奇偶校验位，在算法中不起作用。DES 的加密过程可表示为：

$$DES(m) = IP^{-1} \cdot T_{16} \cdot T_{15} \cdots T_2 \cdot T_1 \cdot IP(m)。$$

（1）初始置换 IP 及其逆初始置换 IP^{-1}

初始置换 IP 是将 64bit 明文的位置进行置换，得到一个乱序的 64bit 明文组，而后分为左右两个 32bit 的分段，以 L_0 和 R_0 表示，为随后进行的乘积变换做准备。逆初始置换 IP^{-1} 是将 16 轮迭代后给出的 64bit 组进行置换，得到输出的密文组。初始置换和逆初始置换在密码意义中作用不大，它们主要用于打乱输入明文码字的划分关系，并将分布在明文不同位置的 8 位校验位作为初始置换输出的一个字节。

如图 3-6 所示，64bit 下标序号依次为 1～64 的明文输入，经过初始置换后，其下标依次

为 58，50，…，15，7，即 $m \to IP \to \tilde{m}$ 置换后，$\tilde{m}_1 = m_{58}$，$\tilde{m}_2 = m_{50}, \cdots$，$\tilde{m}_{64} = m_7$，$\tilde{m} = m_{58} m_{50} m_{42} \cdots m_{23} m_{15} m_7$。对于逆置换 IP^{-1} 来说，满足性质 $IP \cdot IP^{-1} = IP^{-1} \cdot IP = I$，经过 $\tilde{m} \to IP^{-1} \to m$ 置换后，有 $m = \tilde{m}_{40} \tilde{m}_8 \tilde{m}_{48} \cdots \tilde{m}_{17} \tilde{m}_{57} \tilde{m}_{25}$。

IP:

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}:

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

图 3-6　初始置换和逆初始置换

（2）乘积变换

乘积变换是 DES 算法的核心部分，主要完成 DES 的迭代运算过程，它将经过 IP 置换后的数据分成 32bit 的左右两组，在迭代过程中左右交换位置。每次迭代时只对右边的 32bit 进行一系列的加密变换，在此轮迭代快结束时，将左边的 32bit 与右边得到的 32bit 逐位模 2 运算，作为下一轮迭代时右边的分段，并将原来右边未经变换的段直接送到左边的寄存器中作为下一轮迭代时左边的段，如图 3-7 所示。

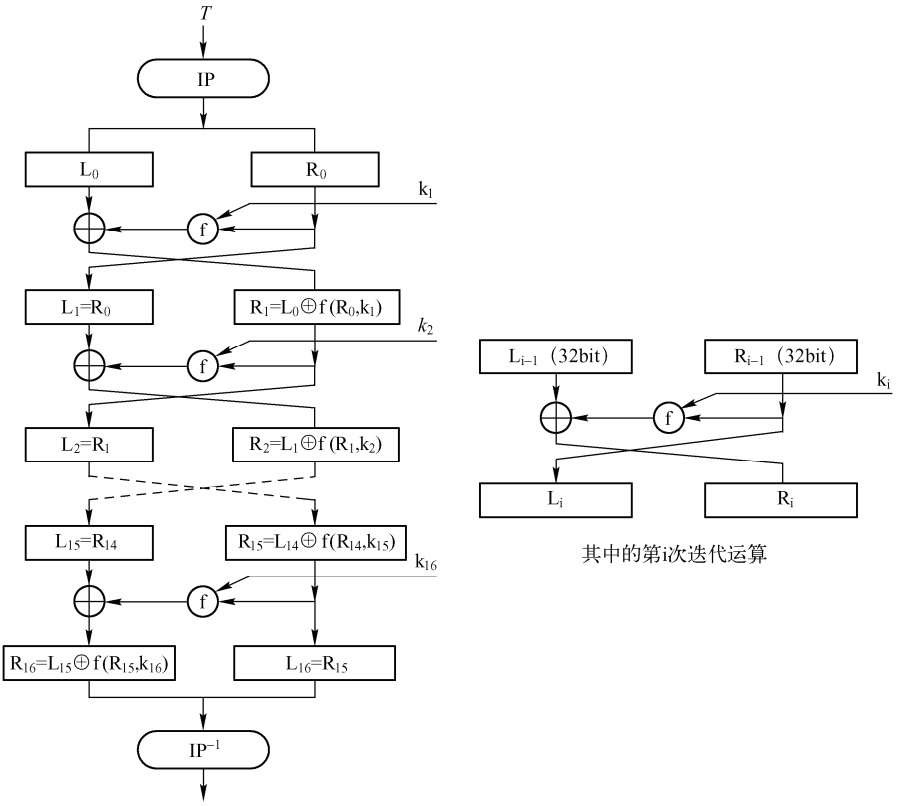
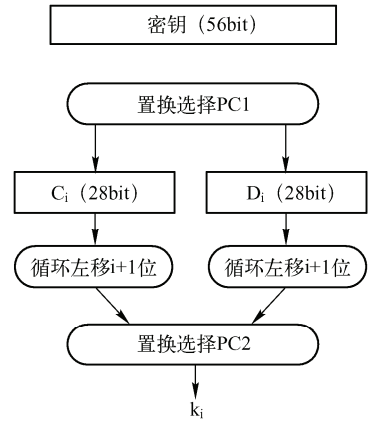


图 3-7　DES 迭代过程

图 3-7 的右侧为 DES 第 i 次迭代运算的操作，这里 i=1，2，…，16，L_{i-1} 和 R_{i-1} 分别为第 i-1 次迭代结果的左右两个部分，均为 32bit。易知 $L_i=R_{i-1}$，$R_i=L_{i-1}\oplus f(R_{i-1}, k_i)$，$L_0$ 和 R_0 是输入明文经过初始置换 IP 后的运算结果，$\oplus$ 是按位模 2 相加运算符。k_i 是由 64bit 密钥产生的子密钥，其长度为 48bit，子密钥的产生过程如图 3-8 所示，它将 64bit 初始密钥经过置换选择 PC1、循环移位置换、置换选择 PC2 得到迭代加密用的子密钥 k_i。具体过程为：将 64bit 中的 56 位有效密钥位送入置换选择 PC1、经过坐标置换后分成两组，每级为 28bit，分别送入 C 寄存器和 D 寄存器中，在每次迭代运算中，C 和 D 寄存器分别将所存数据进行左循环移位置换，置换选择 PC2 将 C 寄存器中第 9、18、22、25 位和 D 寄存器中第 7、9、15、26 位删去，并将其余数字置换位置后送出 48bit 数字作为第 i 次迭代时所用的子密钥 k_i，置换选择 PC1、PC2，以及左循环移位置换的次数均如图 3-8 所示。



PC1

57	49	41	33	25	17	9		14	17	11	24	1	5
1	58	50	42	34	26	18		3	28	15	6	21	10
10	2	59	51	43	35	27		23	19	12	4	26	8
19	11	3	60	52	44	36		16	7	27	20	13	2
63	55	47	39	31	23	15		41	52	31	37	47	55
7	62	54	46	38	30	22		30	40	51	45	33	48
14	6	61	53	45	37	29		44	49	39	56	34	53
21	13	5	28	20	12	4		46	42	50	36	29	52

PC2

左移位次数

迭代顺序	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
左移位数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

图 3-8　DES 迭代过程子密钥的产生及置换选择和左移位次数

（3）选择扩展运算、选择压缩运算和置换运算

由图 3-7 可知，DES 的关键在于 $f(R_{i-1}, k_i)$的功能，f 是将 32bit 的输入转化为 32bit 的输出，其中需要进行选择扩展运算 E、密钥加密运算和选择压缩运算 S，以及置换运算 P，具体转化过程如图 3-9 所示。

选择扩展运算 E 是将输入的 32bit R_{i-1} 扩展成 48bit 的输出。选择压缩运算 S 是将密钥加密运算得到的 48bit 数据自左至右分成 8 组，每组 6 个 bit，而后并行送入 8 个 S 盒中，每个 S 盒为一非线性代换网络，有 4 个输出。这样，8 个 S 盒输出的 32bit 数据可以进行坐标置换运算 P。这几种运算作为 DES 加密过程的重要组成部分涉及的计算比较复杂，其详细说明可参阅专业论著。

（4）DES 安全性分析及其变形

DES 的出现是密码学上的一个创举，由于其公开了密码体制及其设计细节，因此其安全性完全依赖于其所用的密钥，关于 DES 的安全问题，学术界有过激烈的争论，普遍的印象是密钥仅有 56bit 有点偏短。Diffie 和 Hellman 曾设想花千万美元来制造一台专用机，希望一天内找到 DES 的一个密钥，其基本思想是穷举，即强行攻击。此外，1990 年 Eli Biham 和 Adi Shamir 提出用“微分分析法”对 DES 进行攻击，但其也只有理论上的价值。后来，有人提出一种明文攻击法——“线性逼近法”，它需要 $2^{43}=4.398\times10^{12}$ 对明文-密文对，在这样强的要求条件下，要 10 多台工作站协同工作数天才能完成攻击。总之，随着各种针对 DES 新攻击手法

的不断出现，DES 已感觉到面临的实际威胁。尽管如此，自 DES 正式成为美国标准以来，已有许多公司设计并推广了实现 DES 算法的产品，有的设计专用 LSI 器件或芯片，有的用现成微处理器实现，有的只限于实现 DES 算法，有的则可运行各种工作模式。

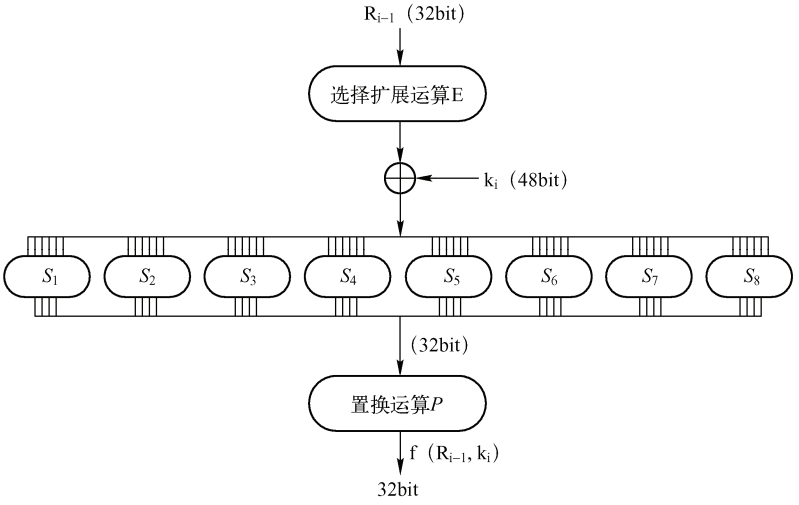


图 3-9　DES 的 $f(R_{i-1},k_i)$ 转化过程

为了解决 DES 存在的安全问题，同时也为了适应不同情况的需求，人们设计了多种应用 DES 的方式，即 DES 变形，主要有独立子密钥方式、DESX、CRYPT（3）、S 盒可变的 DES、RDES、S^nDES_i、$xDES_i$，以及 GDES 等，这里不再赘述。

2．国际数据加密算法 IDEA

近年来新的分组加密算法不断出现，IDEA 就是其中的杰出代表。IDEA 是 International Data Encryption Algorithm 的缩写，即国际数据加密算法。它是根据中国学者朱学嘉博士与著名密码学家 James Massey 于 1990 年联合提出的建议标准算法 PES（Proposed Encryption Standard）改进而来的。它的明文与密文块都是 64bit，密钥长度为 128bit，作为单钥体制的密码，其加密与解密过程相似，只是密钥存在差异，IDEA 无论是采用软件还是硬件实现都比较容易，而且加解密的速度很快。IDEA 算法的加密过程如图 3-10 所示。

64bit 的数据块分成 4 个子块，每一子块为 16bit，令这 4 个子块为 X_1、X_2、X_3 和 X_4，作为迭代第 1 轮的输入，全部共 8 轮迭代运算。每轮迭代都是 4 个子块彼此间以及 16bit 的子密钥进行异或，$\mathrm{mod}\,2^{16}$ 做加法运算，$\mathrm{mod}(2^{16}+1)$ 做乘法运算。任何一轮迭代第 2 和第 3 子块互换，每一轮迭代运算步骤如下。

1）X_1 和第 1 个子密钥块做乘法运算。

2）X_2 和第 2 个子密钥块做加法运算。

3）X_3 和第 3 个子密钥块做加法运算。

4）X_4 和第 4 个子密钥块做乘法运算。

5）1）和 3）的结果做异或运算。

6）2）和 4）的结果做异或运算。

7）5）的结果与第 5 个子密钥块做乘法运算。

8）6）和 7）的结果做加法运算。

9）8）的结果与第 6 个子密钥块做乘法运算。

10）7）和 9）的结果做加法运算。

11）1）和 9）的结果做异或运算。

12）3）和 9）的结果做异或运算。

13）2）和 10）的结果做异或运算。

14）4）和 10）的结果做异或运算。

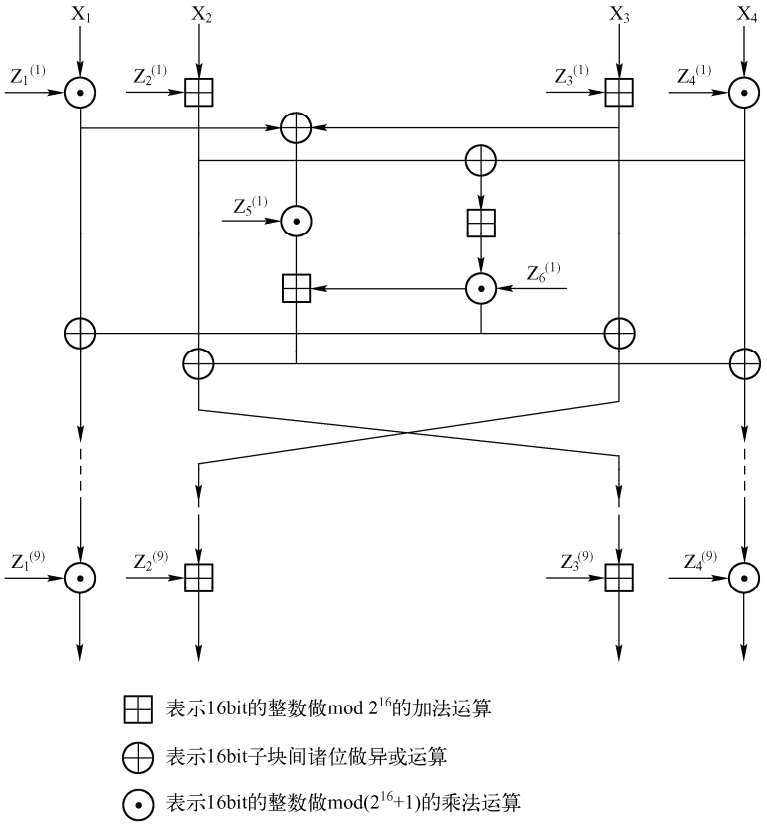


图 3-10　IDEA 加密算法原理框图

结果输出为 11）、13）、12）、14），除最后一轮外，第 2 和第 3 块交换。第 8 轮结束后，最后输出变换如下。

1）X_1 和第 1 个子密钥块做乘法运算。

2）X_2 和第 2 个子密钥块做加法运算。

3）X_3 和第 3 个子密钥块做加法运算。

4）X_4 和第 4 个子密钥块做乘法运算。

子密钥块的产生过程也比较简单。子密钥块每轮输出 6 个，最后输出变换 4 个，共 52 个。首先将 128bit 的密钥分成 8 个子密钥，每个子密钥 16bit。这 8 个子密钥正好是第 1 轮的 6 个及第 2 轮的前两个。再将密钥左旋转 25bit，再将它分成 8 个子密钥。前 4 个是第 2 轮的子密钥，后 4 个是第 3 轮的子密钥。将密钥再向左旋转 25bit，产生后 8 个子密钥。以此类

推，直至算法结束。

解密密钥和加密密钥的对应关系如下所示。

轮次	加密子密钥块	解密子密钥块
1	$Z_1^{(1)}Z_2^{(1)}Z_3^{(1)}Z_4^{(1)}Z_5^{(1)}Z_6^{(1)}$	$(Z_1^{(9)})^{-1}-Z_2^{(9)}-Z_3^{(9)}(Z_4^{(9)})^{-1}Z_5^{(8)}Z_6^{(8)}$
2	$Z_1^{(2)}Z_2^{(2)}Z_3^{(2)}Z_4^{(2)}Z_5^{(2)}Z_6^{(2)}$	$(Z_1^{(8)})^{-1}-Z_2^{(8)}-Z_3^{(8)}(Z_4^{(8)})^{-1}Z_5^{(7)}Z_6^{(7)}$
3	$Z_1^{(3)}Z_2^{(3)}Z_3^{(3)}Z_4^{(3)}Z_5^{(3)}Z_6^{(3)}$	$(Z_1^{(7)})^{-1}-Z_2^{(7)}-Z_3^{(7)}(Z_4^{(7)})^{-1}Z_5^{(6)}Z_6^{(6)}$
4	$Z_1^{(4)}Z_2^{(4)}Z_3^{(4)}Z_4^{(4)}Z_5^{(4)}Z_6^{(4)}$	$(Z_1^{(6)})^{-1}-Z_2^{(6)}-Z_3^{(6)}(Z_4^{(6)})^{-1}Z_5^{(5)}Z_6^{(5)}$
5	$Z_1^{(5)}Z_2^{(5)}Z_3^{(5)}Z_4^{(5)}Z_5^{(5)}Z_6^{(5)}$	$(Z_1^{(5)})^{-1}-Z_2^{(5)}-Z_3^{(5)}(Z_4^{(5)})^{-1}Z_5^{(4)}Z_6^{(4)}$
6	$Z_1^{(6)}Z_2^{(6)}Z_3^{(6)}Z_4^{(6)}Z_5^{(6)}Z_6^{(6)}$	$(Z_1^{(4)})^{-1}-Z_2^{(4)}-Z_3^{(4)}(Z_4^{(4)})^{-1}Z_5^{(3)}Z_6^{(3)}$
7	$Z_1^{(7)}Z_2^{(7)}Z_3^{(7)}Z_4^{(7)}Z_5^{(7)}Z_6^{(7)}$	$(Z_1^{(3)})^{-1}-Z_2^{(3)}-Z_3^{(3)}(Z_4^{(3)})^{-1}Z_5^{(2)}Z_6^{(2)}$
8	$Z_1^{(8)}Z_2^{(8)}Z_3^{(8)}Z_4^{(8)}Z_5^{(8)}Z_6^{(8)}$	$(Z_1^{(2)})^{-1}-Z_2^{(2)}-Z_3^{(2)}(Z_4^{(2)})^{-1}Z_5^{(1)}Z_6^{(1)}$
输出变换	$Z_1^{(9)}Z_2^{(9)}Z_3^{(9)}Z_4^{(9)}$	$(Z_1^{(1)})^{-1}-Z_2^{(1)}-Z_3^{(1)}(Z_4^{(1)})^{-1}$

这里 Z^{-1} 表示 Z mod（$2^{16}+1$）乘法的逆，即 $Z\odot Z^{-1}=1$。$-Z$ 表示 Z mod 2^{16} 加法运算的逆，即 $Z\oplus(-Z)=0$。

IDEA 的密钥长为 128bit，若采用穷搜索进行破译，则需要进行 $2^{128}=34028\times10^{38}$ 次尝试，这将是用同样方法对付 DES 的 $2^{72}=4.7\times10^{21}$ 倍工作量，有关学者进行分析表明 IDEA 对于线性和差分攻击是安全的。此外，将 IDEA 的字长由 16bit 加长为 32bit，密钥相应长为 256bit，采用 2^{32} 模加，$2^{32}+1$ 模乘，可进一步强化 IDEA 的安全性能。

3．单钥算法性能分析

前面重点介绍了单钥密码体制的典型代表 DES 和 IDEA 算法，类似的算法还有 SAFER K-64（Secure And Fast Encryption Routine）、GOST、RC-4、RC-5、Blowfish 和 CAST-128 等。为了提高单钥密码的安全性，人们还将分组密码算法通过组合以得到新的分组密码算法，但这种组合密码的安全性必须经仔细检验后才能付诸实用，如二重 DES 加密、三重 DES 加密等。

各种加密算法的具体实现互不相同，其性能也存在较大差异，表 3-1 对单钥密码体制的主要算法在总体实现、速度、安全性能和改进措施等方面进行了比较，并基于比较结果给出了各算法合适的应用场合。

表 3-1　单钥算法性能比较表

名　称	实现方式	运算速度	安　全　性	改进措施	应用场合
DES	40～56bit 密钥	一般	完全依赖于密钥，易受穷举攻击	双重、三重 DES，AES	适用于硬件实现
IDEA	128bit 密钥、8 轮迭代	较慢	军事级，可抗差值分析和相关分析，没有 DES 意义下的弱密钥	加长字长为 32bit、密钥为 256bit，采用 2^{32} 模加、$2^{32}+1$ 模乘	适用于 ASIC 设计
GOST	256bit 密钥、32 轮迭代	较快	军事级	以长密钥 S 盒代换盒、加大迭代轮数	S 盒可随机秘密选择，便于软件实现
Blowfish	256～448bit 密钥、16 轮迭代	最快	军事级、可通过改变密钥长度调整安全性	—	适合固定密钥场合，不适合常换密钥场合和智能卡
RC4	密钥长度可变	快 DES 10 倍	对差分攻击和线性攻击具免疫能力，无短循环且具有高度非线性	密钥长度放宽到 64bit	算法简单，易于编程实现

（续）

名　称	实现方式	运算速度	安全性	改进措施	应用场合
RC5	密钥长度和迭代轮数均可变	速度可根据3个参数的取值进行选择	6轮以上时即可抗线性攻击，通过调整字长、密钥长度和迭代轮数可以在安全性和速度上取得折中	引入数据相倚旋转	适用于不同字长的微处理器
CAST128	密钥长度可变、16轮迭代	较快	强度取决于S盒、抗线性和差分攻击，具有SAC和BIC，没有弱密钥和半弱密钥等特性	增加密钥长、形成CAST256	适用于PC和UNIX工作站

3.2.3　双钥加密算法

双钥密码体制的加密密钥和解密密钥不相同，它们的值不等，属性也不同，一个是可公开的公钥，另一个则是需要保密的私钥。双钥密码体制的特点是加密能力和解密能力是分开的，即加密与解密的密钥不同，很难由一个推出另一个。其应用模式有两种，一是多个用户用公钥加密的消息可由一个用户用私钥解读，二是一个用户用私钥加密的消息可被多个用户用公钥解读。对于前者，可用于在公共网络中实现保密通信，后者则可用于认证系统对消息进行数字签名。

双钥密码体制大大简化了复杂的密钥分配管理问题，但公钥算法要比私钥算法慢得多。因此，在实际通信中，双钥密码体制主要用于认证（如数字签名、身份识别）和密钥管理等，而消息加密仍采用私钥密码体制。下面先介绍双钥密码体制的杰出代表RSA加密算法。

1．RSA算法

RSA体制是由R. L. Rivest、A. Shamir和L. Adleman共同提出的，它既可用于加密，也可用于数字签名。国际标准化组织ISO、ITU及SWIFT等均已接受RSA体制作为标准。在Internet中所采用的PGP（Pretty Good Privacy）也将RSA作为传送会话密钥和数字签名的标准算法。RSA算法的安全性建立在数论中“大数分解和素数检测”的理论基础上，能够抵抗到目前为止已知的绝大多数密码攻击。

（1）大数分解

双钥密码体制算法按由公钥推算出密钥的途径可分为两类：一类是基于素数因子分解问题（如RSA算法），其安全性基于100位十进制数以上的所谓“大数”的素数因子分解难题，这是一个至今尚无有效快速算法的数学难题；另一类是基于离散对数问题（如ElGamal算法），其安全性基于计算离散对数的困难性，离散对数问题是指模指数运算的逆问题，即找出一个数的离散对数。一般地，计算离散对数是非常困难的。

（2）RSA算法表述

假定用户A要传送消息m给用户B，则RSA算法的加/解密过程如下。

1）首先用户B产生两个大素数p和q（p、q是保密的）。

2）B计算$n=pq$和$\varphi(n)=(p-1)(q-1)$（$\varphi(n)$是保密的）。

3）B选择一个随机数e（$0<e<\varphi(n)$），使得$(e,\varphi(n))=1$，即e和φ互素。

4）B通过计算得出d，使得$de \bmod \varphi(n)\equiv 1$（即在与n互素的数中选取与φ(n)互素的数，可以通过Euclidean算法得出。d是B自留且保密的，用做解密密钥）。

5）B将n及e作为公钥公开。

6）用户A通过公开渠道查到n和e。

7）对m施行加密变换，即$E_B(m)=m^e \bmod n=c$。

8）用户 B 收到密文 c 后，施行解密变换。

$$D_B(c) = c^d \bmod n = (m^e \bmod n)^d \bmod n = m^{ed} \bmod n = m \bmod n \text{ 。}$$

下面举一个简单的实例来说明这个过程：令 26 个英文字母对应于 0～25 的整数，即 a→00，b→01，…，y→24，z→25。设 m = public，则 m 的十进制数编码为：m = 15 20 01 11 08 02。设 n = 3×11 =33，p =3，q =11，φ(n) = 2×10 = 20。取 e =3，则 d =7。B 将 n = 33 和 e = 3 公开，保留 d = 7。

A 查到 n 和 e 后，将消息 m 加密。

$E_B(p) = 15^3 = 9 \bmod 33$，

$E_B(u) = 20^3 = 14 \bmod 33$，

$E_B(b) = 1^3 = 1 \bmod 33$，

$E_B(l) = 11^3 = 11 \bmod 33$，

$E_B(i) = 8^3 = 17 \bmod 33$，

$E_B(c) = 2^3 = 8 \bmod 33$，

则 $c = E_B(m) = 09\ 14\ 01\ 11\ 17\ 08$，它对应的密文为 c =joblri。

当 B 接到密文 c 后施行解密变换。

$D_B(j) = 09^7 = 15 \bmod 33$，即明文 p，

$D_B(o) = 14^7 = 20 \bmod 33$，即明文 u，

$D_B(b) = 01^7 = 01 \bmod 33$，即明文 b，

$D_B(l) = 11^7 = 11 \bmod 33$，即明文 l，

$D_B(r) = 17^7 = 08 \bmod 33$，即明文 i，

$D_B(i) = 08^7 = 02 \bmod 33$，即明文 c。

（3）RSA 安全性分析

在理论上，RSA 的安全性取决于模 n 分解的困难性，但数学上至今还未证明分解模就是攻击 RSA 的最佳方法，也未证明分解大整数就是 NP 问题。尽管如此，人们还是从消息破译、密钥空间选择等角度提出了针对 RSA 的其他攻击方法，如迭代攻击法、选择明文攻击法、公用模攻击、低加密指数攻击和定时攻击法等，但其攻击成功的概率微乎其微。有关 RSA 安全性的全面评述，可参阅 Kaliski 和 Robshaw 于 1995 年发表的论文 The secure use of RSA。

2．ElGamal 算法

RSA 算法是基于素数因子分解的双钥密码，ElGamal 算法则是基于离散对数问题的另一种类型的双钥密钥，它既可用于加密，也可用于签名。

（1）ElGamal 算法方案

令 z_p 是一个有 p 个元素的有限域，p 是素数，令 g 是 z_p^*（z_p 中除去 0 元素）中的一个本原元或生成元。明文集 m 为 z_p^*，密文集 e 为 $z_p^* \times z_p^*$。

公钥为：选定 p（$g < p$ 的生成元），计算公钥 $\beta \equiv g^a \bmod p$；

私钥为：$\alpha < p$。

（2）ElGamal 加解密及其安全性

选择随机数 $k \in z_{p-1}$，且 $(k, p-1) = 1$，计算：$y_1 = gk \bmod p$（随机数 k 被加密），$y_2 = M\beta^k \bmod p$，这里，M 是发送明文组。密文则由 y_1 和 y_2 级连构成，即密文 $C = y_1 \| y_2$。这种加密方式的特点是，密文由明文和所选随机数 k 来决定，因而是非确定性加密，一般称之

为随机化加密，对同一明文由于不同时刻的随机数 k 不同而给出不同的密文，这样做的代价是使数据扩展一倍。

在收到密文组 C 后，ElGamal 的解密是通过下列计算得到明文的。

$$M = \frac{y_2}{y_1^{\alpha}} = \frac{M\beta^k}{g^{k\alpha}} = \frac{Mg^{\alpha k}}{g^{k\alpha}} \bmod p \text{。}$$

例如，选 p=2579，g=2，$\alpha = 765$，计算出$\beta = g^{765} \bmod 2579 = 949$。若明文组为 M=1299，现在选择随机数 k=853，可算出$y_1 \equiv 2^{853} \bmod 2579 = 435$及$y_2 \equiv 1299 \times 949^{853} \bmod 2579 = 2396$。密文$C = (435, 2396)$。解密时由 C 可算出消息组$M = 2396/(435)^{765} \bmod 2579 = 1299$。

ElGamal 算法的安全性是基于z_p^*中有限群上的离散对数的困难性。研究表明，mod p 生成的离散对数密码可能存在陷门，这会造成有些“弱”素数 p 下的离散对数较容易求解，但密码学家也发现可以较容易地找到这类陷门，以免选用可能会产生脆弱性的这些素数。

3．双钥算法性能分析

双钥密钥体制因其密钥管理和分配较为简单，进而可以方便地用于数字签名和认证，尽管其算法都较为复杂、运算量大，但仍不失为一种非常有前途的加密体制，它的出现是密码学发展史上的划时代事件。前面分析了双钥密码体制的典型代表 RSA 和 ElGamal 算法，类似的算法还有 LUC 密码、Rabin 密码及 DSA 密码等。

对于 RSA 体制，可以将其推广为有多个密钥的双钥体制，即在多个密钥中选用一部分密钥作为加密密钥，而另一些作为解密密钥。同样地，RSA 还可以推广为多签名体制，例如有k_1、k_2和k_3共 3 个密钥，可将k_1作为 A 的签名私密钥，k_2作为 B 的签名私密钥，k_3作为公开的验证签名用密钥，实现这种多签名体制需要一个可信赖中心对 A 和 B 分配秘密签名密钥。近年来，人们还提出了一些新的双钥密钥体制，如隐含域方程和多项式同构等，但有的方案并没有达到其宣称的安全水平。

表 3-2 对双钥密码体制的主要算法在总体实现、速度、安全性能和改进措施等方面进行了比较，并基于比较结果给出了各算法合适的应用场合。

表 3-2　双钥算法性能比较表

算法名称	运算速度	安全性	改进措施	适用场合
RSA	很慢，RSA 最快时也比 DES 慢 100 倍	安全性完全依赖大数分解，产生密钥麻烦，n 至少要为 600bit 以上	改用 2048bit 长度的密钥	只用于少量数据加密
ElGamal	较慢	主要基于z_p^*中的有限群上的离散对数求解的困难性	将 ElGamal 方案推广到z_n^*上的单元群	适用于加密密钥，或单重或多重签名
LUC	较慢	由求 d 和 P 的难度决定，比 RSA 难破译	采用各种置换多项式取代指数运算	适用于少量数据加密场合
Rabin	最快	其安全性相当于分解大整数，在选择明文攻击下不安全	用M^3代替M^2，即 williams 体制	可用于签名系统
DSA	比 RSA 慢，有预计算时远快于 RSA	基于整数有限域离散对数难题，安全性与 RSA 接近	密钥加长到 512～1024 中可被 64 除尽的数	可用于数字签名中，以及电子邮件、电子转账等认证系统中

3.2.4　同态加密算法

随着互联网的发展和云计算概念的诞生，以及人们在密文搜索、电子投票、移动代码和多方计算等方面的需求日益增加，同态加密（Homomorphic Encryption）变得更加重要。同态

加密是一类具有特殊自然属性的加密方法，此概念是 Rivest 等人在 20 世纪 70 年代首先提出的，与一般加密算法相比，同态加密除了能实现基本的加密操作之外，还能实现密文间的多种计算功能，即先计算后解密可等价于先解密后计算。这个特性对于保护信息的安全具有重要意义，利用同态加密技术可以先对多个密文进行计算之后再解密，不必对每一个密文解密而花费高昂的计算代价；利用同态加密技术可以实现无密钥方对密文的计算，密文计算无须经过密钥方，既可以减少通信代价，又可以转移计算任务，由此可平衡各方的计算代价；利用同态加密技术可以实现让解密方只能获知最后的结果，而无法获得每一个密文的消息，可以提高信息的安全性。正是由于同态加密技术在计算复杂性、通信复杂性与安全性上的优势，越来越多的研究力量投入到其理论和应用的探索中。近年来，云计算受到广泛关注，而它在实现中遇到的问题之一即是如何保证数据的私密性，同态加密可以在一定程度上解决这个技术难题。

本质上，同态加密是指这样一种加密函数，对明文进行环上的加法和乘法运算再加密，与加密后对密文进行相应的运算，结果是等价的。由于这个良好的性质，人们可以委托第三方对数据进行处理而不泄露信息。具有同态性质的加密函数是指两个明文 a、b 满足 $Dec(En(a)\otimes En(b))=a\oplus b$ 的加密函数，其中 En 是加密运算，Dec 是解密运算，⊗、⊕分别对应明文和密文域上的运算。当⊕代表加法时，称该加密为加同态加密；当⊗代表乘法时，称该加密为乘同态加密。

全同态加密是指同时满足加同态和乘同态性质，可以进行任意多次加和乘运算的加密函数。用数学公式来表达，即 $Dec\ (f\ (En\ (m_1)，En(m_2)，\cdots，En(m_k)))=f\ (m_1，m_2，\cdots，m_k)$，或写成：$f\ (En(m_1)，En(m_2)，\cdots，En(m_k))=En\ (f\ (m_1，m_2，\cdots，m_k))$，如果 f 是任意函数，称为全同态加密。

直到 2009 年，IBM 的研究人员 Gentry 首次设计出一个真正的全同态加密体制，即可以在不解密的条件下对加密数据进行任何可以在明文上进行的运算，使得对加密信息仍能进行深入和无限的分析，而不会影响其保密性。经过这一突破，存储他人机密电子数据的服务提供商就能受用户委托来充分分析数据，不用频繁地与用户交互，也不必看到任何隐私数据。同态加密技术允许公司将敏感的信息储存在远程服务器里，既避免从当地的主机端发生泄密，又依然保证了信息的使用和搜索；用户也得以使用搜索引擎进行查询并获取结果，而不用担心搜索引擎会留下自己的查询记录。为提高全同态加密的效率，密码学界对其研究与探索仍在不断推进，这将使得全同态加密越来越向实用化靠近。

3.3 信息加密技术应用

在网络安全领域，网络数据加密是解决通信网中信息安全的有效方法。有关密码算法的知识已在本章前面内容中加以介绍，这里主要讨论通信网中对数据进行加密的应用方式。常见的网络数据加密应用主要有链路加密、结点加密、端到端加密和同态加密等。

3.3.1 链路加密

链路加密（又称在线加密）是对网络中两个相邻结点之间传输的数据进行加密保护，如图 3-11 所示。对于链路加密，所有消息在被传输之前进行加密，在每一个结点对接收到的消息进行解密后，先使用下一个链路的密钥对消息进行加密，再进行传输。在到达目的地之前，

一条消息可能要经过多条通信链路的传输。

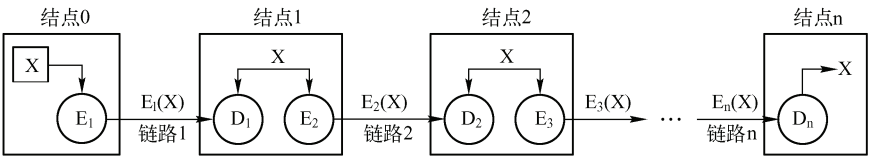


图 3-11　链路加密

由于在每一个中间传输结点消息均被解密后重新进行加密，因此包括路由信息在内的链路上的所有数据均以密文形式出现。这样，链路加密就掩盖了被传输消息的源点与终点。由于填充技术的使用，以及填充字符在不需要传输数据的情况下就可以进行加密，使得消息的频率和长度特性得以掩盖，从而可以防止对通信业务进行分析。

尽管链路加密在计算机网络环境中广泛使用，但也存在一些问题。链路加密通常用在点对点的同步或异步线路上，它要求先对在链路两端的加密设备进行同步，然后使用一种链模式对链路上传输的数据进行加密，这就给网络的性能和可管理性带来了副作用。在线路信号连通性不好的海外或卫星网络中，链路上的加密设备需要频繁地进行同步，带来的后果是数据丢失或重传。因此，即使一小部分数据需要进行加密，也会使得所有传输数据需要重新加密。

在一个网络结点，链路加密仅在通信链路上提供安全性，消息以明文形式存在，因此所有结点在物理上必须是安全的，否则就会泄漏明文内容。在传统的单钥加密算法中，解密密钥与加密密钥是相同的，该密钥必须被秘密保存，并按一定规则进行变化。这样，密钥分配在链路加密系统中就成了一个问题，每一个结点必须存储与其相连接的所有链路的加密密钥，这就需要对密钥进行物理传送或者建立专用网络设施。网络结点地理分布的广阔性使得这一过程变得复杂，同时增加了密钥连续分配时的代价。

3.3.2　结点加密

结点加密是指在信息传输路过的结点处进行解密和加密。尽管结点加密能给网络数据提供较高的安全性，但它在操作方式上与链路加密是类似的，两者均在通信链路上为传输的消息提供安全性，都在中间结点先对消息进行解密，然后进行加密。因为要对所有传输的数据进行加密，所以加密过程对用户是透明的。与链路加密不同的是，结点加密不允许消息在网络结点以明文形式存在，它先把收到的消息进行解密，然后采用另一个不同的密钥进行加密，这一过程是在结点上的一个安全模块中进行的。

结点加密要求报头和路由信息以明文形式传输，以便中间结点能得到如何处理消息的信息，这种方法对于防止攻击者分析通信业务是脆弱的。

3.3.3　端到端加密

端到端加密是指对一对用户之间的数据连续地提供保护，如图 3-12 所示。端到端加密允许数据在从源点到终点的传输过程中始终以密文形式存在。采用端到端加密（又称脱线加密或包加密），消息在被传输时到达终点之前不进行解密，因为消息在整个传输过程中均受到保护，所以即使有结点被损坏也不会使消息泄露。

端到端加密系统的价格便宜，且与链路加密和结点加密相比更可靠，更容易设计、实现和维护。端到端加密还避免了其他加密系统所固有的同步问题，因为每个报文包均是独立被加

密的，所以一个报文包所发生的传输错误不会影响后续的报文包。此外，从用户对安全需求的直觉上讲，端到端加密更自然。

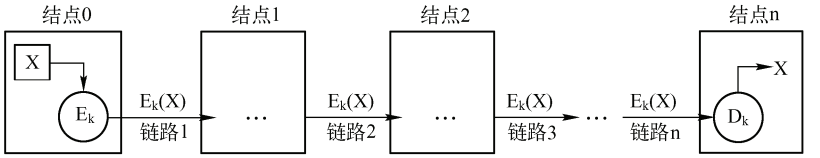


图 3-12　端到端加密

端到端加密系统通常不允许对消息目的地址进行加密，这是因为每一个消息所经过的结点都要用此地址来确定如何传输消息。由于这种加密方法不能掩盖被传输消息的源点与终点，因此它对于防止攻击者分析通信业务也是脆弱的。

3.3.4　同态加密应用

1．应用于云计算

云存储安全是云计算领域的重要安全问题之一，为解决数据隐私保护的问题，常见的方法是由用户对数据进行加密，把加密后的密文信息存储在服务端。但当用户需要服务器提供数据搜索、分析和处理等功能时，传统加密方案难以实现，同态加密为之提供了实现的可能。

（1）云计算中的加密数据检索

随着云计算技术的广泛应用，服务器端存储的加密数据必将成爆炸式增加，对加密数据的检索成为一个迫切需要解决的问题。现有的加密数据检索算法包括线性搜索、公钥搜索和安全索引等，这些算法可以快速地检索出所需信息，但是只适用于小规模数据的检索，而且代价很高。基于全同态加密技术的数据检索方法可以直接对加密的数据进行检索，不但能保证被检索的数据不被统计分析，还能对被检索的数据进行简单的运算，同时保持对应的明文顺序。

数据检索有多种方法，如向量空间模型等。首先对文档进行分词和词干化，即从文档中抽取出能表征文档主要内容特征和形式特征的检索词，以形成文档的向量表示，然后将得到的检索词和待检索文档进行加密，并储存至云服务器。采用了全同态加密方案后，当服务器需要检索加密文档时，可直接提交加密后的检索词，此时每个文档都可根据所提交的关键词进行权重向量表示，对用全同态加密后的词频和倒排文档频率进行操作可以得到权重。该权重反映了关键词与文档的相关度，因而可以根据大小进行排序，筛选出用户需要的文档，用户得到加密文档后，用私钥对文档解密即可得到原始文档。

（2）云计算中的加密数据处理

云计算中的加密数据处理与数据检索的思路类似，首先对待处理的关键数据进行加密和特殊标记，以与普通加密数据区分开来，然后再上传到服务器，服务器会直接对密文数据进行操作来完成用户的需求，并将处理后的密文返回给用户。

在医疗应用中，人们提出了一种医疗记录云存储系统（病人控制加密），医疗服务提供者先对病人的医疗记录进行加密，然后传输到云存储系统，病人通过与某个服务提供者分享私钥，共享其医疗记录，然而，该系统只提供云搜索服务（关键词匹配或者其他的一些搜索方法），并没有提供云计算服务。利用全同态加密体制，该系统可以对加密的医疗记录进行计算，为病人提供云计算服务。随着科技的发展，基于无线局域网的监视器或者其他设备将能够

代替病人连续不断地向云端服务器传输加密数据。利用全同态加密体制，云端服务器可以对加密数据进行计算，并根据具体的计算结果，返回给病人一些警告或者建议等。在这个方案中，可能需要计算平均值、标准差和最小二乘法等统计函数，加密输入可能包括血压、心率等实时信息，以及体重、性别等病人的基本信息，而加密用的函数则可以公开。

在金融行业中，全同态加密也有着潜在的应用，一些数据和进行加密的函数是需要保密的，例如公司的数据、股票价格、绩效和存货清单等信息都与投资决策有关，是制定交易策略的关键信息。全同态加密体制可以使一些函数能够被秘密地计算，用户可以将函数的加密形式和敏感数据的密文分别上传到云端服务器（或许它们分别来自不同的用户）；第三方的管理者可利用这些函数的加密形式对加密数据进行处理，在处理完成后，云端服务器把处理的结果以密文的形式发送给用户，用户解密后则可得到处理后的敏感数据。

2．应用于电子投票

电子投票在计票的快捷准确、人力和开支的节省，以及投票的便利性等方面有着传统投票方式无法企及的优越性，而设计安全的电子选举系统是全同态加密的一个典型应用。这里，以一个简单的电子选举方案为例进行说明。若有同态函数 $Enc_k(x_1+x_2)=Enc_k(x_1)\times Enc_k(x_2)$，选民将自己的选票进行加密 $C_i=Enc_k(M_i)$，其中 $M_i\in\{0，1\}$；投票中心收集同态加密后的选民选票 C_i；投票中心基于全同态加密方案的同态性质对加密后的选票 C_i 进行计票 $C=C_1\times C_2\times\cdots\times C_n$，得到经过同态加密后的选举结果 $C=Enc_k(M_1+M_2+\cdots+M_n)$；只有拥有解密密钥的某个可信机构才能够对加密后的选举结果进行解密，公布选举结果。在上述过程中，选票收集与计票完全对加密后的选票数据进行操作，不需要使用任何解密密钥，因此，任何一个主体或机构都可以完成计票员的职责，无论其是否可信。

3．应用于数字水印

数字水印技术是指用信号处理的方法在数字化的多媒体数据中嵌入隐蔽的标记，这种标记通常是不可见的，只有通过专用的检测器或阅读器才能提取，如何应对复杂网络环境下数据隐藏与数字水印系统的安全挑战，是目前需要迫切解决的问题。针对数字水印的一种主要的安全性攻击手段是非授权检测攻击，即攻击者在未经授权的情况下对含有水印的载体进行检测，以确定水印是否存在，进而猜测或破译水印的含义，甚至去除载体中的水印并嵌入一个伪造的水印。将全同态加密技术应用于数字水印可以有效地抵抗这种攻击。首先利用全同态加密体制对水印信号与原始载体进行加密，然后将加密后的水印嵌入到原始载体中，在用户检测水印之前，必须对含有水印的载体进行同态解密，从而保证解密后的水印信号与含水印的载体之间没有明显的相关性，在解密含水印的载体之后，可以通过计算解密后的载体与水印信号之间的相关度，判断水印的存在性，进而提取水印。

3.3.5 其他应用

除上述应用之外，加密技术还在电子商务、移动通信和 VPN 等其他领域发挥着作用，这里就以虚拟专用网 VPN（Virtual Private Network）为例来说明远程访问中的加密应用。

当前，越来越多的公司走向国际化，一个公司可能在多个国家或地区驻有办事机构或销售中心，每一个机构都有自己的局域网 LAN（Local Area Network），为将这些分布在不同地域的 LAN 连接在一起构成一个公司广域网，可以在 Internet 环境中构建 VPN。VPN 是专用网络在公共网络如 Internet 上的扩展，它通过运用私有隧道技术在公共网络上虚拟一条点到点的专线来达到数据安全传输的目的。VPN 属于远程访问技术，为保证利用公网链路架设私有网络

时数据的安全，VPN 服务器和客户机之间的通信数据都进行了加密处理。有了数据加密，就可认为数据是在一条专用的数据链路上进行安全传输，如同架设了一个专用网络，因此 VPN 实质上就是利用加密技术在公网上封装出一个数据通信隧道。有了 VPN 技术，用户无论是在外地出差还是在家中办公，只要能上互联网就能利用 VPN 非常方便地访问公司的内网资源。

VPN 主要采用隧道（Tunneling）、加解密、密钥管理，以及用户与设备身份认证等技术来保证用户数据的安全。用户依托 VPN 传输数据过程中，数据离开发送者所在的局域网时，将首先被用户端连接到互联网上的路由器进行硬件加密，而后数据在互联网上以加密形式进行传送，当到达目的 LAN 路由器时，该路由器将对数据进行解密，这样目的 LAN 中的用户就可以看到正确的数据信息。

3.4 认证技术

如前所述，数据加密是密码技术应用的重要领域，而在认证技术中密码技术也同样作用明显，但两者的应用目的不同。加密是为了隐蔽消息内容，认证是防止不法分子实施主动信息攻击的一种重要技术，其应用目的包括 3 个方面：一是消息完整性认证，验证信息在传送或存储过程中是否被篡改；二是身份认证，验证消息的收发者是否持有正确的身份认证符，如口令、密钥等；三是消息的序号和操作时间（时间性）等认证，目的是防止消息重放或会话劫持等攻击。

3.4.1 认证技术分层模型

如图 3-13 所示，认证技术可以分为 3 个层次：安全管理协议、认证体制和密码体制。安全管理协议的主要任务是在安全体制的支持下，建立、强化和实施整个网络系统的安全策略；认证体制在安全管理协议的控制和密码体制的支持下，完成各种认证功能；密码体制是认证技术的基础，它为认证体制提供数学方法支持。

典型的安全管理协议有公用管理信息协议 CMIP、简单网络管理协议 SNMP 和分布式安全管理协议 DSM。典型的认证体制有 Kerberos 体制、X.509 体制和 Light Kryptonight 体制。密码体制已在本章前面内容中介绍过。这里将主要介绍认证体制层的有关技术。

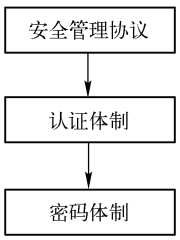


图 3-13 认证技术层次模型

3.4.2 认证体制要求与模型

一个安全的认证体制应该至少满足以下要求。

1）指定的接收者能够检验和证实消息的合法性、真实性和完整性。

2）消息的发送者对所发的消息不能抵赖，有时也要求消息的接收者不能否认收到的消息。

3）除了合法的消息发送者外，其他人不能伪造发送消息。

认证体制的基本模型（又称纯认证系统模型）如图 3-14 所示。

在这个模型中，发送者通过一个公开的无扰信道将消息送给接收者。接收者不仅得到消息本身，而且还要验证消息是否来自合法的发送者及消息是否经过篡改。攻击者不仅可截收和分析信道中传送的密报，而且可能伪造密文送给接收者进行欺诈等主动攻击。认证体制中通常存在一个可信中心或可信第三方（如认证机构 CA），用于仲裁、颁发证书或管理某些机密信息。

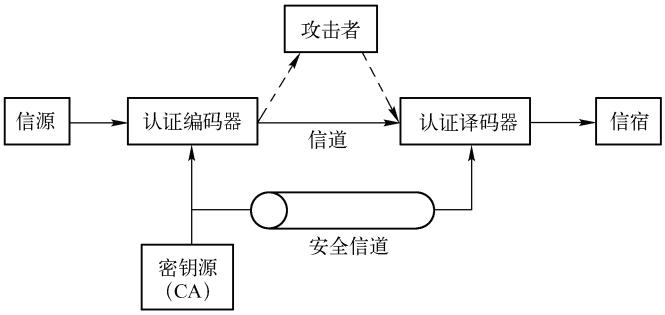


图 3-14　纯认证系统模型

3.4.3　数字签名技术

数字签名技术是一种实现消息完整性认证和身份认证的重要技术。

一个数字签名方案由安全参数、消息空间、签名、密钥生成算法、签名算法和验证算法等成分构成。根据接收者验证签名的方式可将数字签名分为真数字签名和公证数字签名两类。在真数字签名中（见图 3-15），签名者直接把签名消息传送给接收者，接收者无须求助于第三方就能验证签名。而在公证数字签名中（见图 3-16），签名者把签名消息通过被称为公证者的可信第三方发送给接收者，接收者不能直接验证签名，签名的合法性是通过公证者作为媒介来保证的，也就是说接收者要验证签名必须同公证者合作。

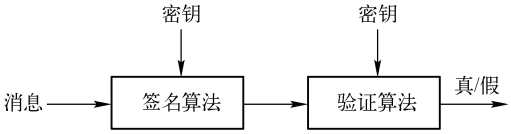


图 3-15　真数字签名方式

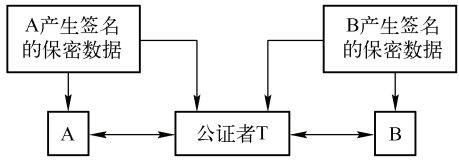


图 3-16　公证数字签名方式

数字签名算法可分为普通数字签名算法、不可否认数字签名算法、Fail-Stop 数字签名算法、盲数字签名算法和群数字签名算法等。普通数字签名算法包括 RSA 数字签名算法、ElGamal 数字签名算法、Fiat-Shamir 数字签名算法和 Guillou-Quisquarter 数字签名算法等。数字签名与手写签名的主要区别在于：一是手写签名是不变的，而数字签名对不同的消息是不同的，即手写签名因人而异，数字签名因消息而异；二是手写签名是易被模拟的，无论哪种文字的手写签名，伪造者都容易模仿，而数字签名是在密钥控制下产生的，在没有密钥的情况下，模仿者几乎无法模仿出数字签名。

3.4.4　身份认证技术

身份认证的目的是验证信息收发方是否持有合法的身份认证符（口令、密钥和实物证件等）。从认证机制上讲，身份认证技术可分为两类：一类是专门进行身份认证的直接身份认证技术，另一类是在消息签名和加密认证过程中，通过检验收发方是否持有合法的密钥进行的认证，称为间接身份认证技术。下面着重介绍直接身份认证技术。

在用户接入（或登录）系统时，直接身份认证技术要首先验证他是否持有合法的身份认证符（口令或实物证件等）。如果他有合法的身份认证符，就允许他接入系统中，进行允许的收发等操作，否则就拒绝其接入系统。通信和数据系统的安全性常常取决于能否正确识别通信

用户或终端的个人身份，如银行的自动取款机（ATM）系统可将现金发放给经它正确识别的账号持卡人。对计算机的访问和使用，以及安全地区的出入放行等都是以准确的身份认证作为基础的。

进入信息社会，传统的身份认证方法，如户籍管理、身份证制度以及单位机构的证件和图章等，都已不能适应时代的要求。虽然有不少学者试图电子化生物唯一识别信息（如指纹、掌纹、声纹、视网膜和脸形等），但由于代价高、传输效率低，只能作为辅助措施应用。使用密码技术，特别是公钥密码技术，能够设计出安全性高的识别协议。下面介绍一些常用的身份认证技术。

1．身份认证方式

身份认证常用的方式主要有两种：通行字（口令）方式和持证方式。

通行字方式是使用最广泛的一种身份认证方式。比如我国古代调兵用的虎符、现代通信网的接入协议等。通行字一般为数字、字母和特殊字符等组成的长字符串，通行字识别的方法是：被认证者先输入他的通行字，然后计算机确定其正确性。被认证者和计算机都知道这个秘密的通行字，每次登录时计算机都要求输入通行字，这样就要求计算机存储通行字，一旦通行字文件暴露，攻击者就有机可乘。为此，人们采用单向函数来克服这种缺陷，此时，计算机存储通行字的单向函数值而不是存储通行字本身，其认证过程如下。

1）被认证者将他的通行字输入计算机。

2）计算机完成通行字的单向函数值计算。

3）计算机把单向函数值和机器存储的值进行比较。

由于计算机不再存储每个人的有效通行字表，即使攻击者侵入计算机也无法从通行字的单向函数值表中获得通行字，当然这种保护对字典式攻击是比较脆弱的。

持证方式是一种实物认证方式。持证（token）是一种个人持有物，它的作用类似于钥匙，用于启动电子设备。使用较多的是一种嵌有磁条的塑料卡，磁条上记录有用于机器识别的个人识别号（PIN）。这类卡易于伪造，因此产生了一种被称为“智能卡”（smart card）的集成电路卡来代替普通的磁卡，智能卡已经成为身份认证的一种更有效、更安全的方法。但智能卡仅为身份认证提供一个硬件基础，要想得到安全的识别，还需要与安全协议配套使用。

2．身份认证协议

目前，认证协议大多数为询问－应答式协议，其基本工作过程是：认证者提出问题（通常为口令、图像识别或验证码等），由被认证者回答，然后认证者验证其身份的真实性。询问－应答式协议可分为两类：一类是基于私钥密码体制，在这类协议中认证者知道被认证者的秘密；另一类是基于公钥密码体制，在这类协议中认证者不知道被认证者的秘密，因此，又称为零知识身份认证协议。

下面介绍著名的 Feige-Fiat-Shamir 零知识身份认证协议。在该协议中，可信赖的 CA（认证机构）选定一个随机数 m 作为模数，并把 m 分发给认证双方（用户 A 和 B）。CA 产生随机数 v，使 $x^2 = v \bmod m$（v 为模 m 的平方剩余），且存在 v 的逆元 v^{-1}（即 $v * v^{-1} = 1 \bmod m$）。以 v 作为公钥分发给用户。然后后计算最小的整数 s，$s = \sqrt{1/v} \bmod m$，并把 s 作为私钥分发给用户 A。实施身份证明的协议如下。

1）用户 A 取随机数 r（$r < m$），计算 $x = r^2 \bmod m$ 送给 B。

2）B 将一个随机位数 b 送给 A。

3）若 b＝0，则 A 将 r 送给 B；若 b＝1，则 A 将 y＝rs 送给 B。

4）若 b = 0，则 B 证实 $x = r^2 \bmod m$，从而证明 A 知道 $\sqrt{x}$；若 b = 1，则 B 证实 $x = y^2 * v \bmod m$，从而证实 A 知道 s。

这是一次鉴定，A 和 B 可重复 t 次鉴定，每次采用不同的 r 和 b，直到 B 相信 A 知道 s 为止。

该协议的安全性分析如下。

1）A 欺骗 B 的可能性。A 不知道 s，他也可取 r，送 $x = r^2 \bmod m$ 给 B，B 送 b 给 A，A 可将 r 送出。当 b=0 时，则 B 可通过检验而受骗，当 b=1 时，则 B 可发现 A 不知 s，B 受骗的概率为 1/2，但连续重复 t 次受骗的概率仅为 2^{-t}。

2）B 伪装 A 的可能性。B 和其他被认证者 c 开始一个协议，第一步他可使用 A 用过的随机数 r，若 c 所选的 b 值恰好与以前发给 A 的一样，则 B 可将在协议第 3 步所发的数值重发给 c，从而成功地伪装 A，但 c 随机选 b 为 0 或 1，故这种攻击的成功概率仅为 1/2。但重复执行 t 次后，攻击成功概率降为 2^{-t}。

3.4.5 消息认证技术

消息认证是指通过对消息或消息相关信息进行加密或签名变换进行的认证，其目的包括消息内容认证（即消息完整性认证）、消息的源和宿认证（即身份认证），以及消息的序号和操作时间认证等。

1．消息内容认证

在介绍消息内容认证方法之前，首先介绍一下杂凑函数。

（1）杂凑函数

杂凑（Hash）函数是将任意长的数字串 M 映射成一个较短的定长数字串 H 的函数，以 h 表示，h(M)易于计算，称 H=h(M)为 M 的杂凑值，也称杂凑码、杂凑结果等。这个 H 无疑打上了输入数字串的烙印，因此又称其为输入 M 的数字指纹（Digital Fingerprinting）或数据摘要（Message Digest）。h 是多对一映射，因此无法从 H 求原来的 M，但可以验证任意给定序列 M′ 是否与 M 有相同的杂凑值。

若杂凑函数 h 为单向函数，则称其为单向杂凑函数。用于消息认证的杂凑函数都是单向杂凑函数。单向杂凑函数按其是否有密钥控制划分为两大类：一类有密钥控制，以 h(k,M)表示，为密码杂凑函数；另一类无密钥控制，为一般杂凑函数。无密钥控制的单向杂凑函数，其杂凑值只是输入字串的函数，任何人都可以计算，因而不具备身份认证功能，只用于检测接收数据的完整性。而有密钥控制的单向杂凑函数要满足各种安全要求，其杂凑值不仅与输入有关，而且与密钥有关，只有持此密钥的人能够计算出相应的杂凑值，因此具有身份验证功能。杂凑函数在实际工作中有着广泛的应用，在密码学和数据安全技术中，它是实现有效、安全可靠数字签名和认证的重要工具，是安全认证协议中的重要模块。由于杂凑函数应用的多样性和其本身的特点而有很多不同的名称，其含义也有差别，如压缩（Compression）函数、紧缩（Contraction）函数、数据认证码、消息摘要、数字指纹、数据完整性校验（Data Integrity Check）、密码检验和（Cryptographic Check Sum）、消息认证码 MAC（Message Authentication Code）和窜改检测码 MDC（Manipulation Detection Code）等。

构造杂凑函数的方法有两种，一是直接构造，比如由美国麻省理工学院 Rivest 设计的 MD5 杂凑算法，可以将任意长度的明文转换为 128 位的数据摘要；美国国家标准局（NIST）

为配合数字签名标准于 1993 年对外公布的安全杂凑函数（SHA），可对任意长度的明文产生 160 位的数据摘要。另一种是间接构造，主要是利用现有的分组加密算法，如 DES、AES 等，对其稍加修改，采用它们加密的非线性变换构造杂凑函数。如 Rabin 在 1978 年利用 DES 提出了一种简单快速的杂凑函数，其方法是：首先将明文分成长度为 64 位的明文组 m_1，m_2，…，m_N，采用 DES 的非线性变换对每一明文组依次进行变换，即令 h_0＝初始值，$h_i=E_{mi}[h_{i-1}]$，最后输出的 h_N 就是明文的杂凑值。

杂凑函数必须满足密码学的安全性要求。显然，对于一个单向杂凑函数 h，由 M 计算 H = h(M)是容易的，但要产生一个 M′使 h(M′)等于给定的杂凑值 H 则非常困难，这正是应用密码所希望的，否则对手就会用 M′代替 M，窜改消息内容。若单向杂凑函数 h 对任意给定 M 的杂凑值 H = h(M)，找一个 M′使 h(M′) = H 在计算上可行，则称 h 为弱单向杂凑函数；若要找任意一对输入$(M_1,M_2:M_1 \neq M_2)$，使 $h(M_1)=h(M_2)$在计算上不可行，则称 h 为强单向杂凑函数。

杂凑函数的安全性取决于其抗击各种攻击的能力，攻击者的目标是找到两个不同消息可映射为同一杂凑值。一般假定攻击者知道杂凑算法，采用选择明文攻击法。强杂凑函数是基于生日攻击法定义的。所谓“生日攻击”，是指在一个会场参加会议的人中，找一个人与某人生日相同的概率超过 0.5 时，所需参加会议人员为 183 人。但要使参会人员至少有两个生日相同的概率超过 0.5 的参会人数仅为 23 人。即在一定元素所组成的集合中，给定 M 找与 M 匹配的 M′概率要比从集合中任意取出一对相同元素（M= M′）的概率小得多。弱单向杂凑函数考察的是任意元素与特定元素的无碰撞性（Collision-free）；而强单向杂凑函数考察的是输入集中任意两个元素的无碰撞性。因此，就无碰撞性而言，对强单向杂凑函数的要求比对弱单向杂凑函数的要求高。为了抵抗生日攻击及其他杂凑函数的攻击法，根据目前的计算技术，杂凑函数值至少为 128 位长。

目前已研制出适合各种用途的杂凑算法，这些算法都是伪随机函数，任何杂凑值都是等可能的，输出并不以可辨别的方式依赖于输入。在任何输入串中单个位的变化，将会导致输出位串中大约一半的位发生变化。

总之，为了抵抗各种攻击，所采用的杂凑函数应满足单向性、伪随机性、非线性性及杂凑速率的高效性等密码学性质。

（2）消息内容认证

消息内容认证的常用方法是：消息发送者在消息中加入一个鉴别码（MAC、MDC 等），经加密后发送给接收者（有时只需加密鉴别码即可），接收者利用约定的算法对解密后的消息进行鉴别运算，若获得的鉴别码与原鉴别码相等则接收，否则拒绝接收。

2．消息的源和宿认证

在消息认证中，消息源和宿认证的常用方法有两种：一种是通信双方事先约定发送消息的数据加密密钥，接收者只需证实发送来的消息是否能用该密钥还原成明文就能鉴别发送者，如果双方使用同一个数据加密密钥，那么只需在消息中嵌入发送者识别符即可。另一种是通信双方事先约定用于各自发送消息的通行字，发送消息时将通行字一并进行加密，接收者只需判别消息中解密的通行字是否与约定通行字相符就可鉴别发送者。为安全起见，通行字应该是可变的。

3．消息的序号和操作时间认证

消息的序号和操作时间的认证主要用于阻止消息的重放攻击，常用的方法有消息的流水作业、链接认证符随机数认证法和时戳等。

3.4.6 数字签名与消息认证

杂凑函数产生的杂凑值（鉴别码）可直接用于消息认证，也可通过数字签名方法间接用于消息认证。一般地，对长度较大的明文直接进行数字签名需要的运算量和传输开销也较大，而杂凑值就是明文的“指纹”或“摘要”，因而对杂凑值进行数字签名可以视为对其明文进行数字签名。实际应用中，通常也是对明文杂凑值而非明文本身进行数字签名，目的就在于提高数字签名效率。

数字签名与消息认证的区别是，消息认证可以帮助接收方验证消息发送者的身份，以及消息是否被篡改。当收发者之间没有利害冲突时，这种方式对于防止第三者破坏是有效的，但当收发者之间存在利害冲突时，单纯采用消息认证技术就无法解决纠纷，这时就需要借助于数字签名技术来辅助进行更有效的消息认证。

3.5 公开密钥基础设施（PKI）

随着互联网技术的迅速推广和普及，各种网络应用如电子商务、电子政务、网上银行和网上证券交易等也在迅猛发展。互联网以其开放性、易接入、信息丰富及成本低廉等优点获得了人们的广泛认可。同时，其安全问题也成为人们担心的焦点，网络非法入侵、网上诈骗等案件造成的损失已逐年上升。因此，解决网络信息安全问题已成为发展网络通信的重要任务。

在信息安全技术领域，特别是网络安全技术方向，公开密钥加密技术（即前面介绍的双钥加密技术）近年来发展很快，这主要是由公钥体制本身的特点所决定的。公钥体制采用了两个密钥，一个公钥作为加密密钥，一个私钥作为用户专有的解密密钥，通信双方无须交换专用密钥，这就避免了在网上传递私钥这样的敏感信息，进而可以实现保密通信。

在这项技术基础上形成和发展起来的 PKI（Public Key Infrastructure，公钥基础设施）很好地适应了互联网的特点，为互联网及类似网络应用提供了全面的安全服务，如安全认证、密钥管理、数据完整性检验和不可否认性等。可以说，今天互联网的安全应用已经离不开 PKI 的有力支持。

从参与电子政务与电子商务的用户实体出发，网络应用常规的安全需求主要包括以下几个。

1）认证需求：提供某个实体（人或系统）的身份保证。

2）访问控制需求：保护资源，防止被非法使用和操作。

3）保密需求：保护信息不被泄漏或暴露给非授权的实体。

4）数据完整性需求：保护数据，防止未经授权的增删、修改和替代。

5）不可否认需求：防止参与某次通信交换的一方事后否认交换行为。

针对电子政务和电子商务的这些安全需求，以公钥加密技术为基础的 PKI 应运而生。

3.5.1 PKI 的基本概念

所谓安全基础设施，就是为整体网络应用系统提供的安全基本框架，它应该可以被系统中的任何用户按需使用。安全基础设施的本质必须是统一的、便于使用的，只有这样，那些需要基础设施支撑的对象在使用安全服务时才不会遇到困难。因此，PKI 首先是适用于多种环境的框架，这个框架避免了零碎的、点对点的、特别是那些没有互操作性的解决方案，它引入了可管理的机制，以及跨越多个应用和多种计算平台的一致安全性。

PKI 是一个用公钥密码算法原理和技术来提供安全服务的通用性基础平台，用户可利用

PKI 平台提供的安全服务进行安全通信。PKI 采用标准的密钥管理规则，能够为所有应用透明地提供加密和数字签名等服务需要的密钥和证书管理。

1．认证机构

使用公钥技术实现安全通信面临的一个基本问题是，通信发送方如何可靠地获得接收方的真实公钥。如果发送方获得的不是接收方的真实公钥，那么，接收方就不能解密发送方加密的信息。更严重的是，如果接收方获得的是由窃密者提供的假冒公钥，则窃密者就可以解密该信息，并利用它进行其他破坏活动。PKI 通过使用公钥证书来解决这一问题，公钥证书是用户（接收方）的身份标识与其持有公钥的结合，在生成公钥证书之前，由一个可信任的权威机构 CA（认证机构或认证中心）来证实用户的身份，然后 CA 对由该用户身份标识及对应公钥组成的证书进行数字签名，以证明公钥的有效性。因此，CA 是 PKI 的核心部分，它是数字证书的签发机构。PKI 首先必须具有可信任的权威 CA，然后在公钥加密技术基础上，实现证书的产生、管理、存档及作废管理等功能。

2．身份识别

为了启动一个应用系统，简单的做法是本地安全登录，其操作过程是用户输入身份标识符（用户 ID）及认证口令，计算机通过检查这两个输入验证用户身份，确认是否为合法登录。这种身份识别方法较为简单，其假设前提是除合法用户之外，无人能获取该用户口令。当系统要求用户远程登录时，口令在未受保护的网络上传送，很容易被截取或监听，即使口令被加密也无法防范重放攻击，因此这种简单识别带来的问题是明显的。

PKI 采用公钥技术、高级通信协议和数字签名等方式进行远程登录，既不需要事先建立共享密钥，也不必在网上传递口令等敏感信息。因此，口令的保密性较高，机器对用户身份识别的可靠性高。与简单的身份识别机制相比，PKI 的身份识别机制称为强识别。

3．透明性

作为一种基础设施，PKI 对终端用户的操作是透明的，即所有安全操作在后台自动进行，无须用户干预，也不应由于用户的错误操作对安全造成危害。总之，安全不应该成为用户完成其他任务的障碍。除初始登录操作之外，PKI 对用户是完全透明的。

4．一致性

作为安全基础设施，PKI 的最大优势是在整个应用环境中使用单一可信的安全技术，如公钥技术，它能保证数目不受限制的应用程序、设备和服务器无缝地协调工作，安全地传输、存储和检验数据，安全地进行事务处理等。电子邮件、Web 服务、防火墙、远程访问设备、应用服务器、文件服务器、数据库及其他应用等，都能够采用统一的方式理解和使用安全服务基础设施，PKI 是使系统达到全面安全性的一个重要机制。

5．相关的标准

（1）X.509

X.509 是 ISO 和 CCITT/ITU-T 的 X.500 标准系列中的一部分，在 PKI 概念由小的封闭式网络试验环境发展到大的开放式分布环境的过程中，X.509 标准的作用不可或缺。从发展的角度来看，X.509 标准是 PKI 的雏形，PKI 源于 X.509 标准并标准化了一个通用的证书格式。X.509 被广泛应用，其实用性来源于其版本 3（V3 版）中证书撤销列表定义的强有力的扩展机制，这一机制是很通用的，并且指示了认证者如何在认证过程中校验这些扩展。

（2）X.500

ISO/ITU-T 中有关目录的标准族通常称为 X.500 规范系列。X.500 目录服务是一个高度复

杂的信息存储机制，包括客户机—目录服务器访问协议、服务器—服务器通信协议、完全或部分的目录数据复制、服务器对查询的响应，以及复杂搜寻的过滤功能等。X.500 对 PKI 有着特别重要的作用，它定义了一种方案，即在实体目录访问入口处使用标准化方法，完成证书和证书撤销列表数据结构的存储访问。

（3）LDAP

LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）最初被视为 X.500 目录访问协议（DAP）中那些容易被描述、易于执行的功能子集。后来其功能逐渐增强扩展，进而可以适应不同环境的需求，这些环境都采用 LDAP 作为存储器的访问协议。

3.5.2 PKI 认证技术的组成

公钥基础设施在组成上主要包括认证机构 CA、证书库、密钥备份（即恢复系统）、证书作废处理系统和 PKI 应用接口系统等。

1．CA

CA 作为数字证书签发机构是 PKI 的核心，是 PKI 应用中权威的、可信任的、公正的第三方机构。

由于公钥需在网上公开传输，PKI 服务系统的关键问题是如何实现公钥的管理，因而引入证书机制至关重要。证书是公开密钥体制的一种密钥管理媒介，是一种权威的电子文档，形同网络计算环境中的一种身份证，用于证明某一主体（如用户、服务器等）的身份及其公开密钥的合法性。在使用公钥体制的网络环境中，必须向公钥使用者证明公钥的真实合法性。因此，必须有一个可信的机构来对任何一个主体的公钥进行公证，证明主体的身份及其与公钥的匹配关系。CA 正是这样的机构，其职责有以下几个。

- 验证并标识证书申请者的身份。
- 确保用于签名证书的非对称密钥的质量。
- 确保整个鉴证过程中的安全性，确保签名私钥的安全性。
- 证书资料信息（包括公钥证书序列号、CA 标识等）的管理。
- 确保并检查证书的有效期限。
- 发布并维护作废证书列表。
- 对整个证书签发过程做日志记录。
- 向申请人发出通知。

其中，最重要的是 CA 自己的一对密钥的管理，它必须确保其高度的机密性，防止他人伪造证书。CA 公钥在网上公开，整个网络系统必须保证完整性。CA 的数字签名保证了证书（实质是持有者的公钥）的合法性和权威性。主体（用户）的公钥有两种产生方式。

1）用户自己生成密钥对，然后将公钥以安全的方式传送给 CA，该过程必须保证用户公钥的可验证性和完整性。

2）CA 替用户生成密钥对，然后将其以安全的方式传送给用户，该过程必须确保密钥对的机密性、完整性和可验证性。由于这里的用户私钥为 CA 所产生，故对 CA 的可信性要求更高，CA 必须在事后有效地销毁用户的私钥。

用户 A 在网上可通过两种方式获取用户 B 的证书和公钥，一种是由 B 将证书随同发送的正文信息一起传送给 A，一种是所有的证书集中存放于一个证书库中，用户 A 通过网络从该库中获取 B 的证书。

前面提到，公钥不仅可以用于加密信息，还可以用于数字签名。相应地，系统中需要配置用于数字签名/验证的密钥对和用于数据加密/解密的密钥对，它们分别被称为签名密钥对和加密密钥对，这两对密钥对之于密钥管理有不同的要求。

（1）签名密钥对

签名密钥对由签名私钥和验证公钥组成。为保持其唯一性，签名私钥不能存档备份，丢失后需重新生成新的密钥对，原来的签名可以使用旧公钥的备份来验证，所以验证公钥需要存档备份，以用于验证旧的数字签名。

（2）加密密钥对

加密密钥对由公钥和脱密私钥组成。为防止密钥丢失时不能脱密数据，脱密私钥应该进行存档备份，以便能在任何时候脱密密文数据，加密公钥无须存档备份，加密公钥丢失时，需要重新产生密钥对。

显然，这两对密钥对的管理要求存在互相冲突的地方，因此系统必须针对不同的用途使用不同的密钥对。若加密和签名采用同一对密钥，那是不安全的。

2．证书库

证书库是 CA 颁发证书和撤销证书的集中存放地，是网上的一种公共信息库，供广大用户进行开放式查询。

证书及证书撤销信息的分发办法是发布（Publication），其思想是将 PKI 的信息放在一个广为人知的、公开且易于访问的地点，这对广大用户群体来说十分重要，因为即使属于同一群体中的人也难以互相认识。

到证书库访问查询，可以得到想要与之通信的实体的公钥。若甲想与乙进行保密通信，就必须找到乙的公钥，而证书签发机构事先已将乙的身份与其公钥捆绑，进行了数字签名，发布在证书库中。甲可以通过某种可靠的、安全的方式从证书库中找到乙的证书，从而得到其公钥。

由于证书的不可伪造性，因此，可以在数据库中公布，而无须其他的安全措施来保护这些证书。现在，通常的做法是将证书和证书撤销信息发布到一个数据库（证书库或目录服务器）中，它采用 LDAP 目录访问协议，其格式符合 X.500 标准，客户端可以通过多种访问协议从证书库中实时查询证书和证书撤销信息。

证书库支持分布式存放，当 PKI 所支持的环境扩充到几十万或上百万用户时，PKI 信息的及时和强有力的分布机制就显得非常关键，如目录服务器的分布式存放，这是任何一个大规模 PKI 系统成功实施的基本需求，也是创建一个有效认证机构 CA 的关键技术之一。

3．证书撤销

认证机构 CA 通过签发证书来为用户的身份和公钥进行捆绑，但同时还必须存在一种机制来撤销这种捆绑关系，将现行的证书撤销。比如，在用户身份姓名改变、私钥被窃或泄漏、用户与其所属单位关系变更时，就需要一种方法警告其他用户不要再使用其原来的公钥。在 PKI 中，这种警告机制被称为证书撤销，它所使用的手段为证书撤销列表（CRL）。

证书撤销信息的更新和发布频率是非常重要的，一定要确定合适的间隔频率来发布证书撤销信息，并且要将这些信息及时地散发给那些正在使用这些证书的用户。通常，两次证书撤销信息之间的间隔被称为撤销延迟。

证书撤销的实现方法有多种，一种方法是利用周期性的发布机制，如 CRL，这是常用方法，另一种方法是在线查询机制，如在线证书状态协议 OCSP。

（1）CRL

CRL 的结构是按 X.509 证书标准定义的，其结构如图 3-17 所示。

事实上，CRL 是一种包含撤销证书列表的签名数据结构，CRL 的完整性和可靠性由其自身的数字签名来保证。CRL 的签名者一般也就是颁发证书的签名者。

版 本 号	签　名	颁 发 者	本次更新	下次更新	撤销的证书列表	扩 展 域

① 版本号——指出CRL的版本号。
② 签名——计算本CRL的数字签名所用的算法的对象标识符。
③ 颁发者——CRL颁发者（即CRL的签名者）的可识别名（DN），本字段必须写出且唯一。
④ 本次更新——本CRL的发布时间，以UTC Time或Generalized Time的形式表示。
⑤ 下次更新——属可选项，下一个CRL的发布时间，其表示形式与本次更新字段一样。
⑥ 撤销的证书——撤销的证书的列表，每个证书对应一个唯一的标识符。
⑦ 扩展域——有 4 个定义可用于每项的扩展。
理由代码——证书撤销理由，包括密钥损坏、CA损坏、关系变动、取代、操作终止、证书控制、从CRL的去除，以及未指明的理由。
证书颁发者——证书颁发者的名字。
控制指示代码——用于证书的临时冻结。
无效日期——本证书不再有效的时间。

图 3-17　CRL 结构

（2）在线查询机制

对证书撤销信息的查询，也可利用在线查询机制，即要求用户无论检索证书撤销与否都必须与数据库保持在线状态。

目前，最普遍的在线撤销机制就是在线证书状态协议（OCSP），这是一种相对简单的请求/响应协议。一个 OCSP 请求由协议版本号、服务请求类型，以及一个或多个证书标识符组成。

响应信息由证书标识符、证书状态（“正常”、“撤销”等），以及对应于原请求中具体证书标识符的验证响应时间组成。响应信息必须经过数字签名，以保证其源于可信任方并且在传输过程中未被篡改。签名密钥一般属于颁发证书的 CA，是一个可信任的第三方。因此，在任何情况下，用户必须信任这个响应信息。

关于证书撤销信息查询问题，有多种技术来实现，但不同的技术适用于不同的环境，PKI 应提供多种选择，进而构成最佳的撤销方案。

4．密钥备份和恢复

为避免解密密钥丢失带来的不便，PKI 提供了密钥备份与解密密钥的恢复机制，即密钥备份与恢复系统，它由可信任的 CA 来完成。值得注意的是，密钥备份与恢复只针对解密密钥，签名密钥是不能做备份的。

一个证书的生命周期主要包括 3 个阶段，即证书初始化注册阶段、颁发阶段和取消阶段。而证书密钥的备份与恢复就发生在初始化注册阶段和颁发阶段。

（1）密钥/证书生命周期

密钥/证书的生命周期可分为初始化、颁发和取消 3 个阶段，如图 3-18 所示。

初始化阶段指的是终端用户在使用 PKI 服务之前，必须经过初始化程序进入 PKI，由以下几步组成。

- 终端实体注册。
- 密钥对产生。
- 证书创建和密钥/证书分发。
- 密钥备份。

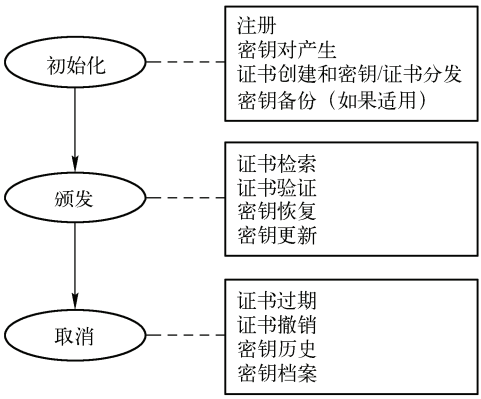


图 3-18　密钥/证书生命周期管理

颁发阶段包括以下几个。

- 证书检索——远程数据库的证书检索。
- 证书验证——确定一个证书的有效性。
- 密钥恢复——不能正常解读加密文件时，从 CA 中恢复。
- 密钥更新——当一个合法的密钥对将要过期时，新的公/私密钥对会自动产生并颁发。

取消阶段是密钥/证书生命周期管理的结束，主要步骤包括以下几个。

- 证书过期——证书的自然过期。
- 证书撤销——宣布一个合法证书（及相关密钥）不再生效。
- 密钥历史——维护一个有关密钥资料的连续记录，以便以后过期的密钥所加密的数据可以被解密。
- 密钥档案——为了密钥历史恢复、审计和解决争议的目的，密钥历史档案由 CA 储存。

由此可见，密钥备份与恢复贯穿证书的整个生命周期。

（2）密钥备份

用户在申请证书的初始阶段，如果声明公/私密钥对是用于数据加密的，则 CA 对该用户的密钥和证书进行备份，备份设备的位置可以从一个 PKI 域变到另一个 PKI 域。

（3）密钥恢复

密钥恢复功能发生在颁发阶段，其功能是将终端用户丢失的加密密钥予以恢复，这种恢复由可信任的密钥恢复中心或 CA 完成。密钥恢复的手段可以从远程设备恢复，也可由本地设备恢复。考虑到可扩展性并将 PKI 管理员和终端用户的负担减到最小，恢复过程必须尽可能地自动化和透明化。此外，任何综合的生命周期管理协议都必须具有对这个能力的支持。

密钥恢复和密钥备份一样，只适用于用户的加密密钥，签名密钥或私钥不应备份，因为这样将影响提供不可否认性的能力。

5．自动更新密钥

一个证书的有效期是有限的，这样规定既有理论原因，又有实际操作因素。因此，在很多 PKI 环境中，一个已颁发的证书需要有过期的措施，以便更换新的证书。为避免密钥更新的复杂性和人工操作的烦琐，PKI 支持自动密钥或证书更新。其指导思想是，无论用户的证书用于何种目的，认证时都会在线自动检查有效期，在失效日期到来之前的某段时间内，自动启

动更新程序，生成一个新的证书来代替旧证书，新旧证书的序列号也不相同。

（1）密钥更新

密钥更新发生在证书的颁发阶段。当证书“接近”过期时，必须颁发一个新的公/私密钥和相关证书，这称为密钥更新。所谓“接近”过期，一般是指在证书到达有效期之前的时间“提前量”，通常规定这个提前量为整个密钥生存期的 20%左右。实践证明，这是一个合理的转变时间，可以防止证书过期而得不到安全服务。源于扩展性的要求，这个更新过程必须自动进行，对终端用户而言，也应该是透明的。

（2）证书更新与证书恢复

证书更新与证书恢复是两个不同的概念，证书恢复是保持最初的公钥/私钥对，密钥证书更新是在证书中产生了一个新的公钥/私钥对。证书之所以能够恢复，取决于最初颁发证书的环境没有变化，并且还认为这个公/私钥对仍是可信的。

6．密钥历史档案

从密钥更新的概念可知，在经过一段时间之后，每个用户都会形成多个“旧”证书和至少一个“当前”证书，这一系列旧证书和相应的私钥就组成了用户密钥和证书的历史档案。

记录整个密钥历史是一件十分重要的事情。例如，甲 5 年前加密的数据或他人用甲的公钥加密的数据无法用现在的私钥解密，那么，甲就需要从其密钥历史档案中找到正确的解密密钥来解密数据。以此类推，有时也需要从密钥历史档案中找到合适的证书验证甲 5 年前的数字签名。与密钥更新相同，管理密钥历史档案也应由 PKI 自动完成，密钥历史档案发生在密钥/证书生命周期的取消阶段。

（1）密钥历史

即使密钥资料已过期，可靠和安全地存储加密密钥也是必需的。在 PKI 中，存储加密密钥的数据库称为密钥历史。一定程度上，密钥历史主要是为保证数据的机密性服务的。具体而言，就是用做解密的私有密钥资料被存储，以便将来对已加密数据进行恢复。对于那些用于数字签名目的的密钥，只能通过密钥档案适当地满足这种需求。

（2）密钥档案

与密钥历史不同，密钥档案主要在审计和交易争端时使用。密钥历史一般直接与终端实体相结合，以便在访问已过期密钥加密的数据时，快捷地提供过期密钥资料。密钥档案一般则是由第三方提供服务，其提供的服务包括公证和时间戳服务、跟踪审计，以及终端实体的密钥历史恢复等。当局部密钥历史丢失或遭破坏后，密钥档案服务就显得相当重要。一个给定终端实体的密钥历史可以由密钥档案设备存储起来，以便将来响应来自密钥历史所有者的请求，或者其他无终端实体但已被授权访问该密钥资料者的请求。

另外，当试图验证一个已过期的密钥资料所创建的数字签名时，密钥档案设备可能是必需的，因为在这种情况下，需要恢复对该数字签名有用的公钥证书。

7．交叉认证

在全球范围内建立一个容纳所有用户的单一 PKI 是不太可能实现的，可行的模型是建立多个 PKI 域，进行独立的运行和操作，为不同环境和不同行业的用户团体服务。

为在不同 PKI 之间建立信任关系，“交叉认证”的概念应运而生。在没有统一的全球 PKI 的环境下，交叉认证是一个可以接受的机制，因为它能够保证一个 PKI 团体的用户验证另一个团体的用户证书。总之，交叉认证是一种把以前无关的 CA 连接在一起的机制，从而使得它们在各自主体群间实现安全通信。

交叉认证方式以 CA 所在的域为标准，可分为域内交叉认证和域间交叉认证两种形式。如果两个 CA 属于相同的域，即在一个组织的 CA 层次结构中，某一层的 CA 认证下一层的 CA，这种处理方式被称为域内交叉认证。如果两个 CA 属于不同的域，即在一个公司中的 CA 认证在另一家公司中的 CA，这种处理方式被称为域间交叉认证。

交叉认证既可以是单向的，也可以是双向的。所谓单向认证，是指 CA1 可以交叉认证 CA2，但 CA2 却无法交叉认证 CA1。双向认证则是指 CA1 与 CA2 可以互相交叉认证，这种相互交叉认证需要两个不同的交叉证书。

在 X.509 标准中，对于交叉认证给出的定义是：从 CA1 的观点来看，把它当作主体，由其他 CA 来颁发证书，被称为“正向交叉证书”，被 CA1 颁发的证书则称为“反向交叉证书”。如果一个 X.500 目录被用作证书资料库，则正确的正向和反向交叉证书可以被存储在每个相关的 CA 目录项中的交叉证书对结构中，这个结构可以构造证书路径，如图 3-19 所示。

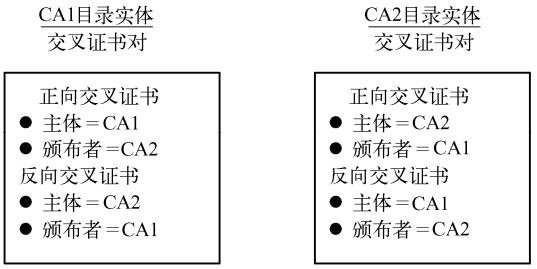


图 3-19　CA1 与 CA2 之间的相互交叉认证证书对

交叉认证的目的在于，在不同的群体中扩展信任，其方法有 3 类。

1）一个给定的 CA 可承认另一个 CA 在其所控制的范围内被授权颁发的证书。

2）允许不同的 PKI 域建立互操作路径。

3）交换根 CA 的密钥，并用外部域的根 CA 的密钥填充每个终端实体的软、硬件。

现举例说明如何使交叉认证能在不同的证书群体中扩展信任。假设：甲已被 CA1 认证，并持有一份可信的 CA1 的公钥，并且乙已经被 CA2 认证，也持有一份可信的 CA2 的公钥。最初，甲只信任其证书是由 CA1 签发的实体，因为甲能够验证这些证书。此时甲尚不能验证乙的证书，因为甲此时还没有持有一份可信的 CA2 的公钥。类似地，此时乙也不能验证甲的证书。然而，在 CA1 和 CA2 交叉认证之后，甲的信任能够扩展到 CA2 的包括乙在内的主体群，这是因为甲能够用其可信的 CA1 的公钥验证 CA2 的证书，然后用其现在信任的 CA2 的公钥验证乙的证书。

8．不可否认性

PKI 的不可否认性适用于从技术上保证实体对他们行为的不可否认性，即他们对自己发送和接收数据这个事实的不可抵赖性。如甲签发了某份文件，一段时间后他不能否认他对该文件进行了数字签名。

从数字签名的角度来说，一个公司或机构若需要用 PKI 支持不可否认性，则维护多密钥对和多个证书就非常必要。要真正支持不可否认性需要一个必要条件，那就是用户用于不可否认性操作的私钥不能被包括可信任实体 CA 在内的任何其他人知道。否则，实体就会随便地宣布这个操作不是本人所为，某些情况下这种私钥只能装载在防篡改的硬件加密模块中。

另一方面，不是用于不可否认性的密钥，如加密密钥，可备份在一个可信任机构（如

CA）中，甚至可以存放在软件里。正是由于这种冲突，一个 PKI 实体一般需要拥有两对或三对不同的密钥对及相关证书，一对用于加密和解密，一对用于普通的签名和认证，一对用于不可否认性的签名和认证。

9．时间戳

时间戳也称安全时间戳，是一个可信的时间权威用一段可认证的完整数据表示的时间戳（以格林尼治时间为标准的 32 位值）。重要的不是时间本身的精确性，而是相关日期时间的安全性。支持不可否认性服务的一个关键措施就是在 PKI 中使用时间戳，即时间源是可信的，它赋予的时间值必须被安全地传送。

PKI 中必须存在用户可信任的权威时间源，权威时间源的时间并不需要准确，重在为用户指明“参照”时间，以便完成基于 PKI 的事务处理。一般地，PKI 中都设置一个时钟系统，以便统一 PKI 的时间。当然，也可用世界官方时间源所提供的时间，甚至是网络上权威时间源发布的时间。当实体需要在数据上盖上时间戳时，就可向 PKI 权威时间源提出请求，一份文档的时间戳实质上就是文档内容和时间的杂凑值（Hash 值），即数字签名，它可为数据的真实性和完整性验证提供依据。

10．客户端软件

客户端软件是一个全功能、可操作 PKI 的必要组成部分。与常见的客户/服务器应用相同，只有客户端提出请求服务，服务器端才会对此请求做相应处理，这个原理同样适用于 PKI。客户端软件的主要功能有以下几个。

1）询问证书和相关的撤销信息。

2）在一定时刻为文档请求时间戳。

3）作为安全通信的接收点。

4）进行传输加密或数字签名。

5）执行取消操作。

6）证书路径处理。

客户端软件独立于所有应用程序，应用程序应通过标准接入点与客户端软件连接。

对 PKI 而言，这些应用程序是指客户端应用程序、协议引擎、数据库和操作系统等，它们都需要诸如认证、完整性、机密性和不可否认性等安全服务。为了在应用程序之间获得一致的安全性，客户端软件必须被置于一个单一的应用程序之外，可以被应用程序调用。

3.5.3 PKI 的特点

PKI 的主要特点包括以下几个。

1）节省费用。在一个大型的应用系统中，实现统一的安全解决方案，比起实施多个有限的解决方案，费用要少得多。

2）互操作性。在一个系统内部，实施多个点对点的解决方案，无法实现互操作性。在 PKI 中，每个用户程序和设备都以相同的方式访问和使用安全服务功能。

3）开放性。任何先进技术的早期设计，都希望在将来能与其他系统实现互操作，而一个专有的点对点技术方案不能处理多域间的复杂性，不具有开放性。

4）一致的解决方案。一致的解决方案在一个系统内更易于安装、管理和维护，并且开销小。

5）可验证性。PKI 在所有应用系统和设备之间所采用的交互处理方式都是统一的，因此，它的操作和交互都可以被验证是否正确。

6）可选择性。PKI 为管理员和用户提供了许多可选择性。

3.6 常用加密软件介绍

在日常工作和学习过程中，PGP（Pretty Good Privacy）软件及其免费代替产品 GnuPG 软件是两款常见的加密产品，下面主要介绍其功能、主要技术特点及使用方法。

3.6.1 PGP

1．PGP 简介

PGP 是一款基于 RSA 公钥加密体系的邮件加密软件，提出了公共钥匙或不对称文件加密和数字签名的方法。该软件的创始人是美国的 Phil Zimmermann，他创造性地把 RSA 公钥体系的方便和传统加密体系的高速结合起来，并且在数字签名和密钥认证管理机制上有巧妙的设计，因此 PGP 几乎成为目前最流行的公钥加密软件包。

由于美国对信息加密产品有严格的法律约束，特别是向美国、加拿大以外的其他国家散播、出售和发布该类软件的约束更为严格，因而限制了 PGP 的一些发展和普及，现在该软件的主要使用对象为情报机构、政府机构和信息安全工作者。PGP 最初的设计主要是用于邮件加密，如今已经发展到了可以加密整个硬盘、分区、文件及文件夹，甚至可以对 ICQ 等即时通信软件的聊天信息实时加密。

PGP 不是一种完全的非对称加密体系，它是一个混合加密算法，由一个对称加密算法（IDEA）、一个非对称加密算法（RSA）、一个单向散列算法（MD5）及一个随机数产生器（从用户击键频率产生伪随机数序列的种子）组成，每种算法都是 PGP 不可分割的组成部分。PGP 之所以流行，并得到广泛认可，最主要的就是它集成了几种加密算法的优点，使它们彼此得到互补。

2．PGP 的功能与使用

PGP 软件原来是美国 PGP 公司的产品，后来被 Symantec 公司收购，并更名为 Symantec Encryption Desktop，目前版本是 10.3，下面就以 Symantec Encryption Desktop 10.3 为例对其功能进行介绍。

Symantec Encryption Desktop 10.3 的主操作界面如图 3-20 所示，主要包括 PGP Keys、PGP Messaging、PGP Zip、PGP Disk、PGP Viewer 和 File Share Encryption 等几个功能模块。

其中，PGP Keys 模块主要负责密钥的生成与管理，PGP Messaging 模块主要完成邮件、即时消息等的加解密，PGP Zip 模块主要用来创建和查看压缩包，PGP Disk 模块主要用来创建和管理虚拟磁盘、加密磁盘或分区，PGP Viewer 模块主要完成加密邮件消息的解密与查看，File Share Encryption 模块主要完成文件或目录的加密分享。此外，Symantec Encryption Desktop 的 Shred Files 和 Shred Free Space 模块可以实现文件和磁盘空闲空间的安全擦除。下面仅对密钥创建和 PGP Disk 创建虚拟磁盘进行介绍，其他功能的使用可以参考该软件的帮助文档。

（1）创建 PGP Key

要使用 PGP 加密系统，首先要创建一对 PGP Key，方法是在 PGP Desktop 主界面上选择 File→New PGP Key 命令，在弹出对话框中按提示执行下一步操作，进入如图 3-21 所示的界面，输入用户名和邮件地址。此时可以通过单击 Advanced 按钮进一步设置密钥的类型、加密算法和密钥长度等信息。

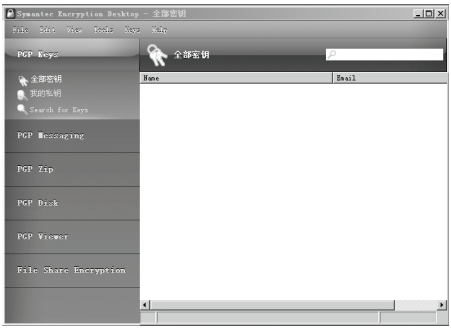


图 3-20　PGP 的操作界面

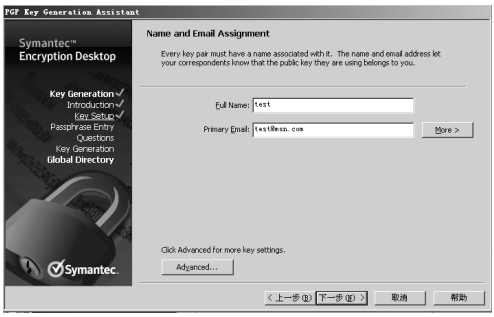


图 3-21　创建 PGP Key 的用户信息

单击“下一步”按钮，进入设置私钥保护密码界面，如图 3-22 所示。

根据提示执行余下操作即可以完成 PGP Key 的创建，如图 3-23 所示。在创建了 PGP Key 后，就可以利用该 PGP Key 进行各种加解密操作。

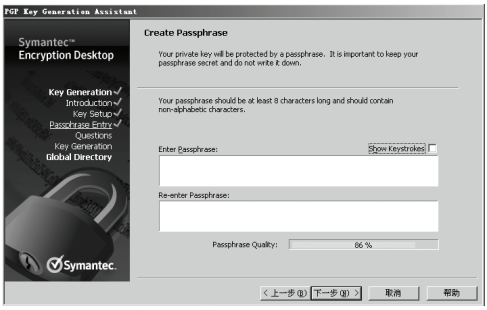


图 3-22　创建 PGP Key 的密码信息

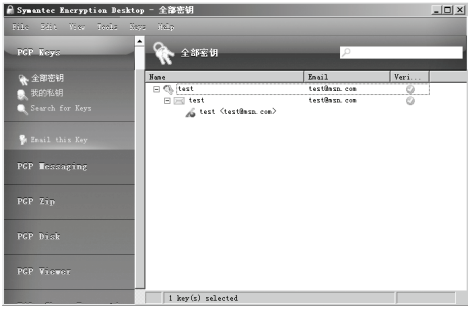


图 3-23　创建的 PGP Key

（2）创建 PGP Disk

创建 PGP Disk 的方法是在 PGP Desktop 主界面左侧功能导航栏中选择 New Virtual Disk，图 3-24 给出了创建的界面，其中要设置的内容主要包括虚拟盘的文件名、存储路径、挂载虚拟盘符、容量、分区格式、加密级别和选用密钥等信息。设置了所需信息后单击 Create 按钮，即可以完成 PGP Disk 的创建。

在创建完成 PGP Disk 后，会在图 3-24 指定目录下创建 New PGP Disk1.pgd 文件，在如图 3-25 所示的界面中，先选中创建的 New PGP Disk1.pgd，然后单击 mount 按钮，即可进行虚拟磁盘的加载，同时 mount 按钮变为 unmount 按钮，单击该按钮就可以卸载虚拟磁盘。在进行加载时会提示输入私钥的保护密码。

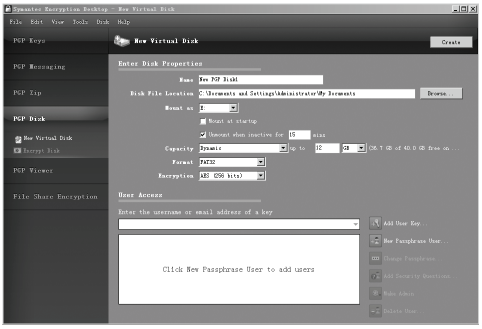


图 3-24　创建 PGP Disk

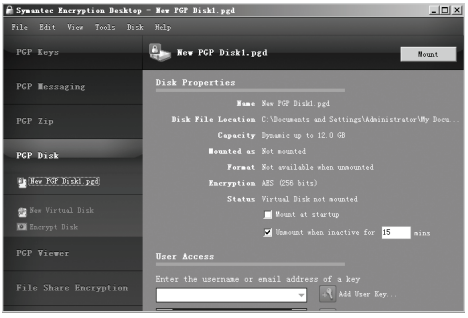


图 3-25　使用 PGP Disk

3.6.2 GnuPG

1．GnuPG 简介

GnuPG（http://www.gnupg.org）是 PGP 的免费代替软件。PGP 使用了 IDEA 等许多专利算法，属于美国加密出口限制产品。GnuPG 是 GPL 软件，并且没有使用任何专利加密算法，所以使用起来自由很多。作为 PGP 的替代产品，GnuPG 的技术特点主要包括以下几个。

- 完全兼容 PGP。
- 没有使用任何专利算法，无专利问题。
- 遵循 GNU 公共许可证。
- 支持多种加密算法。
- 支持扩展模块。
- 用户标识遵循标准结构。
- 多语言支持（包括简体中文）。
- 在线帮助系统。
- 拥有众多的 GUI 界面支持。

GnuPG 最初是运行在 UNIX 系列操作系统之上，现在已经可以在 Windows 系列操作系统上运行，目前的最新版本是 2.1.9。下面以 Windows 版本 GnuPG 为例介绍其功能和使用方法。

2．GnuPG 的功能与使用

（1）GnuPG 的安装

在 Windows 系统上安装 GnuPG 非常简单，只需到 GnuPG 网站下载并运行最新的安装包（目前为 gnupg-w32-2.1.9_20151009），然后按照提示即可完成安装过程。

（2）GnuPG 的主要功能

GnuPG 的主要功能可以通过在命令行窗口中执行 gpg –h 命令来查看。该命令的执行结果如下。

```
gpg –h
gpg (GnuPG) 2.1.9
libgcrypt 1.6.4
Copyright (C) 2015 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home：C:\Documents and Settings\Administrator\Application Data\gnupg
Supported algorithms：
Pubkey：RSA，ELG，DSA，ECDH，ECDSA，EDDSA
Cipher：IDEA，3DES，CAST5，BLOWFISH，AES，AES192，AES256，TWOFISH，
CAMELLIA128，CAMELLIA192，CAMELLIA256
Hash：SHA1，RIPEMD160，SHA256，SHA384，SHA512，SHA224
Compression：Uncompressed，ZIP，ZLIB，BZIP2

Syntax: gpg [options] [files]
Sign, check, encrypt or decrypt
Default operation depends on the input data

Commands:
```

```
  -s, --sign                  make a signature
      --clearsign             make a clear text signature
  -b, --detach-sign           make a detached signature
  -e, --encrypt               encrypt data
  -c, --symmetric             encryption only with symmetric cipher
  -d, --decrypt               decrypt data (default)
      --verify                verify a signature
  -k, --list-keys             list keys
      --list-sigs             list keys and signatures
      --check-sigs            list and check key signatures
      --fingerprint           list keys and fingerprints
  -K, --list-secret-keys      list secret keys
      --gen-key               generate a new key pair
      --quick-gen-key         quickly generate a new key pair
      --quick-adduid          quickly add a new user-id
      --full-gen-key          full featured key pair generation
      --gen-revoke            generate a revocation certificate
      --delete-keys           remove keys from the public keyring
      --delete-secret-keys    remove keys from the secret keyring
      --quick-sign-key        quickly sign a key
      --quick-lsign-key       quickly sign a key locally
      --sign-key              sign a key
      --lsign-key             sign a key locally
      --edit-key              sign or edit a key
      --passwd                change a passphrase
      --export                export keys
      --send-keys             export keys to a key server
      --recv-keys             import keys from a key server
      --search-keys           search for keys on a key server
      --refresh-keys          update all keys from a keyserver
      --import                import/merge keys
      --card-status           print the card status
      --card-edit             change data on a card
      --change-pin            change a card's PIN
      --update-trustdb        update the trust database
      --print-md              print message digests
      --server                run in server mode

Options:
  -a, --armor                 create ascii armored output
  -r, --recipient USER-ID     encrypt for USER-ID
  -u, --local-user USER-ID    use USER-ID to sign or decrypt
  -z N                        set compress level to N (0 disables)
      --textmode              use canonical text mode
  -o, --output FILE           write output to FILE
  -v, --verbose               verbose
  -n, --dry-run               do not make any changes
  -i, --interactive           prompt before overwriting
      --openpgp               use strict OpenPGP behavior
```

```
Examples:
  -se -r Bob [file]          sign and encrypt for user Bob
  --clearsign [file]         make a clear text signature
  --detach-sign [file]       make a detached signature
  --list-keys [names]        show keys
  --fingerprint [names]      show fingerprints
```

（3）生成密钥对

要生成密钥对，只需在命令行下执行 gpg --gen-key 命令，然后根据提示选择相应的选项即可完成。图 3-26 给出了一个生成名为 hacker 的密钥的过程。

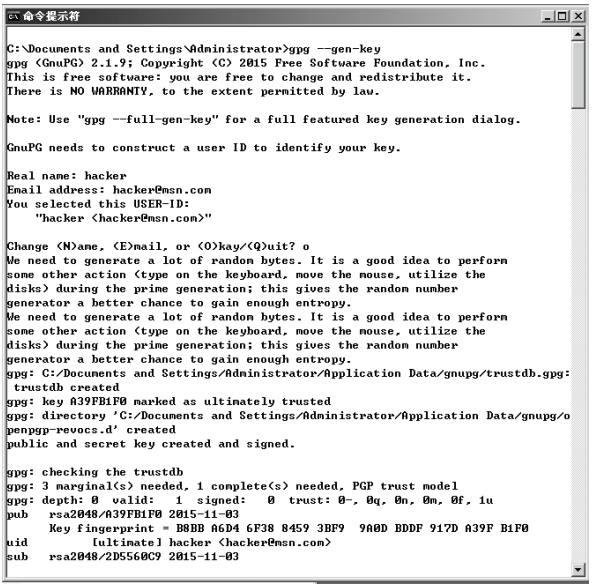


图 3-26　生成 GnuPG 密钥

可以通过 gpg --list-keys 命令查看当前的密钥列表，如图 3-27 所示。

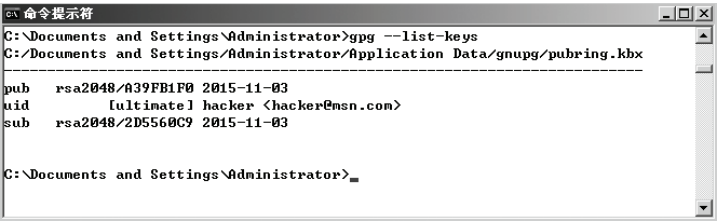


图 3-27　查看 GnuPG 密钥

（4）加密与解密

加密和解密一个文件非常容易，这里以密钥 hacker <hacker@msn.com>为例来进行说明，操作过程如图 3-28 所示。在测试前，首先创建一个内容为“GnuPG 测试”的文本文件 sn.txt。

其中，命令 gpg –ea –r hacker sn.txt 的功能是用 hacker 的公钥对 sn.txt 进行加密，并将密文以 ASCII 的方式输出到 sn.txt.asc。命令 gpg –d sn.txt.asc 对信息原文进行加密，此过程中会要求输入加密者 hacker 的私钥保护密码。其中，原文 sn.txt 与密文 sn.txt.asc 的内容如图 3-29 所示。

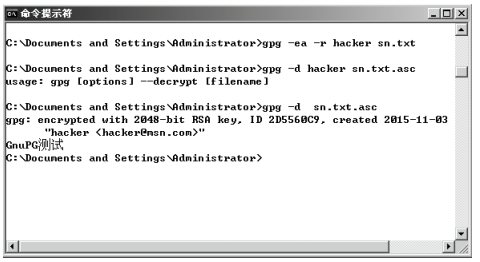


图 3-28　GnuPG 加密与解密

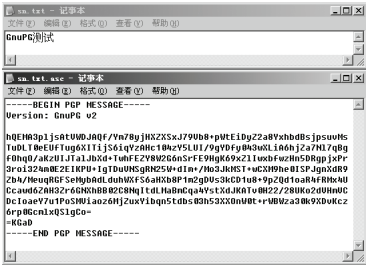


图 3-29　原文与密文

3.7　小结

信息加密是保障信息安全最核心的技术措施和理论基础，它采用密码学的原理与方法对信息进行可逆的数学变换，从而使非法接入者无法理解信息的真正含义，达到保证信息机密性的目的。信息加密算法共经历了古典密码、单钥密码体制（对称密钥密码）和双钥密码体制（公开密钥密码）3 个阶段，近年来云计算、电子商务等迅速发展，人们对同态加密的研究与应用日益重视。

古典密码是密码学的源头，常见的算法有：简单代替密码或单字母密码、多名或同音代替、多表代替，以及多字母或多码代替等。现代密码按照使用密钥方式的不同，可分为单钥密码体制和双钥密码体制两类。按照加密模式的差异，单钥密码体制有序列密码（也称流密码）和分组密码两种方式，它不仅可用于数据加密，还可用于消息认证，其中，最有影响的单钥密码是 DES 算法和 IDEA 算法。双钥密码体制的加密密钥和解密密钥不同，在网络通信中，主要用于认证（如数字签名、身份识别等）和密钥管理等，其杰出的算法有基于素数因子分解问题的 RSA 算法和基于离散对数问题的 ElGamal 算法。同态加密是一类具有特殊自然属性的加密方法，与一般加密算法相比，同态加密除了能实现基本的加密操作之外，还能实现密文间的多种计算功能，即先计算后解密等价于先解密后计算。

在网络安全领域，网络数据加密是解决通信网中信息安全的有效方法，网络数据加密常见的方式有链路加密、结点加密和端到端加密，以及一些同态加密典型应用等。其中，链路加密是对网络中两个相邻结点之间传输的数据进行加密保护，结点加密是指在信息传输路过的结点处进行解密和加密，端到端加密是指对一对用户之间的数据连续地提供保护。同态加密可对密文数据进行直接运算，而不会破坏对应明文信息的完整性和保密性，对密文的操作等价于对明文实施相应操作之后再加密。

在认证技术领域，通过使用密码手段，一般可实现 3 个目标，即消息完整性认证、身份认证，以及消息的序号和操作时间（时间性）等认证。认证技术模型在结构上由安全管理协议、认证体制和密码体制 3 层组成。

PKI 是一个采用公钥密码算法原理和技术来提供安全服务的通用性基础平台，用户可利用 PKI 平台提供的安全服务进行安全通信，PKI 采用标准的密钥管理规则，能够为所有应用透明地提供采用加密和数字签名等密码服务所需要的密钥和证书管理。PKI 在组成上主要包括认证机构 CA、证书库、密钥备份、证书作废处理系统和 PKI 应用接口系统等。

PGP 和 GnuPG 是两个常用的公钥加密软件，PGP 软件被 Symantec 公司收购后，已经融入其产品体系，形成了 Symantec Encryption 解决方案，GnuPG 作为 PGP 的代替软件，属于开

源免费软件，可以自由使用。

3.8 习题

1．简述信息加密技术对于保障信息安全的重要作用。
2．简述加密技术的基本原理，并指出有哪些常用的加密体制及其代表算法。
3．试分析古典密码对于构造现代密码有哪些启示。
4．选择凯撒（Caesar）密码系统的密钥 k=6，若明文为 Caesar，密文是什么？
5．DES 加密过程有哪几个基本步骤，试分析其安全性能。
6．在本章 RSA 实例的基础上，试给出 m=student 的加解密过程。
7．RSA 签名方法与 RSA 加密方法对密钥的使用有什么不同？
8．试简述网络数据加密中的链路加密、结点加密和端到端加密方式。
9．试简述同态加密技术在云计算中的典型应用方式。
10．认证的目的是什么？试简述认证技术相互间的区别。
11．什么是 PKI？其用途有哪些？
12．简述 PKI 的功能模块组成。
13．通过学习，你认为密码技术在网络安全实践中还有哪些重要应用领域，请举例说明。