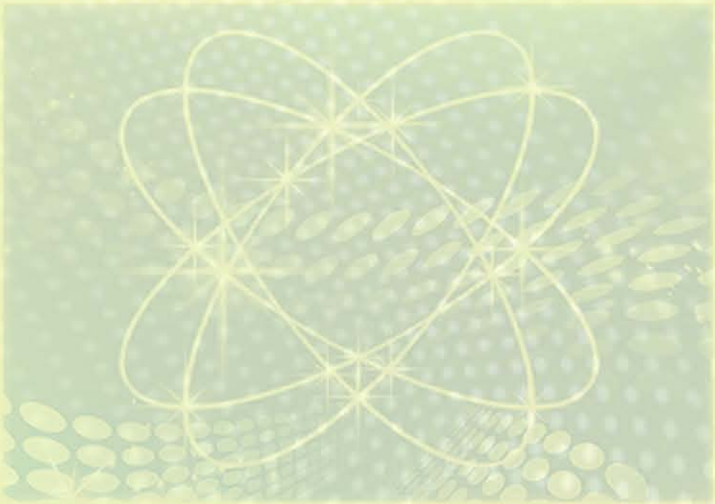
网络安全运行与维护

穆德恒　主编



北京理工大学出版社

网络安全运行与维护

主　编　穆德恒

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

内 容 提 要

本书系统地介绍了网络安全运行所需的基础知识和部分主要的应用技术。本书以安全漏洞为主线，主要内容包括计算机信息加密的原理、操作系统的安全及漏洞、网络协议的分析与安全漏洞、网络漏洞后门的利用、数据库的攻击与渗透等。在每章中，根据理论知识，设计实践内容，力求合理地将理论和实践进行有机结合，帮助学生顺利掌握网络安全运维所需的技能。

本书内容丰富，结构合理清晰，语言通俗易懂；注重网络安全运维的知识和实践应用相结合，力求通过实践帮助学生循序渐进地学好网络安全运维的主要技术。本书可作为普通高等院校计算机网络课程的教材，同时也可供广大网络技术人员参考使用。

图书在版编目(CIP)数据

网络安全运行与维护 / 穆德恒主编. -- 北京 : 北京理工大学出版社，2021.10

ISBN 978-7-5763-0510-4

Ⅰ.①网… Ⅱ.①穆… Ⅲ.①网络安全－教材 Ⅳ.①TP915.08

中国版本图书馆CIP数据核字（2021）第211209号

出版发行 / 北京理工大学出版社有限责任公司

社　　址 / 北京市海淀区中关村南大街5号

邮　　编 / 100081

电　　话 / （010）68914775（总编室）

（010）82562903（教材售后服务热线）

（010）68948351（其他图书服务热线）

网　　址 / http://www.bitpress.com.cn

经　　销 / 全国各地新华书店

印　　刷 / 河北鑫彩博图印刷有限公司

开　　本 / 787毫米×1092毫米　1/16

印　　张 / 16　　责任编辑 / 阎少华

字　　数 / 405千字　　文案编辑 / 阎少华

版　　次 / 2021年10月第1版　2021年10月第1次印刷　　责任校对 / 周瑞红

定　　价 / 69元　　责任印制 / 边心超

Preface
前言

本书根据网络技术发展，及时更新知识，在内容和结构上做了细致安排，较多地从实践性和可操作性上仔细描述，从先进性和实用性出发，以网络协议中存在的安全漏洞为主线，介绍了信息加密的方法、操作系统的安全漏洞、TCP/IP协议、局域网、广域网等技术知识。本书侧重于实际应用和动手能力的培养，以提高学习者分析问题、解决问题的能力。本书叙述简明扼要，通俗易懂，实用性强，学做合一，并提供实验操作内容。

本书第1章概要介绍网络安全以及网络安全运维的关键点；第2章主要介绍计算机对称加密、非对称加密、散列函数、证书签名等重要基础知识；第3章主要介绍Windows操作系统、Linux操作系统的安全配置知识；第4章简单介绍了网络协议存在的先天漏洞及如何补救；第5章介绍了网络漏洞扫描、渗透攻击的方法及如何防护；第6章介绍数据库SQL注入知识，主要以MySQL数据库为例讲解了如何渗透和防护。

教学实施时，可根据教学计划规定的学时数和教学大纲的要求，灵活选取内容。

本书由穆德恒主编并统一筹划与安排。

书中不妥之处在所难免。殷切希望广大读者提出宝贵意见，以使教材不断完善。

编　者

Contents
目录

Contents

第 1 章

网络安全概述

案例导入

某公司报案称，有人在网上大量出售该公司开发的某游戏用户账户。侦查后发现，犯罪分子通过盗取游戏账户，并按游戏角色的等级定价后，批量售卖。警方通过缜密侦查成功抓获 2 名犯罪分子，此案共缴获各类邮箱账户密码 30 余万条，取缔平台 2 个，并成功端掉一个非法售卖账户的网络黑产业链。

此案的发生源于大批量邮箱密码泄露事件。密码安全是信息安全的核心，但是在当今的网络环境中，相当一部分人并不重视账户密码的设置及保管，突出表现在不修改默认密码，采用弱密码、单一密码全平台通用等问题上。这导致了犯罪分子轻易盗取某一平台用户账户后，再进行多平台账户关联，使用户遭到更严重的损失。

所需知识

网络产生的初衷是实现电子数据资源的共享及备份，在最初的构建过程中没有考虑安全的要素，所以很多网络协议虽然可以很好地进行通信工作，但是天生存在安全的缺陷，所以可以被人利用做违反法律和道德的事情。本章主要介绍几个违反网络安全的实例，同时也总结出网络安全的重要性及需要注意的内容。

1.1 认识网络安全的重要性

1.1.1 网络安全的概念和内容

网络安全，通常指计算机网络的安全，实际上也可以指计算机通信网络的安全。计算机通信网络是将若干台具有独立功能的计算机通过通信设备及传输媒体互连起来，在通信软件的支持下，实现计算机间的信息传输与交换的系统。而计算机网络是指以共享资源为目的，利用通信手段把地域上相对分散的若干独立的计算机系统、终端设备和数据设备连接起来，并在协议的控制下进行数据交换的系统。计算机网络的根本目的在于资源共享，通信网络是实现网络资源共享的途径，因此，若要计算机网络是安全的，相应的计算机通信网络也必须是安全的，应该能为网络用户实现信息交换与资源共享。下文中，网络安全既指计算机网络安全，又指计算

机通信网络安全。

安全的基本含义：客观上不存在威胁，主观上不存在恐惧。即客体不担心其正常状态受到影响。网络安全定义：一个网络系统不受任何威胁与侵害，能正常地实现资源共享功能。要使网络能正常地实现资源共享功能，首先要保证网络的硬件、软件能正常运行，然后要保证数据信息交换的安全。由于资源共享的滥用，导致了网络的安全问题。因此网络安全的技术途径就是要实行有限制的共享。

1.1.2 网络空间安全威胁的发展态势

随着计算机技术的飞速发展，信息网络已经成为社会发展的重要保证。网络信息有很多是敏感信息，甚至是国家机密，所以难免会吸引来自世界各地的各种人为攻击(例如信息泄漏、信息窃取、数据篡改、数据删添、计算机病毒等)。同时，网络实体还要经受诸如水灾、火灾、地震、电磁辐射等方面的考验。

1. 国外

2012 年 2 月 4 日，黑客集团 Anonymous 公布了一份来自 1 月 17 日美国 FBI 和英国伦敦警察厅的工作通话录音，时长 17 分钟，主要内容是双方讨论如何寻找证据和逮捕 Anonymous、LulzSec、Antisec、CSL Security 等黑帽子黑客的方式。FBI 已经确认了该通话录音的真实性。

2012 年 2 月 13 日，据称一系列美国政府网站均遭到了 Anonymous 组织的攻击，而其中 CIA 官网周五被黑长达 9 小时。

2. 国内

2011 年 12 月 21 日，国内知名程序员网站 CSDN 遭到黑客攻击，大量用户数据库被公布在互联网上，600 多万个明文的注册邮箱被迫裸奔。

2011 年 12 月 29 日下午消息，继 CSDN、天涯社区用户数据泄露后，互联网行业人心惶惶，而在用户数据最为重要的电商领域，也不断传出存在漏洞、用户泄露的消息，漏洞报告平台乌云昨日发布漏洞报告称，支付宝用户大量泄露，被用于网络营销，泄露总量达 1 500 万～2 500 万之多，泄露时间不明，里面只有支付用户的账户，没有密码。已经被卷入的企业有京东商城、支付宝和当当网，其中京东及支付宝否认信息泄露，而当当表示已经向当地公安报案。

未来二三十年，信息战在军事决策与行动方面的作用将显著增强。在诸多决定性因素中包括以下几点：互联网、无线宽带及射频识别等新技术的广泛应用；实际战争代价高昂且不得人心，以及这样一种可能性，即许多信息技术可秘密使用，使黑客高手能够反复打进对手的计算机网络。

据网易、中搜等媒体报道，为维护国家网络安全、保障中国用户合法利益，我国即将推出网络安全审查制度。该项制度规定，关系国家安全和公共安全利益的系统使用的重要信息技术产品和服务，应通过网络安全审查。审查的重点在于该产品的安全性和可控性，旨在防止产品提供者利用提供产品的方便，非法控制、干扰、中断用户系统，非法收集、存储、处理和利用用户有关信息。对不符合安全要求的产品和服务，将不得在中国境内使用。

近几年，几起大型数据隐私丑闻，有平台方面的漏洞造成的结果，也有事务处理不严谨造成的漏洞。网络数据安全从来不是一劳永逸的事情，人们在享受网络给生活带来便利的同时，也需要不断地学习，提高网络自身及其上面所承载的数据的安全。

了解各国网络安全部队，可阅读图 1.1～图 1.3 中所示资料。

图 1.1　美国国家网络安全部队

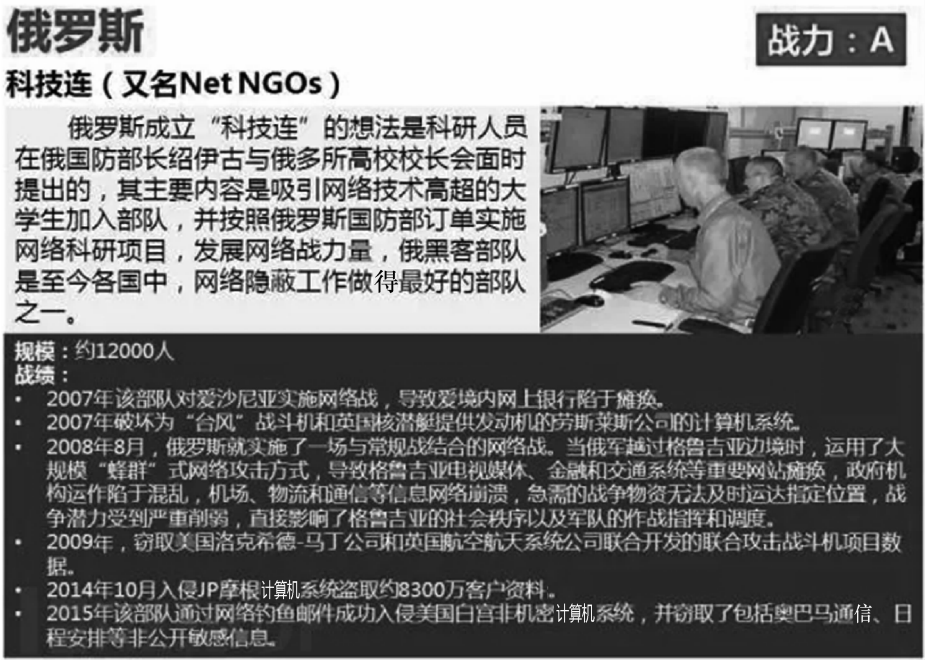


图 1.2　俄罗斯国家网络安全部队

图 1.3　以色列国家网络安全部队

1.2　总结网络安全问题的产生原因

1.2.1　网络安全威胁的种类及途径

1. 安全隐患

(1)Internet 是一个开放的、无控制机构的网络，黑客(Hacker)经常会侵入网络中的计算机系统，或窃取机密数据和盗用特权，或破坏重要数据，或使系统功能得不到充分发挥直至瘫痪。

(2)Internet 的数据传输是基于 TCP/IP 通信协议进行的，这些协议缺乏使传输过程中的信息不被窃取的安全措施。

(3)Internet 上的通信业务多数使用 Unix 操作系统来支持，Unix 操作系统中明显存在的安全脆弱性问题会直接影响安全服务。

(4)在计算机上存储、传输和处理的电子信息，还没有像传统的邮件通信那样进行信封保护和签字盖章。信息的来源和去向是否真实，内容是否被改动，以及是否泄露等，在应用层支持的服务协议中是凭着君子协定来维系的。

(5)电子邮件存在着被拆看、误投和伪造的可能性。使用电子邮件来传输重要机密信息存在着很大的危险。

(6)计算机病毒通过 Internet 的传播给上网用户带来极大的危害，病毒可以使计算机和计算机网络系统瘫痪、数据和文件丢失。在网络上传播病毒可以通过公共匿名 FTP 文件传送，也可以通过邮件和邮件的附加文件传播。

2. 攻击形式

网络攻击形式主要有中断、截获、修改和伪造四种。

(1)中断是以可用性作为攻击目标，它毁坏系统资源，使网络不可用。

(2)截获是以保密性作为攻击目标，非授权用户通过某种手段获得对系统资源的访问。

(3)修改是以完整性作为攻击目标，非授权用户不仅获得访问而且对数据进行修改。

(4)伪造是以完整性作为攻击目标，非授权用户将伪造的数据插入正常传输的数据。

3. 主要类型

网络安全由于不同的环境和应用而产生了不同的类型，主要有以下几种：

(1)系统安全。运行系统安全即保证信息处理和传输系统的安全。它侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的消息造成破坏和损失；避免由于电磁泄漏，产生信息泄露，干扰他人或受他人干扰。

(2)网络信息安全。网络上系统信息的安全，包括用户口令鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，安全问题跟踪，计算机病毒防治，数据加密等。

(3)信息传播安全。网络上信息传播安全，即信息传播后果的安全，包括信息过滤等。它侧重于防止和控制由非法、有害的信息进行传播所产生的后果，避免公用网络上大量自由传播的信息失控。

(4)信息内容安全。网络上信息内容的安全，侧重于保护信息的保密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。其本质是保护用户的利益和隐私。

1.2.2　网络安全风险及隐患分析

广义的网络安全涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论等领域。随着计算机技术的不断发展，基于网络连接的安全问题日益突出，甚至给人们的生活、工作造成巨大经济损失。尤其是病毒的侵袭、黑客的非法闯入、数据“窃听”、拦截和拒绝服务等网络攻击更是让人们防不胜防。总体而言，计算机网络安全主要表现在网络的物理安全、拓扑结构安全、系统安全、应用系统安全和网络管理安全等方面。

首先，系统安全。所谓系统安全是指网络操作系统、应用系统的安全问题。就目前我们的应用系统来看，只是处于一种相对安全状态。因为任何一个操作系统必然会有后门(Back-Door)，这也就让系统必然存在漏洞，漏洞也就是安全隐患的根源，而漏洞永远无法根除，这也就让每一个操作系统无法摆脱安全隐患的困扰。

其次，应用系统的安全。在计算机网络中，应用系统是不断发展变化的，也是动态的。应用系统的安全性涉及面较广，如增加一个新的应用系统，就会出现新的漏洞，而此时就需在安全策略上进行一定的调整，不断完善系统的漏洞，大量的补丁也就随之出现。就计算机应用系统的安全性而言，重点是在系统平台的安全上。要保证一个系统的正常运行，就需以专业的安全工具对应用系统进行监控，不断发现存在的漏洞，从而修补漏洞，让攻击者无法在未授权的情况下访问或对系统进行破坏，以提高系统的安全性。

从计算机网络安全管理上看，这是计算机网络安全最重要的内容，因其中涉及信息的安全

和机密信息的泄露、未经授权的访问、破坏信息的完整性、假冒信息、破坏信息的可用性等内容，一旦信息管理出现问题，就可能被攻击者窃取、破坏，从而给信息所有者带来经济上的损失或不良影响。而要加强网络信息管理，就需对用户使用计算机进行身份认证，对于重要信息的通信必须授权，传输必须加密。这样，当网络中出现攻击行为或网络受到威胁时，或在网络受到攻击后，可根据使用计算机的用户身份进行追踪，提高网络的可控性和审查性，让非法入侵行为得到一定的控制。

1.3 理解网络安全的内涵

网络通信具有全程全网联合作业的特点。就通信而言，它由五大部分组成：传输和交换、网络标准、协议和编码、通信终端、通信信源。这五大部分都会遭到严重的威胁和攻击，都会成为对网络和信息的攻击点。而在网络中，保障信息安全是网络安全的核心。网络中的信息可以分成用户信息和网络信息两大类。

1. 用户信息

在网络中，用户信息主要指面向用户的话音、数据、图像、文字和各类媒体库的信息，它大致有以下几种：

一般性的公开信息：如正常的大众传媒信息、公开性的宣传信息、大众娱乐信息、广告性信息和其他可以公开的信息。

个人隐私信息：如纯属个人隐私的民用信息，应保障用户的合法权益。

知识产权保护的信息：如按国际上签订的《建立世界知识产权组织公约》第二条规定的保护范围，应受到相关法律保护。

商业信息：包括电子商务、电子金融、证券和税务等信息。这种信息包含大量的财和物，是犯罪分子攻击的重要目标，应采取必要措施进行安全防范。

不良信息：主要包括涉及政治、文化和伦理道德领域的不良信息，还包括称为“信息垃圾”的无聊或无用信息，应采取一定措施过滤或清除这种信息，并依法打击犯罪分子和犯罪集团。

攻击性信息：它涉及各种人为的恶意攻击信息，如国内外的“黑客”攻击、内部和外部人员的攻击、计算机犯罪和计算机病毒信息。这种针对性的攻击信息危害很大，应当重点进行安全防范。

保密信息：按照国家有关规定，确定信息的不同密级，如秘密级、机密级和绝密级。这种信息涉及政治、经济、军事、文化、外交等各方面的秘密信息，是信息安全的重点，必须采取有效措施给予特殊的保护。

2. 网络信息

在网络中，网络信息与用户信息不同，它是面向网络运行的信息。网络信息是网络内部的专用信息。它仅向通信维护和管理人员提供有限的维护、控制、检测和操作层面的信息资料，其核心部分仍不允许随意访问。特别应当指出，当前对网络的威胁和攻击不仅是为了获取重要的用户机密信息，得到最大的利益，还把攻击的矛头直接指向网络本身。除对网络硬件攻击外，还会对网络信息进行攻击，严重时能使网络陷于瘫痪，甚至危及国家安全。网络信息主要包括以下几种：

通信程序信息：由于程序的复杂性和编程的多样性，而且常以人们不易读懂的形式存在，所以在通信程序中很容易预留下隐藏的缺陷、病毒，隐蔽通道和植入各种攻击信息。

操作系统信息：在复杂的大型通信设备中，常采用专门的操作系统作为其硬件和软件应用程序之间的接口程序模块。它是通信系统的核心控制软件。由于某些操作系统的安全性不完备，会招致潜在的入侵，如非法访问、访问控制的混乱、不完全的中介和操作系统缺陷等。

数据库信息：在数据库中，既有敏感数据又有非敏感数据，既要考虑安全性又要兼顾开放性和资源共享。所以，数据库的安全性，不仅要保护数据的机密性，重要的是必须确保数据的完整性和可用性，即保护数据在物理上、逻辑上的完整性和元素的完整性，并在任何情况下，包括灾害性事故后，都能提供有效的访问。

通信协议信息：协议是两个或多个通信参与者(包括人、进程或实体)为完成某种功能而采取的一系列有序步骤，使得通信参与者协调一致地完成通信联系，实现互连的共同约定。通信协议具有预先设计、相互约定、无歧义和完备的特点。在各类网络中已经制定了许多相关的协议。如在保密通信中，仅仅进行加密并不能保证信息的机密性，只有正确地进行加密，同时保证协议的安全才能实现信息的保密。然而，协议的不够完备，会给攻击者以可乘之机，造成严重的恶果。

电信网的信令信息：在网络中，信令信息的破坏可导致网络的大面积瘫痪。为信令网的可靠性和可用性，全网应采取必要的冗余措施，以及有效的调度、管理和再组织措施，以保证信令信息的完整性，防止人为或非人为的篡改和破坏，防止对信令信息的主动攻击和病毒攻击。

数字同步网的定时信息：我国的数字同步网采用分布式多地区基准钟(LPR)控制的全同步网。LPR 系统由铷钟加装两部全球定位系统(GPS)组成，或由综合定时供给系统 BITS 加上 GPS 组成。在北京、武汉、兰州三地设立全国的一级标准时钟(PRC)，采用铯钟组定时作为备用基准，GPS 作为主用基准。为防止 GPS 在非常时期失效或基准精度下降，应加强集中检测、监控、维护和管理，确保数字同步网的安全运行。

网络管理信息：网络管理系统是涉及网络维护、运营和管理信息的综合管理系统。它集高度自动化的信息收集、传输、处理和存储于一体，集性能管理、故障管理、配置管理、计费管理和安全管理于一身，对于最大限度地利用网络资源，确保网络的安全具有重要意义。安全管理主要包括系统安全管理、安全服务管理、安全机制管理、安全事件处理管理、安全审计管理和安全恢复管理等内容。

本章小结

本章主要介绍网络安全内涵及几个安全事例，从网络安全的重要性谈起，总结了网络安全威胁的种类及途径，分析了网络安全的风险及隐患。

课后学习任务

1. 请列举几个威胁网络安全的实例。
2. 威胁网络安全的要素有哪些?
3. 如何评估一个网站的安全风险。

第 2 章

信息加密的方法及应用

案例导入

刘先生要把一份广告创意方案书通过电子邮件发给其外地客户张女士，出于商业机密性考虑，为了保护这份方案书，刘先生想到了你——网络安全工程师，并提出如下需求：要保护这份方案书通过互联网传到张女士的过程中不被其他人看到(机密性保护)(图 2.1)；同时，要保证这份方案书传输过程中不被其他人修改或破坏(完整性保护)；最后还要保证被张女士收到后能确认是刘先生发送的(源认证保护)。请你提供有效的技术并加以实施，以满足刘先生的三方面的要求。

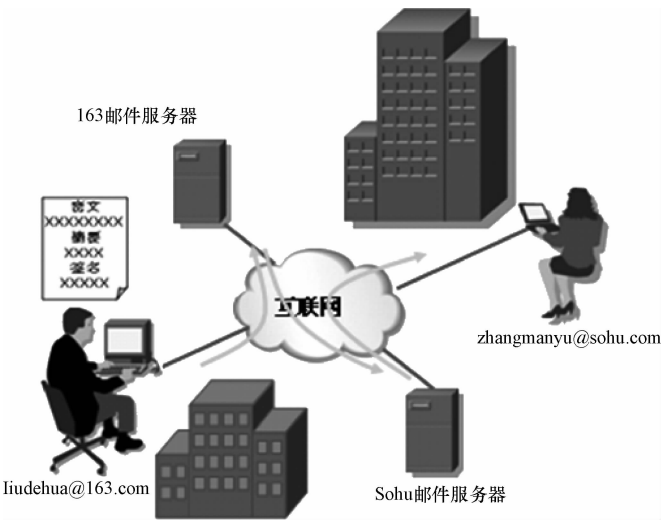


图 2.1　发送广告创意方案书

所需知识

1. 网络安全的保证离不开密码学的支持，正是因为把密码学的算法应用到网络信息的通信上，使明文的信息变为密文，从而保证了通信的安全，即信息的机密性。对应知识点为对称加密和非对称加密。

2. 在通信过程中还要考虑到信息是否被篡改过，即信息的完整性。对应的知识点为哈希函数。

3. 接收方对发送方身份的确认，即信息的可靠性。对应的知识点为数字签名。

2.1　了解加密通信的基本概念

加密通信的基本过程如图 2.2 所示。

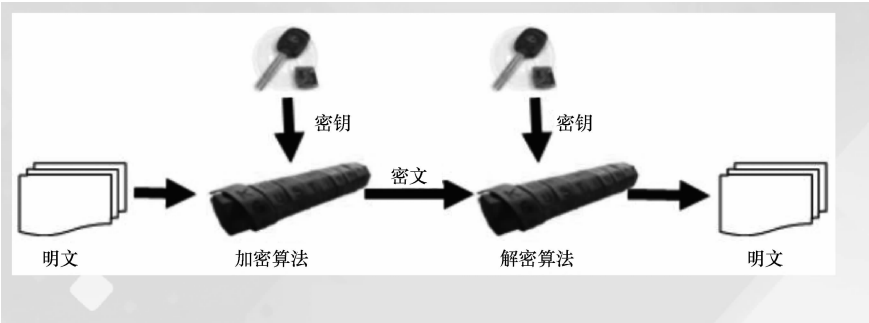


图 2.2　加密通信的基本过程

2.1.1　加密通信的概念

明文消息(Plaintext)：未加密的原消息，简称明文。

密文消息(Ciphertext)：加密后的消息，简称密文。

截收者(Eavesdropper)：非法授权者通过各种办法，如搭线窃听、电磁窃听、声音窃听等来窃取信道中机密信息者。

加密(Encipher、Encode)：明文到密文的变换过程。

解密(Decipher、Decode)：密文到明文的恢复过程。

加密算法(Encryption Algorithm)：对明文进行加密时所采用的一组规则的集合。

解密算法(Decryption Algorithm)：对密文进行解密时所采用的一组规则的集合。

密码算法强度(Algorithm Strength)：对给定密码算法的攻击难度。

密钥(Key)：加解密过程中只有发送者和接收者知道的关键信息，分为加密密钥(Encryption Key)和解密密钥(Decryption Key)。

2.1.2　密码体系

1. 对称密码体系(Symmetric Cryptosystem)

对称密码体系又称为私钥(Private Key)或单钥(One－Key)或传统(Classical)密码体系。在对称密码体系中，加密密钥和解密密钥是一样的或者彼此之间是容易相互确定的。私钥密码体系按加密方式可分为流密码(Stream Cipher)和分组密码(Block Cipher)2 种。

2. 非对称密码体系(Asymmetric Cryptosystem)

非对称密码体系又称为公钥(Public Key)或双钥(Two-Key)密码体系。在公钥密码体系中，加密密钥和解密密钥不同，从一个难于推出另一个，可将加密能力和解密能力分开。

3. 密码体系的基本类型

错乱：按照规定的图形和线路，改变明文字母或数码等的位置成为密文。

替换：用一个或多个代替表将明文字母或数码等代替为密文。

密本：用预先编定的字母或数字编码组，代替一定的词组单词等明文为密文。

加乱：用有限元素组成的一串序列全为乱数，按规定的算法，同明文序列相结合变成密文。

问题：Caser 密码、Stycle 棒、栅栏密码属于上述哪一种？

4. Kerckhoffs 准则

Kerckhoffs(柯克霍夫)早在 1883 年就指出，密码算法的安全性必须建立在密钥保密的基础上，即使敌手(Opponent)知道算法，若不掌握特定密钥也应难以破解密码，这就是著名的 Kerckhoffs 准则。

2.1.3 加密技术发展的历史

第一阶段：古代到 1949 年。

这阶段的密码技术可以说是一种艺术，而不是一种科学，密码学专家常常是凭知觉和信念来进行密码设计和分析而不是推理和证明。这阶段发明的密码算法在现代计算机技术条件下都是不安全的。

第二阶段：1949 年到 1976 年。

1949 年 C. E. Shnnon(香农)发表在《贝尔实验室技术》杂志上的 *Communication Theory of Secrecy System*(保密系统的信息理论)为私钥密码体系(对称加密)建立了理论基础，从此密码学成为一门科学。

1967 年 David Kahn 发表了 *The Code Breakers*(《破译者》)。

1976 年，Pfister 和美国国家安全局 NSA(National Security Agency)一起制定了 DES 标准，这是一个具有深远影响的分组密码算法。

第三阶段：1976 年至今。

1976 年 Diffie 和 Hellman(图 2.3)发表的文章“密码学的新动向”一文导致了密码学上的一场革命。他们首先证明了在发送端和接收端无密钥传输的保密通信是可能的，从而开创了公钥密码学的新纪元。从此，密码开始充分发挥它的商用价值和社会价值。

1978 年，在 ACM 通信中，Rivest、Shamir 和 Adleman(图 2.4)公布了 RSA 密码体系，这是第一个真正实用的公钥密码体系，可以用于公钥加密和数字签名。由于 RSA 算法对计算机安全和通信的巨大贡献，该算法的 3 个发明人因此获得计算机界的诺贝尔奖——A. M. Turing Award(图灵奖)。

图 2.3 Diffie(右)、Hellman and Markle(左)

图 2.4 RSA 公开密钥算法的发明人，从左到右 Ron Rivest、Adi Shamir 和 Leonard Adleman

为了对付美国联邦调查局 FBI(Federal Bureau of Investigation)对公民通信的监控，Philip Zimmermann 在 1991 年发布了基于 IDEA 的免费邮件加密软件 PGP。

PGP(Pretty Good Privacy)，是一个基于 RSA 公匙加密体系的邮件加密软件，可以用它对邮件加密以防止非授权者阅读。它还能对邮件加上数字签名从而使收信人可以确信邮件是签名人发来的。它让用户可以安全地和从未见过的人们通信，事先并不需要任何保密的渠道用来传递密匙。它采用了：审慎的密匙管理，一种 RSA 和传统加密的杂合算法，用于数字签名的邮件文摘算法，加密前压缩等，还有一个良好的人机工程设计。它的功能强大，有很快的速度。而且它的源代码是免费的。

PGP 加密软件是采用公开密钥加密与传统密钥加密相结合的一种加密技术。它使用一对数学上相关的钥匙，其中一个(公钥)用来加密信息，另一个(私钥)用来解密信息。PGP 采用的传统加密技术部分所使用的密钥称为“会话密钥”(sek)。每次使用时，PGP 都随机产生一个 128 位的 IDEA 会话密钥，用来加密报文。公开密钥加密技术中的公钥和私钥则用来加密会话密钥，并通过它间接地保护报文内容。

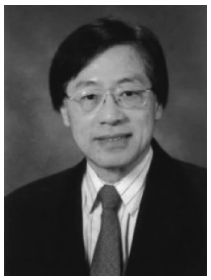


图 2.5　姚期智

现代密码学的另一个主要标志是基于计算机复杂度理论的密码算法安全性证明。清华大学姚期智教授(图 2.5)在保密通信计算复杂度理论上有重大的贡献，并因此获得 2000 年度图灵奖。

随着计算能力的不断增强，现在 DES(对称数据加密系统)已经变得越来越不安全。1997 年美国国家标准学会 ANSI(American National Standards Institute)公开征集新一代分组加密算法，并于 2000 年选择 Rijndael 作为高级加密算法 AES(Advanced Encryption Standard)以取代 DES。

在实际应用方面，古典密码算法有替代加密、置换加密；对称加密算法包括 DES 和 AES；非对称加密算法包括 RSA、背包密码、Rabin、椭圆曲线等。此外还有辫子密码、量子密码、混沌密码、DNA 密码等新的密码技术。目前在数据通信中使用最普遍的算法有 DES 算法和 RSA 算法(图 2.6)等。

图 2.6　RSA 算法工作过程

2.1.4　密码体系举例

1. Caser 密码

已知字母与数字对应表见表 2.1。

表 2.1　字母与数字对应表

字母	a	b	c	d	e	f	g	h	i	j	k	l	m
数字	0	1	2	3	4	5	6	7	8	9	10	11	12
字母	n	o	p	q	r	s	t	u	v	w	x	y	z
数字	13	14	15	16	17	18	19	20	21	22	23	24	25