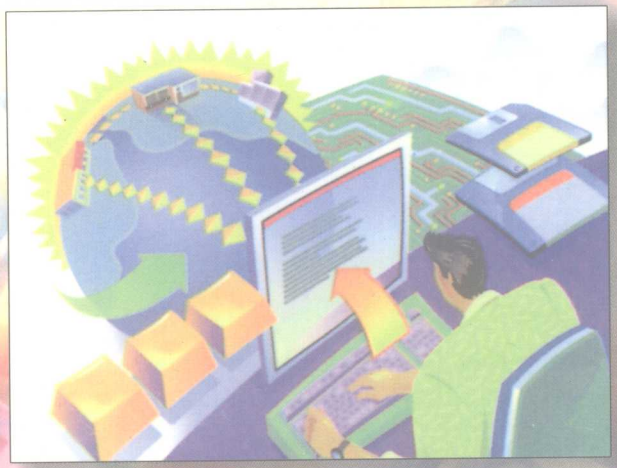
实用密码学与计算机数据安全

主编　李克洪　王大玲　董晓梅



NEUPRESS
东北大学出版社

实用密码学与计算机数据安全

主编　李克洪　王大玲　董晓梅

东北大学出版社

内 容 提 要

本书介绍了实用密码技术和计算机数据安全方面的知识。全书共分13章，包括密码学的数学基础、传统加密算法、对称密钥加密算法、公开密钥加密算法、序列密码算法、密码协议、密钥管理及算法模式、密码学的实际应用、安全操作系统、数据库安全、Internet安全以及计算机病毒方面的内容。该书是作者在查阅了大量中、外文参考文献的基础上，结合几年来的教学、科研实践编写而成的，具有范围广、内容新的特点。本书可做为计算机专业和通信工程专业学生、研究生的教材，也可供从事计算机安全保密研究的人员参阅。

图书在版编目(CIP)数据

实用密码学与计算机数据安全/李克洪，王大玲，董晓梅主编 .—沈阳：东北大学出版社，01.9(2002.9)
ISBN 7-81054-268-0

Ⅰ.实… Ⅱ.①李… ②王… ③董… Ⅲ.①密码-理论 ②电子计算机-安全技术 .TP309

中国版本图书馆CIP数据核字(2001)第060872号

(沈阳市和平区文化路3号巷11号 邮政编码 110004)
电话：(024)83680265 传真：(024)83680267
网址：http://www.neupress.com E-mail：neuph@neupress.com
东北大学印刷厂印刷 东北大学出版社发行

开本：787mm×1092mm 1/16 字数：552千字 印张：22.125
印数：3001～6000册
2001年9月第2版 2002年9月第2次印刷

责任编辑：李毓兴 责任校对：米 戎
封面设计：唐敏智 责任出版：杨华宁

定价：34.00元

第二版前言

自 1946 年世界上第一台计算机诞生到现在，计算机已经历了 50 多年的发展历史。今天的计算机已广泛应用于国民经济各个领域，各种计算机信息处理系统应运而生，给我们带来了巨大的社会、经济效益。计算机网络技术的应用，更为世界各国、各地区之间的信息交流提供了极大的方便。但是，随着计算机的广泛应用及其在社会生活各方面所起作用的日益增强，计算机安全方面的脆弱性也明显暴露出来。

由于利用计算机进行犯罪活动与传统的犯罪形式相比，具有风险小，效率高的特点，因此，利用计算机从事犯罪的人很容易根据自己所掌握的计算机知识，利用计算机安全方面的脆弱性，以各种技术手段达到偷窃计算机系统中秘密信息或破坏计算机系统的正常工作等种种犯罪目的。由此可见，信息的保密及计算机系统安全问题已成为计算机技术中一个重要的组成部分，因此，对于计算机专业的学生来说，在掌握计算机硬件、软件及相关学科领域知识的同时，还应学习计算机安全保密方面的理论和方法，为此，我们编写了这本《实用密码学与计算机数据安全》。

本教材的第一版是我们在查阅了大量中、外文参考文献的基础上，结合几年来的教学、科研实践编写而成的，除大部分同类教材所具有的知识外，在各种数据加密体制的有关章节中，增加了一些新的算法，在密码技术一章中增加了算法类型与模式的介绍，此外，还增加了密码协议、密码学的实际应用、防火墙技术等当时同类教材罕见的章节，具有范围广泛、内容新颖的特点。

使用了四年之后，本书的主编们针对当前信息安全技术的发展，对原书进行了适当的删改，除修正了原书中的错误外，删除了陈旧过时的内容，增加了新的内容，新教材可分为两条主线，一条是讲述密码技术，包括相关的数学理论基础、各种保密体制、算法及分析、密码协议、密钥管理、算法类型与模式及密码学的实际应用；另一条是讲述计算机数据安全，包括操作系统安全、数据库安全、Internet 安全及计算机病毒的预防等。

全书共分 13 章，第 1 章叙述了信息保密及计算机安全的重要意义，介绍了计算机安全保密研究的内容；第 2 章阐述了密码学所涉及的数学基础，特别是数论方面的有关知识；第 3 章介绍了传统密码体制的一些算法；第 4 章介绍了对称密码体制及有关的算法，并着重介绍了该体制的代表——DES 算法的加密、解密过程；第 5 章介绍了公开密钥密码体制的理论及有关算法，重点介绍了 RSA 算法的加密、解密过程；第 6 章介绍了序列密码的概念、算法及加密、解密过程；第 7 章介绍了密码协议的概念及一些重要的密码协议内容；第 8 章讨论了密钥管理技术，并介绍了几种常用的算法模式；第 9 章介绍了一些应用密码协议、密码算法及模式的实际系统；第 10 章介绍了操作系统安全的有关知识；第 11 章介绍了通用数据库及统计数据库的概念及安全知识；第 12 章在回顾了 TCP/IP 技术基础上，介绍了计算机网络安全的最重要手段——防火墙技术，入侵检测技术以及 Web 安全问题。

本书可作为高等学校计算机专业和通信工程专业学生和研究生教材，也可作为计算机安

全保密等有关专业人员的参考书。

参加本书编写的有：李克洪、兰春岭（第 1，3 章）、董晓梅（第 2，4，5，6 章，12.7 节）、张晓津（第 7 章）、王大玲（第 8，9，10，11 章，12.8 节）、赵秀春（第 12 章）、罗世毅（第 13 章），全书由李克洪、王大玲、董晓梅主编。

另外，在本教材出版之前，我们在教学中曾使用了东北大学校内教材。在此，对参加过校内教材编写的王丽娜、谢军、李晓燕、李春山和王国仁表示感谢。

由于编者水平有限，教材中定有不少欠妥和尚待完善之处，希望读者不吝指正。

编　者

2001 年 8 月

目　录

1 绪　论

在计算机科学迅速发展的今天，计算机已广泛应用于各行业部门。计算机的广泛应用，给用户带来了巨大的社会、经济效益，但同时也给利用计算机犯罪的人提供了可乘之机。因此，在把计算机作为科学研究和信息存储及传输工具的同时，计算机的安全及信息保密问题也是应引起足够重视的。

1.1 计算机安全及信息保密的意义

自1946年世界上第一台计算机问世以来，至今已有50多年的发展历史。从采用电子元器件、使用机器语言到采用超大规模集成电路、具有各种高级软件，计算机已经历了四个发展阶段，并正在向第五代计算机即非诺依曼结构计算机的方向发展。今天的计算机已不仅仅是用于科学计算的快捷工具，而且是几乎用于各个领域的信息处理工具，政府机关、企业、银行及军事机构等国家重要部门都使用计算机建立信息系统，各种重要的信息和情报均由计算机进行处理。同时，随着计算机性能的不断提高，设备规模的日益增大，计算机网络已遍及世界。例如，世界上规模最大的计算机网络Internet网，是由世界范围的众多计算机网络连接而成的，它具有强大的信息传送与沟通功能，为世界各行业的用户提供了极其丰富的信息资源和方便快捷的服务，到1996年，Internet已拥有12 881 001台主机，到2000年，Internet上大约有100万个网络、1亿台计算机和10亿个用户。

在我国，计算机已在各行业得以广泛应用，各种计算机信息处理系统层出不穷，特别是近年来，随着我国信息高速公路及跨国数据通信网络的建设，与世界先进计算机技术接轨的步伐大大加快，举世瞩目的“三金”（金桥、金卡、金税）工程已成为覆盖全国、跨世纪的庞大系统工程。

计算机的广泛应用，给我们带来了巨大的社会、经济效益，但同时也给我们提出了新的课题，因为随着计算机技术的发展，计算机系统安全方面的脆弱性也明显暴露出来，利用计算机犯罪的案例也与日骤增。网络技术的发展，为银行、政府机关、商业、企业及私人通信提供了相当便利的条件，大大加快了信息发布和传播的速度，但也带来了一系列的问题。例如，攻击者可以通过各种技术手段非法接收甚至修改一些他本来无权使用的秘密信息，非法用户冒充合法用户操纵计算机终端获取一些机密情报，非法信息进入计算机系统，存储和传输中的合法信息遭到破坏，黄色出版物通过网络传入境内，文件传输携带病毒等。在科学技术高度发达的美国，几年前也曾出现过计算机病毒致使全国计算机网络瘫痪的事件。此外，有时各种人为的破坏和攻击以及没有经验的用户的误操作也会导致计算机操作系统、数据库及其他系统资源的严重故障。凡此种种，都说明计算机系统的安全及信息的保密已成为计算机技术发展的一个重要组成部分。

1.2 计算机安全与信息保密研究的内容

早在六七十年代，美国、英国和日本等一些科学技术先进的国家就制定了一些关于保护软件产权的法律条文，但是只有法律，还不足以防止对计算机系统的攻击或消除对它的威胁。近30年来，计算机技术及相关学科、理论的发展，使人们在利用法律保护的同时，能够利用计算机本身在技术上开展安全及保密的研究并逐步加以实现。计算机安全及信息保密的研究具体包括信息加密的算法、体制、协议及相关技术、操作系统的安全、数据库安全、计算机网络安全以及计算机病毒的防治等几方面问题的研究。

1.2.1 信息加密、解密的概念

设A，B两方要进行通信，他们至少要解决以下两个问题：

(1)A如何能够确信他的信不会为第三者所窃取；

(2)B如何能够确信他收到的信是A发送给他而不是第三者假冒A发送给他的假情报。

如果他们采用写信、邮寄的方式，则通过查看信封是否完好无损及辨认笔迹的方式很容易解决上述问题，但如果他们采用计算机进行通信，这些问题如何解决呢？

我们将人们能够读懂的信称作“明文”，为隐蔽明文，可将其通过某种方式变换成难以理解的“密文”，这一变换处理过程称为加密。同样，密文可以经过变换再还原成明文，这一变换处理的过程称为解密。

A将明文经过加密变换后使之成为密文，将密文发送给B，合法的收信者B拥有解密的手段，因此可以将密文解密成原来的明文，这一过程如图1.1所示。

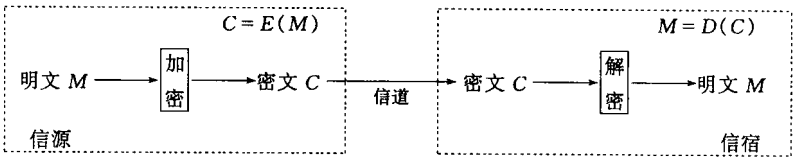


图1.1 保密通信模型

其中，M 代表明文，C 代表密文，E 代表加密变换(enciphering)，D 代表解密变换(deciphering)，显然，D 是 E 的逆变换。

加密的目的是：即使密文在传播过程中被人窃取，也会因窃取者缺乏解密手段而无法理解，从而不能得到此信息，这就解决了上述第一个问题。

对于B来说，由于他相信只有A才知道如何将明文按他们之间的约定加密，而其他人插入的假情报解密后会变得毫无意义，因此，凡解密后有明确意义的明文应该是由A发来的，这就解决了第二个问题。

1.2.2 算法与密钥

1. 算 法

保密算法是用于加密和解密变换的数学函数，使用时，通常包括两个相关的函数，一个用来加密，另一个用来解密。

前面提到，加密的目的之一是使密文的偷窃者因缺乏解密手段而无法理解偷窃的信息，只