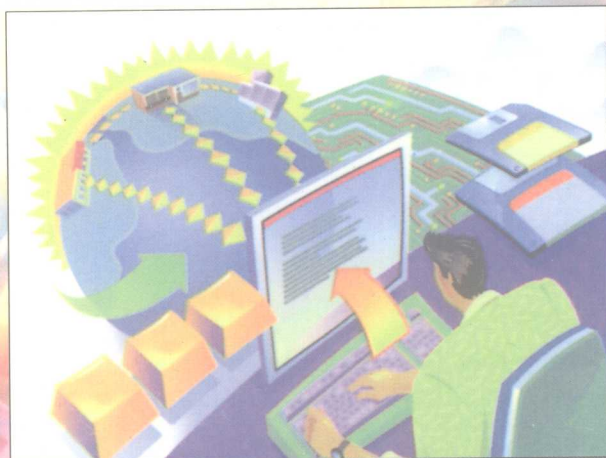


实用密码学 与计算机数据安全

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

©东北大学出版社出版

(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	1
1.1 计算机安全及信息保密的意义	1
1.2 计算机安全与信息保密研究的内容	2
1.2.1 信息加密、解密的概念	2
1.2.2 算法与密钥	2
1.2.3 密码分析	4
1.2.4 算法的安全	5
1.2.5 算法的实现	5
1.2.6 计算机系统安全问题	6
1.3 密码学及计算机安全技术的发展	7
1.3.1 密码学的历史	7
1.3.2 国际著名安全保密机构简介	7
2 密码学的数学基础	9
2.1 信息论	9
2.1.1 熵 (Entropy) 和疑义度 (Uncertainty)	9
2.1.2 自然语言率	10
2.1.3 密码系统的安全性	10
2.1.4 确定性距离	11
2.1.5 混乱与扩散	11
2.2 复杂性理论	12
2.2.1 算法复杂性	12
2.2.2 问题复杂性	13
2.3 初等数论	14
2.3.1 模运算	14
2.3.2 素 数	15
2.3.3 最大公因数	15
2.3.4 乘法逆元素	16
2.3.5 Fermat 小定理和欧拉函数	17
2.3.6 中国剩余定理	18
2.3.7 二次剩余	18
2.3.8 Legendre 符号	19
2.3.9 Jacobi 符号	19
2.3.10 生成元	19
2.3.11 有限域中的计算	20
2.4 因数分解	21
2.5 素数的产生	21

2.5.1	Solovay-strassen 方法	22
2.5.2	Lehmann 法	22
2.5.3	Rabin-Miller 法	22
2.5.4	实际应用	23
2.5.5	强素数	23
2.6	有限域内的离散对数	23
2.7	单向哈希函数	24
2.7.1	概 述	24
2.7.2	Snefru	25
2.7.3	N-hash	25
2.7.4	MD2	27
2.7.5	MD4	27
2.7.6	MD5	27
2.7.7	安全哈希算法 SHA	30
3	传统加密方法	33
3.1	换位法	33
3.2	简单代替密码	34
3.2.1	对简单代替密码的描述	34
3.2.2	单字母频率分析	37
3.3	同音代替密码	38
3.3.1	Beale 密码	39
3.3.2	高阶同音代替密码	40
3.4	多表代替密码	40
3.4.1	Vigenère 和 Beaufort 密码	41
3.4.2	重合度	43
3.4.3	Kasiski 方法	44
3.4.4	游动密钥密码	46
3.4.5	转轮机和 Hagelin 机	47
3.4.6	Vernam 密码与一次一密密码	48
3.5	多字母组代替密码	49
3.5.1	Playfair 密码	49
3.5.2	Hill 密码	50
4	对称密钥算法	52
4.1	概 述	52
4.1.1	分组密码	52
4.1.2	乘积密码	52
4.2	数据加密标准算法 DES	53
4.2.1	背 景	53

4.2.2	DES 算法描述	54
4.2.3	DES 的安全性	60
4.2.4	差分和线性密码分析	62
4.2.5	实际的设计准则	65
4.2.6	DES 的变体	65
4.3	其他分组密码算法	68
4.3.1	LUCIFER	68
4.3.2	Madryga	68
4.3.3	NewDES	69
4.3.4	FEAL	70
4.3.5	REDOC	72
4.3.6	LOKI	73
4.3.7	Khufu 和 Khafre	75
4.3.8	IDEA	76
4.3.9	GOST	79
4.3.10	CAST	81
4.3.11	Blowfish	82
4.3.12	SAFER	83
4.3.13	3-WAY	85
4.3.14	RC5	86
4.3.15	分组算法的设计理论	87
4.3.16	使用单向哈希函数的分组密码	88
4.4	联合分组密码	90
4.4.1	两次加密	91
4.4.2	三次加密	91
4.4.3	其他多重加密体制	92
4.4.4	漂白技术	94
4.4.5	串联多个分组算法	94
5	公开密钥算法	95
5.1	概 述	95
5.1.1	概念的提出	95
5.1.2	公开密钥算法的安全性	95
5.2	背包算法	96
5.2.1	超递增背包	96
5.2.2	从秘密密钥建立公开密钥	97
5.2.3	加 密	97
5.2.4	解 密	97
5.2.5	实际实现	98
5.2.6	背包的安全性	98

5.3	RSA 算法	98
5.3.1	对 RSA 的概述	98
5.3.2	RSA 的安全性	99
5.3.3	对 RSA 的选择密文的攻击	100
5.3.4	对 RSA 的公共模攻击	101
5.3.5	对 RSA 的小加密指数攻击	101
5.3.6	对 RSA 的小解密指数攻击	101
5.3.7	结 论	102
5.4	其他公开密钥算法	102
5.4.1	Rabin 体制	102
5.4.2	ElGamal	103
5.4.3	McEliece	104
5.5	公开密钥数字签名算法	105
5.5.1	数字签名算法 (DSA)	105
5.5.2	DSA 变体	108
5.5.3	GOST 数字签名算法	108
5.5.4	离散对数签名体制	109
5.5.5	Ong-schnorr-shamir	110
5.5.6	ESIGN	111
5.6	身份验证体制	111
5.6.1	Feige-Fiat-shamir	111
5.6.2	Guillou-Quisquater	113
5.6.3	Schnorr	115
5.7	密钥交换算法	115
5.7.1	Diffie-Hellman	115
5.7.2	点对点协议	117
5.7.3	Shamir 的三次通过协议	117
5.7.4	加密的密钥交换	118
5.7.5	加强的密钥协商	119
5.7.6	会期密钥分配与秘密广播	120
6	序列密码	122
6.1	线性同余产生器	122
6.2	线性反馈移位寄存器	122
6.3	序列密码的设计与分析	124
6.4	使用 LFSR 的序列密码	124
6.5	序列密码举例	129
6.5.1	A5 序列密码	129
6.5.2	Hughes XPD/KPD	130
6.5.3	Nanoteg	130

6.5.4	加法产生器	130
6.5.5	RC4	131
6.5.6	WAKE	132
6.6	进位反馈移位寄存器	133
6.7	非线性反馈移位寄存器	135
6.8	设计序列密码的方法	135
6.8.1	设计序列密码的系统理论方法	136
6.8.2	设计序列密码的复杂性理论方法	136
6.8.3	其他方法	137
6.9	串联多个序列密码	138
6.10	由伪随机序列产生器产生多个序列	138
6.11	真正随机的序列产生器	138
7	密码协议	140
7.1	协议构造	140
7.1.1	简介	140
7.1.2	使用对称密码的通信	144
7.1.3	单向函数	145
7.1.4	单向哈希 (Hash) 函数	145
7.1.5	使用公开密钥密码的通信	146
7.1.6	数字签名	148
7.1.7	用加密的办法实现数字签名	152
7.1.8	随机与伪随机序列发生器	154
7.2	基本协议	155
7.2.1	密钥交换	155
7.2.2	验证 (Authentication)	159
7.2.3	验证与密钥交换	162
7.2.4	验证和密钥交换协议的形式化分析	168
7.2.5	多密钥的公开密钥密码术	169
7.2.6	分割秘密	170
7.2.7	秘密共享	171
7.2.8	用密码术保护数据库	173
7.3	中间协议	173
7.3.1	时间戳服务	173
7.3.2	不可否认的数字签名	176
7.3.3	指定的确认者签名	176
7.3.4	代理人签名	177
7.3.5	组签名	177
7.3.6	失败停止数字签名	178
7.3.7	数据位提交 (Bit commitment)	178

7.3.8	公平地抛硬币协议 (Fair coin Flips)	180
7.3.9	智力扑克协议	182
7.3.10	单向累加器	184
7.3.11	秘密全部泄露或者完全不泄露	184
7.4	高级协议	184
7.4.1	零知识证明	184
7.4.2	身份的零知识证明	188
7.4.3	盲签名 (Blind Signatures)	189
7.4.4	基于身份的公开密钥密码术	190
7.4.5	茫然传输 (Oblivious transmission)	190
7.4.6	同时签订合同	191
7.4.7	数字认证邮件 (Digital certified Mail)	194
7.4.8	秘密的同时交换 (Simultaneous Exchange of secrets)	194
7.5	秘密协议 (Esoteric Protocols)	195
7.5.1	安全的选择 (Secure Elections)	195
7.5.2	秘密的多方参与的计算	199
7.5.3	匿名的消息广播	201
7.5.4	数字现金	202
8	密码技术	206
8.1	密钥长度	206
8.1.1	对称密码体制的密钥长度	206
8.1.2	公开密钥密码体制的密钥长度	207
8.1.3	两种密码体制密钥长度的对比	208
8.1.4	关于密钥长度的讨论	209
8.2	密钥管理	210
8.2.1	密钥生成	210
8.2.2	密钥传送	213
8.2.3	密钥验证	214
8.2.4	密钥使用	215
8.2.5	密钥更新	215
8.2.6	密钥存储	215
8.2.7	密钥备份	216
8.2.8	密钥的生存期	216
8.2.9	密钥的废止	217
8.2.10	公开密钥密码系统的密钥管理	217
8.3	算法类型与模式	218
8.3.1	电子代码簿模式 (ECB 模式)	219
8.3.2	密码分组链接模式 (CBC 模式)	220
8.3.3	密码反馈模式 (CFB 模式)	222

8.3.4	输出反馈模式 (OFB 模式)	224
8.3.5	计数器模式	225
8.3.6	密码模式的选择	226
8.3.7	交叉存取技术	226
8.4	算法使用	227
8.4.1	算法选择	227
8.4.2	公钥密码与对称密码的比较	227
8.4.3	加密通信信道	227
8.4.4	用于存储的数据的加密	230
8.4.5	硬件加密与软件加密对比	230
8.4.6	压缩、编码与加密	231
8.4.7	毁坏信息	231
9	密码学的实际应用	233
9.1	IBM 密钥管理协议	233
9.2	MITRENET 网	233
9.3	综合业务数字网 ISDN	234
9.3.1	密 钥	234
9.3.2	电话呼叫过程	234
9.4	Kerberos 协议	235
9.4.1	Kerberos 模型	235
9.4.2	Kerberos 工作步骤	235
9.4.3	凭 证	236
9.4.4	Kerberos Version 5 的消息	237
9.4.5	Kerberos 的安全性	238
9.5	IBM 通用密码体系结构	238
9.6	ISO 鉴别机构	239
9.6.1	认 证	239
9.6.2	验证协议	240
9.7	秘密邮件—PEM	241
9.7.1	PEM 文件	241
9.7.2	认 证	242
9.7.3	PEM 信息	242
9.7.4	PEM 的安全性	245
9.8	公钥密码标准 PKCS	245
9.9	通用电子支付系统 UEPS	246
9.9.1	智能卡	246
9.9.2	通用电子支付系统	247
10	安全操作系统	248
10.1	操作系统保护的对象及保护方法	248

10.1.1	操作系统的发展	248
10.1.2	操作系统保护的对象	248
10.1.3	操作系统提供的保护措施	249
10.2	对存储器的保护	250
10.2.1	栅栏 (Fence) 保护	250
10.2.2	基址/边界寄存器 (Base/Bounds) 保护	250
10.2.3	段式 (Segmentation) 保护	252
10.2.4	页式 (Paging) 保护	254
10.3	一般对象的保护	256
10.3.1	目录的保护	257
10.3.2	访问控制表	258
10.3.3	访问控制矩阵	258
10.3.4	能力标识	259
10.3.5	面向过程的访问控制	259
10.4	文件保护机制	260
10.4.1	无保护机制	260
10.4.2	分组保护机制	260
10.4.3	口令字及其他标识	261
10.5	用户认证	261
10.5.1	口令字的使用	261
10.5.2	对口令的攻击	262
10.5.3	口令字文件的加密	262
10.5.4	一次口令字	263
10.6	安全操作系统设计简介	263
10.6.1	安全操作系统设计原理	263
10.6.2	基本的多道程序操作系统特征	264
11	数据库安全	265
11.1	数据库安全	265
11.1.1	数据库简介	265
11.1.2	数据库安全要求	266
11.1.3	数据库的完整性	267
11.1.4	访问控制策略	268
11.1.5	数据库的安全性	270
11.1.6	数据库恢复	271
11.2	统计数据库模式	272
11.2.1	统计数据库简介	272
11.2.2	统计数据库模型及统计信息类型	272
11.2.3	统计数据库的安全	272
11.3	推理控制机制	273

11.3.1	安全性与精确度的概念	273
11.3.2	推理控制方式	274
11.4	对统计数据库的攻击方式	275
11.4.1	小查询集和大查询集攻击	275
11.4.2	跟踪器攻击	276
11.4.3	对线性系统的攻击	277
11.4.4	中值攻击	277
11.4.5	插入和删除攻击	278
11.5	统计数据库安全措施	278
11.5.1	对统计数据库的限制方式	278
11.5.2	数据搅乱方式	280
12	Internet 安全	282
12.1	TCP/IP 技术回顾	282
12.1.1	TCP/IP 的主要性质	282
12.1.2	数据通信模型	282
12.2	Internet 安全问题	289
12.2.1	Internet 发展简史和所提供的服务	289
12.2.2	Internet 带来的潜在危险	290
12.3	安全策略	293
12.3.1	安全策略的意义	293
12.3.2	基本安全原则	293
12.4	防火墙的设计和建立	294
12.4.1	防火墙的核心思想和作用	295
12.4.2	防火墙的基本概念	295
12.4.3	防火墙的优点	295
12.4.4	防火墙体系结构	296
12.4.5	建立防火墙的主要途径	298
12.4.6	商售防火墙简析	299
12.4.7	防火墙的局限	300
12.4.8	防火墙的未来	301
12.5	基于分组过滤的防火墙设计	301
12.5.1	IP 网络概念的简要回顾	301
12.5.2	筛选路由器和一般的路由器之间的区别	301
12.5.3	分组过滤的优点	302
12.5.4	分组过滤的局限性	302
12.5.5	配置分组过滤规则时应注意的问题	303
12.5.6	分组过滤路由器的工作步骤	303
12.5.7	分组过滤的种类	304
12.5.8	如何选择分组过滤路由器	304

12.5.9	基于分组过滤的防火墙设计举例	306
12.6	基于代理服务的防火墙设计	312
12.6.1	基于代理服务的防火墙的工作过程	313
12.6.2	代理的优点	313
12.6.3	代理的缺点	313
12.6.4	如何实现代理服务	314
12.7	入侵检测技术	315
12.7.1	什么是入侵检测	315
12.7.2	入侵检测方法	317
12.7.3	入侵检测系统的体系结构	319
12.7.4	通用入侵检测框架 CIDEF	320
12.8	Web 安全	320
12.8.1	Web 安全问题	320
12.8.2	Web 站点的安全隐患	321
12.8.3	Web 用户的安全隐患	321
12.8.4	Web 安全防范措施	322
12.8.5	Web 站点与用户安全通信实例	323
12.8.6	黑 客	323
13	计算机病毒概论	325
13.1	计算机病毒的基本概念	325
13.1.1	计算机病毒的定义	325
13.1.2	计算机病毒的起源	325
13.1.3	计算机病毒的特点	326
13.1.4	计算机病毒的分类	327
13.1.5	计算机病毒的破坏现象	329
13.1.6	计算机病毒的程序结构	330
13.1.7	计算机病毒的工作流程	331
13.1.8	计算机病毒的标识	331
13.1.9	计算机病毒的检测	332
13.1.10	计算机病毒的传播载体	334
13.1.11	反病毒的斗争	334
13.2	计算机病毒的理论基础及技术基础	335
13.2.1	程序自我复制理论及病毒产生的可能性	335
13.2.2	磁盘存储结构	335
13.2.3	DOS 基本结构	335
13.2.4	DOS 的中断机制	335
	参考文献	338

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。

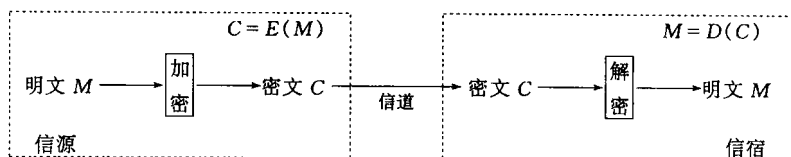


图 1.1 保密通信模型

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