

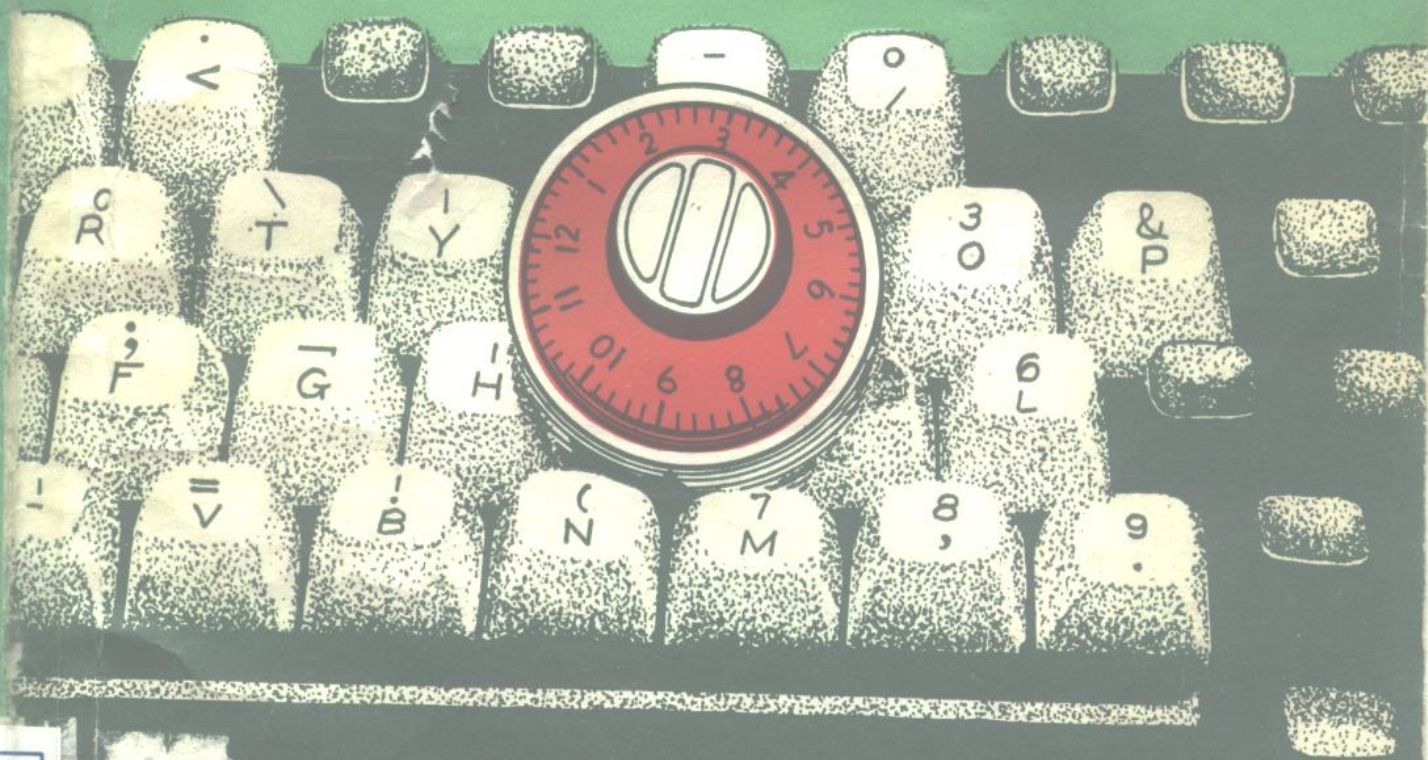
密码学

计算机数据安全的一个新领域

(安全系统设计和实施指南)

[美] 卡尔 H. 梅尔、司蒂芬 M. 马脱耶斯 著

刘景伊、王耀勋、王鸿谷、罗伯鹏、常梦雄、张尔扬 等译



国防工业出版社

密 码 学

计算机数据安全的一个新领域

(安全系统设计和实施指南)

[美] 卡 尔 H. 梅 尔 著
司蒂芬 M. 马脱耶斯

刘景伊 王耀勋 王鸿谷 等译
罗伯鹏 常梦雄 张尔扬

国 防 工 业 出 版 社

内 容 简 介

本书是从美国 IBM 公司的 C.H. 梅尔和 S.M. 马脱耶斯的专著——《密码学》1982年版翻译过来的。全书共十二章，主要内容包括：密码学的基本概念，各种密码的算法；密钥的管理、产生、分配、控制和使用；密码学在计算机通信系统和银行的电子支付系统中的应用实例，以及在应用中所遇到的各类问题（如数字签名联络规程、消息确认、智能银行卡等）。本书是作者从事密码学研究和开发工作的经验总结。

本书可供计算机应用领域中从事数据安全的研究、设计和管理人员参考，也可作为电子工程系、计算机科学系及财经、银行管理系的高年级学生和研究生教材或参考书。

CRYPTOGRAPHY,
A NEW DIMENSION IN COMPUTER DATA SECURITY
A Guide for the Design and Implementation of Secure Systems
CARL H. MEYER
STEPHEN M. MATYAS
JOHN WILEY & Sons, INC. 1982

*

密 码 学

计算机数据安全的一个新领域

(安全系统设计和实施指南)

卡 尔 H. 梅 尔 著
〔美〕 司 蒂 芬 M. 马 脱 耶 斯

刘景伊 王耀勋 王鸿谷 罗伯鼎 常梦雄 张尔扬 等译

责任编辑 王纲李 郑 廷

*

国防工业出版社出版

新华书店北京发行所发行 各地新华书店经售

国防工业出版社印刷厂印刷

*

787×1092 1/16 印张33¹/₂ 766千字

1988年7月第一版 1988年7月第一次印刷 印数：0,001—3,200册

ISBN 7-118-00070-1/TN13 定价：8.85元

译者前言

目前的计算机应用正朝着机、网、库联成一体的方向发展，“数据安全性”这一术语已经远远超出传统的“数据保密”的概念，形成了密码算法和密钥管理体制相结合的一个现代化的崭新学科——密码学(或称密码术)。在现代化信息环境中，机、网、库中信息流的安全性涉及到机、网、库本身是否能存在的问题。如果敌人或对手能获得并利用部分或全部有关信息并向外公开，则将危害社会和国家的安宁和安全。因此，只要是涉及计算机系统的经理人员、设计人员、工程师以及程序员、分析员等，安全性问题就是必要和亟待解决的问题。

本书是由美国两位著名的专家——IBM公司的梅尔(Meyer)和马脱耶斯(Matyas)合著。前者是美国标准局著称的《数据加密标准》的设计人之一；后者是美国著称的较早密码专家。

书中涉及的是当代密码学的概念和实施方法，涉及到诸种密码算法和密钥的管理、产生、分配、设置、控制和使用，指出了密码学对数据安全性所能解决与不能解决的范围。

本书第一章综述了当代对机密数据进行窃取的各种手段和对这些窃取应采取的措施，指出了密码保护的重要性。

第二章提出了块密码和流密码的基本概念，并对DES算法作了简要介绍，对RSA算法作了较详细的说明，还介绍了活门背包算法的概念。介绍了对手可能对密码算法进行攻击的类型(密码的分析法和穷尽法)，指出在设计强密码时所遇到的一些苛刻条件。在算法应用上提出了对短块的一般处理方法，以及有关块连锁的各种概念。最后对块密码和流密码进行了比较。

第三章详尽地阐述和分析了数据加密标准(DES)。首先深入浅出地提出了密码的分类，综述了历史上曾采用的方法及其优缺点。在此基础上提出了DES的设计准则，并说明其操作过程。分析了DES的强的符号间依赖性及密码强度。

第四章介绍了密码学在计算机通信网中的应用，说明了网络的加密方式：终点到终点、链路和节点加密。突出地强调了通信网络中的密钥管理方法，提出了多层次的密钥管理体制来增强系统的安全性。介绍了通信加密和文件加密的例子，最后例举了利用宏指令方式完成的主机密码操作、数据保护和密钥管理的例子。

第五章进一步阐述了主机系统的密码操作，侧重点在于如何设计主机系统的密码操作才不会或不易泄露密钥，增加单域或多域通信中传输数据和文件的安全性。

第六章的主要内容是密码系统中密钥管理的问题，即密钥的产生、存储、分配和设置。在阐述这些问题时都用了生动的例子，并指出了密钥管理中应采取的安全方法。

第七章的主要内容是把密码学和一般的通信规程(或协议)相结合做了阐述，这一点在设计计算机通信网时特别重要。因为把密码通信纳入通信网时，使网的结构和规程进一步复杂化。

第八、九两章是密码学的两种新应用，即消息确认和数字签名。前者用来保证消息的可信性，后者是相距遥远的双方在签署规程时迅速签字的一种电子手段。对公用钥算法和通常算法在数字签名中的应用进行了详细的分析，提出了需要考虑的问题和设计方法。

第十章基本上引用《PIN手册：使用交换网中的个体识别号指南》一书中的部分内容，其中详细讨论了基于银行顾客的个体识别号（PIN）的银行电子支付系统所遇到的有关问题，以及密码学在此系统中应用的细节。

第十一章是对电子支付系统中实行各种安全体制时的分析和比较。特别是对PIN和各种密钥结合使用时的安全体制作了透彻的分析。作者对智能安全卡的提出，使EFT系统的发展开辟了新的途径，对未来的更安全的系统作出了新的构思。

第十二章讨论了密码学安全性度量量的问题。结合三种较好的度量方法讨论了有关的技术问题和理论问题。

本书知识结构完整，技术内容先进，论述深入浅出，图表、资料丰富。它不仅是计算机应用领域中从事数据安全的研究、设计和管理人员以及大专院校师生所必需的指导性论著，而且也是一本较好的电子工程系、计算机科学系、财经银行管理系高年级本科生与研究生的教材和便于自学者的基础用书。

在翻译方面，由于近代密码学是一门崭新的学科，所以采用了直译的方法。在技术术语方面也是如此，例如Block Cipher译成块密码（不译成分组密码），Stream Cipher译成流密码（不译成序列密码），等等。这样便于中英对照和内外交流。

译稿是在刘景伊教授直接领导下完成的。刘教授任总校并翻译了若干章节。参加翻译的有罗伯鹏、王耀勋、王鸿谷和张尔扬同志；担任部分校阅的有常梦雄、欧阳鄂、饶世林同志；最后总校由刘景伊、王耀勋和王鸿谷同志完成。支持本书出版组织工作的还有储非、李情与和陈元兴等同志，编辑同志也为本书的出版做了大量的工作，在此一并表示感谢。由于校译者水平所限，兼以本书内容、术语较新，且篇幅浩大、校译期间人员更迭频繁，故错误和不妥之处在所难免，谨请读者批评指正。

绪 言

本书讨论现代密码学。现代密码学与古典密码学不同。后者是用来保守最高当局和各级政府官员的外交和军事秘密的，而现代密码学则必须用最低的代价和最高的效率，并且用最保险的方法来保护电子数据处理（EDP）系统收集的和与之通信的大量的数字化数据。所以本书内容的适用对象是与日俱增的和计算机数据的安全性和私人秘密打交道的技术人员和非技术人员。

本世纪七十年代，随着完善的基于加密的规程和密码学应用新领域的出现，密码学就以前所未有的速度突飞猛进。1977年1月15日，美国国家标准局通过一项加密算法作为美国联邦政府的标准。这就是数据加密标准（DES），它标志着密码学研究和发展的里程碑。后来，于1980年12月，美国国家标准协会通过了这一算法作为美国商用加密算法。另一个里程碑是有人提出一个新的概念，叫做公用钥密码学，此方法仍在发展之中，而当前还没有一项协议的标准算法。

很多读者可能对密码学一词感到生疏，然而，他们在通信网络或电子数据处理系统中，常会遇到某种程度上的密码设计或密码保护的实施问题。为了迎接向技术界提出的黜黜逼人的挑战，我们向读者全面阐述密码学的这些领域。

值得提出的是，密码学对保护大型通信网络（电话线路、微波、卫星）上传输的信息来说是唯一实用的手段。至于密码学如何才能用来达到通信安全的目的，本书将作详细讨论。此外，还讨论了各种攻击方案，以便工程师和系统设计师能理解和重视在提供密码学安全解法时会遇到的问题 and 困难。

密码学可以用来保护文件的安全。为了对存储在可迁移介质中的数据加密起见，已研制了一套规程。通过密码的技术方法，还可以制订出更完善的确认规程，包括人名验证、消息确认和数字签名。这些课题是在银行业和金融界中与电子支付系统和信用卡应用有关人员所特别感兴趣的，也是那些身处其它领域而必须核对某种包含着始发人、时间性、内容和规定接收人的消息的人员所特别感兴趣的。

银行业和金融界，一直是推进密码学应用的倡导者，他们对通过大型计算机网和终端间传输消息来转移的财产进行保护。为了讲清这一课题，我们从“主控卡国际公司”制定的，原先只能通过该公司保安部才能获得的PIN手册中复印了很多内容，作为此材料的补充，我们对EFT系统的安全性作了具体分析，并提出了一系列电子支付系统的安全性要求。这也许会得到设计或规划电子支付系统应用人员的重视。本书探讨了各种实施方案，包括在将来系统中获得严格安全性所需的设计权衡和技术。

凡是用密钥控制的密码算法，例如DES，都要用某种规程来管理它的密钥。书中详细谈到了密钥管理方案，使之能用来支持各个终端用户（终点到终点）间的通信保护以及在可迁移介质上存储或传输的数据的保护。本书还探讨了安全和保险的密钥产生、分配和设置的程序。

香农对密码学的论述（在其讨论保密系统的划时代论文中）已用作阐述唯一性距离

和工作因素课题的出发点。本书中既用了统计学方法又用了信息论方法，以便使读者对获得密码强度的方法有更全面的理解。

本书的阅读对象是有志于理解密码学的作用以获得高水平计算机数据安全性的各类人员。可能更重要的是这样的事实，即可认为密码学是对某些数据安全问题的一种完整解法。对其他人来说，密码学只能给出某种局部解法，但要知道哪些问题能用哪些不能用密码学来解决，同样也是重要的。无论是工程师、设计师、计划人员、管理人员，还是科学家和大学生都能从本书论述的一些实际和理论课题中得到教益。

本书中的最新资料是我们结合自己从事的密码学领域的研究和开发工作编写出来的，或是根据我们在更广泛的数据安全性领域里的研究工作编写出来的。

本书所述观点由作者负责，不一定代表国际商用机器公司。

C. H. 梅 尔

S. M. 马脱耶斯

1982年7月

目 录

第一章 密码学在电子数据处理中的作用	1
1.1 密码学、私人秘密和数据安全	1
1.1.1 攻击方法	1
1.1.2 私人秘密法案的技术含义	3
1.2 数据加密标准	5
1.3 有效的密码安全性的论证	6
1.4 密码学展望	7
参考文献	8
第二章 块密码和流密码	10
2.1 密码算法	10
2.1.1 加密和解密	11
2.1.2 工作因素	14
2.1.3 攻击类型	14
2.1.4 算法设计	15
2.2 块密码	17
2.2.1 通常算法	19
2.2.2 公用钥算法	23
2.2.3 RSA算法	24
2.2.3.1 素数的分布	29
2.2.3.2 素数性的测试	30
2.2.3.3 密码强度的研究	32
2.2.4 活门背包算法	34
2.3 流密码	38
2.4 具有连锁的块密码	43
2.4.1 数据内的模式	43
2.4.2 用可变钥的块连锁	46
2.4.3 使用明文和密文反馈的块连锁	48
2.4.4 使用密文反馈的自同步方案	49
2.4.5 块连锁的例子	53
2.4.6 短块加密	53
2.5 具有连锁的流密码	59
2.5.1 具有误差传播特性的一个连锁方法	59
2.5.2 具有自同步性质的一种连锁方法	61
2.5.3 密码反馈的流密码	63

2.5.4 种子产生的一个例子	63
2.5.5 密码反馈的例子	66
2.6 填补和初始向量效应	66
2.7 用连锁技术时密码消息的确认	68
2.8 块密码和流密码的比较	73
参考文献	75
第三章 数据加密标准	77
3.1 密码的分类	77
3.2 设计准则	80
3.2.1 破译一个有双密钥带的系统	81
3.2.2 破译一个用线性移位寄存器的钥-自动钥密码	82
3.2.3 破译一个用线性移位寄存器的明文自动钥密码	88
3.2.4 设计一个密码	93
3.2.4.1 捷径法	93
3.2.4.2 蛮劲法	94
3.2.4.3 保密的设计原则	95
3.3 数据加密标准的描述	95
3.3.1 用于DES每次轮回中的密钥向量的产生	97
3.3.2 弱和半弱密钥	100
3.3.3 DES算法的说明	105
3.3.4 DES过程小结	107
3.3.5 数字例子	108
3.3.6 有关DES设计的一些说明	109
3.3.7 S盒设计的实现考虑	110
3.4 数据加密标准的符号间依赖性分析	112
3.4.1 密文和明文间的符号间依赖性	114
3.4.1.1 过程小结	119
3.4.1.2 为获得密文/明文符号间依赖性所要求的最小轮回数	121
3.4.2 密文和密钥间的符号间依赖性	122
3.4.2.1 获得密文/密钥符号间依赖性所要求的最小轮回数	129
3.4.3 小结和结论	130
参考文献	131
第四章 基于密码学的通信安全性和文件安全性	133
4.1 网络	133
4.2 网络加密方式	134
4.3 链路加密的基本原理	138
4.3.1 异步	139
4.3.2 字节同步	140
4.3.3 位同步	140
4.4 终点到终点加密的概述	141

4.5 密钥分配	143
4.5.1 密钥的指标要求	143
4.5.2 数据传输加密的例子	149
4.5.3 数据文件加密的例子	151
4.6 密码设施	152
4.7 密钥的保护	154
4.7.1 终端密钥的保护	154
4.7.2 主机密钥的保护	155
4.7.2.1 主控键的概念	155
4.7.2.2 加密和未加密的初级密钥	155
4.7.2.3 多主控键	156
4.7.2.4 主控键的变体	157
4.7.2.5 小结	157
4.7.3 密钥的层次	158
4.8 主机密码系统	159
4.9 基本密码操作	160
4.9.1 终端的密码操作	161
4.9.2 主机的密码操作	164
4.9.2.1 数据加密操作	164
4.9.2.2 密钥管理操作	165
4.9.3 密钥奇偶性	167
4.9.4 密钥分割	167
4.10 密码宏指令	169
4.11 密钥管理宏指令	174
4.11.1 GENKEY和RETKEY宏指令	175
4.11.2 使用GENKEY和RETKEY	178
4.12 密码键数据集	180
4.13 小结	181
参考文献	181

第五章 主机系统的密码操作

5.1 使用预产生初级键的单域通信安全性	183
5.2 使用动态产生的初级键时单域通信的安全性	185
5.2.1 两个主控键	186
5.2.1.1 在KM1下加密	186
5.2.1.2 通信加密的一个例子	186
5.2.2 要求	187
5.3 使用动态产生的初级键时单域通信安全性和文件安全性	187
5.3.1 与存储着的被加密的数据相联系的问题	187
5.3.2 三个主控键	189
5.3.2.1 主机密钥的保护	190
5.3.2.2 在KM1和KM2下的加密	190
5.3.2.3 文件密钥的产生	190

5.3.3	文件加密的例子	191
5.3.4	要求	192
5.4	多域加密	192
5.4.1	通信安全性用的一个规程	192
5.4.2	文件安全性用的一个规程	194
5.4.3	传送一个新文件	195
5.4.4	传送一个现有文件	195
5.5	附加的考虑	197
5.6	扩展的密码操作	198
5.6.1	使用组合密钥的分配	198
5.6.2	一个组合密钥规程	199
5.7	小结	202
	参考文献	203
第六章 密钥的产生、分配和安装		204
6.1	主机主控键的产生	204
6.1.1	投掷钱币	205
6.1.2	投掷骰子	206
6.1.3	随机数表	206
6.2	钥加密键的产生	206
6.2.1	一个弱的密钥产生程序	206
6.2.2	一个强的密钥产生程序	207
6.2.3	产生钥加密键的另一方法	209
6.2.4	在主控键变体下密钥的加密	210
6.2.5	变换密钥	211
6.3	数据加密键的产生	214
6.3.1	用密码设施产生密钥的一个方法	214
6.3.2	产生数据加密键的另一方法	215
6.4	在主机处理器处送入一主控键	215
6.4.1	用硬线输入	216
6.4.2	间接输入	219
6.5	通过外部操作的攻击	219
6.6	在终端处主控键的输入	220
6.6.1	联机校验	220
6.6.2	脱机校验	220
6.7	密钥的分配	222
6.8	被遗失的密钥	223
6.9	恢复技术	223
6.10	小结	224
	参考文献	225
第七章 密码学与通信结构的结合		226
7.1	在一个单域网络中的会期级密码术	227

7.1.1 操作的透明模式	227
7.1.2 操作的不透明模式	232
7.2 在单域网络中的私人专用密码术	232
7.3 在一个多域网络中的会期级密码术	234
7.4 应用程序到应用程序的密码术	237
7.5 填充考虑	237
参考文献	239
第八章 使用密码学的确认技术	240
8.1 基本概念	240
8.2 信号联络	240
8.3 消息确认	242
8.3.1 消息出处的确认	244
8.3.2 消息及时性的确认	245
8.3.3 消息内容的确认	246
8.3.3.1 用具有误错传播性质的加密法确认	246
8.3.3.2 用不具有误错传播性质的加密法确认	247
8.3.3.3 消息未加密时的确认	247
8.3.4 消息接收者的确认	249
8.3.5 消息确认的一个过程	250
8.4 时不变数据的确认	251
8.4.1 通行字的确认	251
8.4.2 使用由主机主控钥产生的测试模式的确认	254
8.4.2.1 一个简短的分析	256
8.4.2.2 实现AF与AR	257
8.4.2.3 为通信与文件安全性提出的密码学操作的一种实现	258
8.4.3 用于密钥确认的一个过程	260
8.4.4 使用由主机主控钥产生的测试模式的另一种确认方法	262
参考文献	264
第九章 数字签名	266
9.1 签名的意义	266
9.1.1 认可法	267
9.1.2 代理法	267
9.1.3 统一商业法规	267
9.1.4 自己造成的疏忽	268
9.2 获得数字签名	269
9.3 普遍的签名	270
9.3.1 使用公用密钥算法的一种方法	270
9.3.2 使用通常算法的方法	273
9.3.2.1 方法一	273
9.3.2.2 方法二	277

9.3.2.3 方法三	279
9.4 仲裁性签名	281
9.4.1 一个使用DES算法的方法	283
9.4.2 仲裁一个签名的例子	284
9.4.3 一个弱的方法	285
9.4.4 额外的弱点	286
9.5 使用DES 获得公用密钥的特性	287
9.5.1 用于计算机网的一个密钥公证系统	287
9.5.1.1 系统设计	287
9.5.1.2 标识符与密钥公证	288
9.5.1.3 用户确认	289
9.5.1.4 命令	289
9.5.1.5 数字签名	290
9.5.2 使用主机主控钥诸变体的一种方法	290
9.6 使数字签名合法化	292
9.6.1 初始书写的协议	293
9.6.2 法律的选择	293
9.6.3 司法认可	294
参考文献	295

第十章 密码学应用于基于PIN的电子支付系统

10.1 引言	297
10.2 基本的个体标识号 (PIN) 的概念	298
10.2.1 为什么要PIN?	298
10.2.2 PIN的保密	298
10.2.3 PIN的长度	299
10.2.4 许可的PIN输入尝试	300
10.2.5 PIN的发行	301
10.2.5.1 银行选定的PIN	301
10.2.5.2 卡主选定的PIN	302
10.2.5.3 银行选择PIN与卡主选择PIN的比较	304
10.2.5.4 遗忘的PIN	304
10.2.6 本地交易中的PIN验证	305
10.2.6.1 联机PIN验证	305
10.2.6.2 脱机PIN验证	306
10.2.7 在交换网中PIN的验证	306
10.2.8 结论	308
10.3 电子支付系统的诈骗威胁	308
10.3.1 对EFT系统诈骗的种类	309
10.3.2 消极性的诈骗威胁	210
10.3.2.1 银行卡片发放机构	310
10.3.2.2 传送系统	310
10.3.2.3 卡主	310
10.3.2.4 EFT系统	311

10.3.3	相对危险	312
10.3.4	积极性的诈骗威胁	312
10.3.4.1	通信线路	312
10.3.4.2	EDP系统	313
10.3.5	诈骗和责任	313
10.3.6	结论	315
10.4	防止诈骗的原理	316
10.4.1	密码术——防止诈骗的工具	316
10.4.2	防止消极性诈骗威胁	316
10.4.2.1	PIN加密	317
10.4.2.2	密码钥的保护	317
10.4.2.3	PIN和密钥的物理性保护	317
10.4.3	防止积极性诈骗威胁	318
10.4.3.1	数据窜改	318
10.4.3.2	贷款审定的重用	319
10.4.3.3	诈骗性贷款	319
10.4.3.4	加密PIN的替换	320
10.4.4	交换中预防诈骗	321
10.4.5	防止假设备的威胁	322
10.4.6	结论	323
10.5	防止诈骗方法的实施	323
10.5.1	推荐的硬件安全模块实施方案的特点	323
10.5.2	所推荐的模块系统性能	324
10.5.2.1	银行选择的随机PIN	325
10.5.2.2	由帐号用密码技术导出的PIN	325
10.5.2.3	顾客选择的PIN	325
10.5.3	PIN验证	326
10.5.4	密钥管理	326
10.5.5	MAC的产生	327
10.5.6	模块的使用	328
10.5.7	结论	330
	参考文献	331

第十一章 密码学应用于电子支付系统——个体识别号和个体钥

11.1	背景情况	332
11.2	EFT系统中安全措施败露	334
11.2.1	通信链路的保密	334
11.2.2	计算机的安全性	335
11.2.3	终端的安全性	335
11.2.3.1	在不安全环境中的EFT终端	336
11.2.3.2	伪造设备的攻击	336
11.2.4	银行卡片的安全性	337
11.2.4.1	磁条卡片	337
11.2.4.2	智能安全卡片	337

11.3	对系统用户的识别和确认	338
11.3.1	可转移的用户特性	338
11.3.2	不可转移的用户特性	338
11.4	对于个体验证和消息确认的要求	338
11.4.1	确认参数	339
11.4.2	个体确认码	341
11.4.3	只使用AP进行个体验证	341
11.4.4	使用AP和PAC进行个体验证	342
11.4.5	使用MAC进行消息确认	343
11.4.6	EFT安全性要求	344
11.4.7	对于EFT保密要求的评论	349
11.5	联机模式下的个体验证	349
11.5.1	使用非独立PIN和非独立个体钥的个体验证	350
11.5.2	使用独立PIN和独立个体钥的个体验证	352
11.5.3	卡片存储需求的极小化	356
11.6	在脱机和脱主模式下的个体验证	359
11.6.1	使用系统选择的PIN并采用PIN生成钥的个体验证	359
11.6.2	使用用户选择的PIN并采用偏移技术的个体验证	360
11.6.3	使用用户选择的PIN并采用PAC的个体验证	361
11.7	密码术设计指南	363
11.7.1	对于PIN秘密的威胁	366
11.7.1.1	对PIN的监测	366
11.7.1.2	在EFT终端窃听输入信息	366
11.7.1.3	插入伪造的设备	367
11.7.2	密钥管理要求	367
11.7.3	对于储存在磁条卡片上的密钥的安全威胁	371
11.7.3.1	丢失卡片	371
11.7.3.2	被窃卡片	371
11.7.3.3	复制卡片信息	372
11.7.3.4	窃听EFT终端处的输入信息	372
11.7.3.5	伪造设备的插入	372
11.8	PIN/系统钥方法	372
11.8.1	PIN/系统钥方法中密钥管理的考虑	375
11.8.1.1	共享密钥	375
11.8.1.2	密码转换(平移)	375
11.8.1.3	在发付者处PIN的转换(或平移)	375
11.8.1.4	对于错向路由数据的防护	375
11.8.2	防御错向路由攻击	376
11.8.3	非交换网的PIN/系统钥方法	381
11.8.4	交换网的PIN/系统钥方法	381
11.8.5	PIN/系统钥方法的缺点	381
11.8.5.1	系统钥的泄露使得对于PIN的全面攻击成为可能	381
11.8.5.2	入口点处密钥的泄露	382
11.8.5.3	密钥管理不是稳健的	382

11.8.6	PIN/系统钥方法的优点	382
11.9	PIN/个体钥方法	383
11.9.1	使用磁条卡片的PIN/个体钥方法的说明	383
11.9.2	PIN/个体钥方法钥管理的考虑	384
11.9.3	PIN/个体钥方法的优点	385
11.9.3.1	增大了保密用户提供信息的组合数	385
11.9.3.2	在用户和发件者间端点-端点的防护	385
11.9.4	使用磁条卡片的PIN/个体钥方法的缺陷	385
11.9.4.1	对磁条卡上的钥无法提供保护	385
11.9.4.2	在磁条卡上的密钥必须与终端共享	386
11.9.4.3	滥用个体钥和伪造个体钥引起的泄露	386
11.9.4.4	对KP没有联锁	387
11.9.5	使用智能安全卡片的个体钥方法	387
11.9.5.1	理想的智能安全卡片	387
11.9.5.2	实际的智能安全卡片	389
11.10	使用智能安全卡的PIN/个体钥/系统钥(混合钥管理)方法	390
11.10.1	混合钥管理方法的说明	391
11.10.1.1	对KSTR双重加密的理由	392
11.10.1.2	PIN和KP的选择	392
11.10.1.3	PIN和KP的确认	392
11.10.1.4	系统钥的产生	393
11.10.2	混合法密钥管理的考虑	394
11.10.3	非交换网的混合密钥管理方法	394
11.10.4	交换网的混合密钥管理方法	398
11.10.5	对于智能安全卡片的密码技术上的考虑	400
11.10.6	使用数字签名增强安全性	401
11.10.7	优点	401
11.11	密钥管理的考虑——对称与非对称算法的比较	402
11.11.1	带有保密和不带保密的确认	403
11.11.2	无确认的安全方法	407
11.12	使用智能安全卡和公用钥算法的密码系统	410
11.12.1	公用钥管理方法的说明	411
11.12.1.1	PIN的选择	413
11.12.1.2	用户公用钥及私有钥的产生	413
11.12.1.3	用户PIN和卡片密钥的验证	414
11.12.2	非对称算法的密钥管理	414
11.12.3	脱机使用	415
11.12.4	在交换和非交换网中的联机使用	416
11.12.5	附加说明	420
11.13	结束语	421
	参考文献	421
第十二章	密码系统保密性度量	423
12.1	数学密码学的要素	424

12.1.1	在通常密码学系统中的信息流	424
12.1.2	具有消息概率和密钥概率的密码	424
12.1.3	随机密码	428
12.1.4	冗余性语言中有意义消息数	429
12.2	利用随机密码的保密性概率度量	430
12.2.1	分析者只能得到密文时求得密钥的概率	430
12.2.2	英语简单替代密码实例 (仅可得密文)	433
12.2.3	分析者可同时占有明文和相应密文时求得密钥的概率	435
12.2.4	获取明文的概率	435
12.3	利用信息论香农方法的扩展	436
12.3.1	信息度量	437
12.3.2	分析者只可能占有密文时密码的唯一性距离	438
12.3.3	当分析者可同时占有明文及相应的密文时密码的唯一性距离	440
12.3.4	$H(X Y)$ 、 $H(K Y)$ 和 $H(K X, Y)$ 之间的关系	440
12.3.5	数据加密标准的唯一性距离	443
12.4	作为保密性度量的工作因素	443
12.4.1	破译密码所需的时间和费用	443
12.4.2	英语简单替代法的一些预备知识	443
12.4.3	利用双字母组频数分析时对英文简单替代密码的实践结果	446
12.4.4	利用单字母频数分析英语简单替代密码的实践结果	447
12.4.5	结果比较	448
	参考文献	449
	附录 A 联邦信息处理标准公告 (46)	451
	附录 B 其它有关的进一步计算	459
	B.1 时间-存储权衡	459
	B.2 生日疑题	459
	参考文献	461
	附录 C 塑料卡编码实践和标准	462
	C.1 一般的物理特性	463
	C.2 磁迹 1	463
	C.3 磁迹 2	463
	C.4 磁迹 3	463
	参考文献	464
	附录 D 某些密码学概念和攻击方法	465
	D.1 确认参数的进一步讨论	465
	D.1.1 单向函数	465
	D.1.2 重复试验攻击法	467
	D.2 确认参数和个体确认码的进一步讨论	470
	D.2.1 实施之例	470
	D.2.2 攻击一个16位PIN(个体识别号)	471
	D.2.3 攻击一个12位PIN	471
	D.2.4 对确认参数和个体确认码的建议	472
	D.2.5 与ID相关的AP的优点	475