

[美]卡 尔·H·迈 耶等著
卢起骏 黄朝载等译

计算机网络**保密系统**

设计与实现指南



科学技术文献出版社重庆分社

計 算 机 网 絡

保密系統設計与实现指南

卡 尔 · H · 迈 耶 著
斯 蒂 芬 · M · 马 特 斯

黃朝載 杜銀山 陈爵文 王 宪 译
付爭少 吳兴龙 何如賢 卢起駿

卢 起 駿 校

科 学 技 术 文 献 出 版 社 重 庆 分 社

内 容 简 介

本书主要讨论了计算机数据通信网络的信息保密问题,对计算机网络中的通信保密和文件保密以及主要的密码操作等都作了详细的阐述。此外,对于网络保密方案在电子资金传送系统中的某些实际应用也提供了丰富的材料。为了使一般读者了解密码学的知识,书中还用了专门章节来阐述密码基础理论,并对现代密码学的最新成就 DES 算法和公开密钥密码体制作了分析。书中有大量的插图和实例,有助于读者准确的理解。书末还有若干篇附录,提供了一些具体的算法和资料,对正文内容作了进一步的补充和阐述。

计 算 机 网 络 保密系统设计与实现指南

卡尔·H·迈耶 等著

卢起骏 黄朝载 等译

科学技术文献出版社重庆分社	出版
重庆市市中区胜利路132号	
新华书店重庆发行所	发行
重庆通信学院印刷厂	印刷
开本: 787×1092毫米1/16	印张: 36.125 字数: 940千字
1987年7月第一版	1987年7月第一次印刷
科技书目: 147—305	印数: 3050

ISBN 7-5023-0103-8/TP·11

统一书号: 15176·729

定价: 7.95元

作 者 簡 介

卡尔·H·迈耶博士是美国密码界第一流的权威。他曾在西德汉堡工程学院获得工程师学位，后来又在宾夕法尼亚大学获电子工程科学硕士和博士学位，他发表过15项专利，曾到世界各地讲学，是一位国际上知名的作者，他还作为一名设计者，参加了后来成为著名的“数据加密标准”(DES)的密码方案的设计工作。他的科研成就包括：将密码术结合到通信系统中去的设计和分析；在电子资金传送(EFT)系统中开发证实用户与报文的方法，以及研究维护存贮与传送数据的完整性的方法等等。

斯蒂芬·M·马特斯博士是已知的第一个在美国发表密码分析论文的作者。他在洛瓦大学获得了计算机科学博士学位，是一位公认的、在密码体制方面有创见性的专家。他发表过50多篇涉及密码体制各个领域的学术论文，发表了15项专利，无论在密码理论或实践方面他都十分胜任。尤其值得注意的是，他设计了用对称算法来产生数字签名的方法。另外，他的多重加密方案为不同的密钥管理系统提供了透明兼容特性，该方案已经在一些密码系统中得到了实现。

译 者 前 言

社会进入信息时代,计算机网络的发展为数据通信事业开辟了广阔的前景,同时也对信息的安全保密提出了更苛刻的要求。把密码术引入到现代计算机网络中,从而确保信息的保密和系统的完备。这是目前数据通信网开发事业中的一个新领域,也是众所瞩目的一个新课题。在这种形势下,我们组织翻译了美国密码专家迈耶和马特斯于一九八二年合著的“*Cryptography: A New Dimension in Computer Data Security—A Guide for the Design and Implementation of Secure Systems*”一书,定名为《计算机网络保密系统设计及实现指南》。此书是一部系统论述计算机网络保密的专著,它除了阐述密码学基础理论之外,着重对计算机通信网络,数据库,电子资金传送等方面的安全保密问题作了系统的介绍,同时还用大量的篇幅讨论了具体的实施方案。此外,本书还对数据加密标准(DES)、公开密钥密码体制,电子数字签名和验证等问题作了较深的分析。我们翻译此书的目的,是为了给有关单位和读者提供一本了解和掌握数据通信网络保密技术的参考书。以期在有志于祖国保密事业的人们中间引起讨论,促进交流。本书可以作为从事计算机网络保密设计和管理的工程技术人员的工具书,也可作为大专院校有关专业的教科书和参考书。

本书由中国人民解放军总参谋部第五十一研究所和重庆通信学院联合翻译。参加翻译和校对的有杜银山(第一、二章),陈爵文(第三章),黄朝载(第四、十章),王宪(第五、六、七、十二章),付争少(第八、九章和附录B, G),吴兴龙(第十一章),何如贤(附录C, D, E, F和H)等同志,卢起骏审核了全部译文,马春田同志对本书的翻译给予了指导。另外,重庆通信学院的有关领导对本书的翻译出版给予了热情的支持,还有许多同志也对本书的问世给予了大力的协助。在此一并表示衷心的感谢!

由于我们经验不足,水平有限,时间仓促,因而错误和不妥之处在所难免,恳切希望读者批评指正。

一九八六年七月

原 著 前 言

本书论述了现代密码学。与历代君主和各级政府官员用来隐蔽外交及军事秘密的经典密码方法所不同的是，现代密码学必须提供有成效的和安全的方法来保护由电子数据处理系统（EDP）所搜集和传送的大量数字数据。因此，本书中的材料是供日益增多的、关心计算机数据安全和保密的技术人员和非技术人员阅读的。

在本世纪七十年代，由于出现了强有力的基于加密的协议，并开辟了新的密码应用领域，密码学得到了出乎意料的飞速发展。在1977年1月15日，（美国）国家标准局（NBS）采纳了一种加密算法作为联邦的标准——数据加密标准（DES），从而在密码研究和设计方面树起了一个里程碑。随后，在1980年12月，美国国家标准协会（ANSI）采纳了这个算法作为美国的商用加密算法，而称为公开密钥密码的新思想的提出，又树起了另一个里程碑。公开密钥密码目前还在研究中，至今尚无一致认可的标准算法。

许多读者可能会发觉，他们自己并不熟悉密码学，但他们却在不同程度上面临着如何在通信网络或 EDP 系统中实现密码保护的问题。为了满足技术界的迫切需要，本书还提供了密码学方面的详细材料。

值得注意的是，在大型的通信网络中，无论是电话线路、微波还是卫星，密码术是一种唯一所知的保护传送信息的现实方法。本书详细论述了如何用密码术实现通信保密（COMSEC）的问题。此外，本书还讨论了各种密码攻击方法，以便工程技术人员和系统设计人员能了解并评价在解决密码通信保密时所遇到的问题和难点。

密码术还可以用来实现文件保密。为了加密存贮在可装卸媒体中的数据，本书中开发了一种协议。各种鉴别协议，包括个人身份的验证协议、报文鉴别协议以及数字签名协议等，也都可以通过密码术来实现。在银行和金融界中，以及在那些需要验证报文的来源、时间性、内容和指定的收方的其它部门中，凡是关心电子资金传送和信贷卡应用的读者都会特别重视这些课题。

在用密码术来保护计算机网络中传送资金的报文方面，银行和金融界一直处于领先的地位。为了正确地论述这方面的问题，作者在本书中转载了《PIN手册》中的一些重要章节（该手册是由MasterCard国际公司编印的，以前只由该公司的保密部发行）。作者通过对EFT系统保密性的详细分析，对这些材料作了进一步的充实，并提出了一套EFT的保密要求。这些要求将由设计或规划EFT系统的人员加以审定和评价。此外，本书还讨论了各种实现的问题，包括在未来的系统中实现高度保密性所要解决的方案的权衡问题和技术问题。

任何一种受密钥控制的密码算法，比如 DES，都要求有一种管理其密钥的协议。本书给出了密钥管理方案的细节。这种管理方案提供了对个体端点用户之间（端对端）通信的保护，也可以保护存贮在或传送到可装卸媒体之中的数据。同时还讨论了密钥安全可靠地产生、分配和安装的各种方法。

香农在他的关于“保密系统”的著名论文中对密码学的论述，被用来作为讨论唯一解码量和工作因子等问题的出发点。对统计学方法和信息论方法也都作了介绍，使读者得以更加透彻地理解实现密码强度的方法。

本书的写作对象是那些想了解密码学在高级计算机数据保密中的作用的读者。或许更为重要的问题还在于：密码术已被认为是一种能够彻底解决某些数据保密问题的方法，而对于其它的保密问题，则只能提供部分的解决。认识这一点，同样也是重要的，因为它能使我们了解，采用密码术能或不能解决哪些问题。工程师，设计师，计划人员，管理人员，学会会员以及大学生们，都可以从本书所论述的某些实际和理论的课题中得到收益。

本书中最新的材料是作者在密码学领域中研究探讨所取得的，或者一般地说，是作者在数据保密研究工作中所取得的。

本书中所陈述的观点乃是作者自己的观点，并不一定出自IBM公司。

卡 尔·H·迈 耶

斯蒂芬·M·马特斯

1982年7月于纽约金斯敦

縮 写 詞

密 码 方 式 及 其 有 关 参 数

CBC	密码分组链接	CE	压缩编码
CFB	密码反馈	ECB	电子密本 (参见分组密码)
ICV	初始链接值	OCV	输出链接值
OFB	输出反馈 (参见密钥自身密钥密码)	X	明文
Y	密文	Z	初始化向量 (与ICV同义)
DEA	数据加密算法 (ANSI, 与DES 同义)	DES	数据加密标准 (NBS)
PKC	公开密钥密码体制	RSA	里夫斯特—艾德勒曼—沙米尔 (公开密钥) 算法

密 钥

K	初级数据加密密钥	KA	鉴别密钥
KC	初级通信密钥 (与会话密钥同义)	KF	初级文件密钥
KI	交换密钥	KMT	终端主密钥
KN	二级密钥	KNC	二级 (节点) 通信密钥
KNF	二级节点文件密钥	KP	个人密钥
KPG	个人密钥产生密钥, 用来从ID产生KP	KPN	PIN产生密钥, 用来从ID产生PIN
KS	会话密钥	KSTR	交易会话密钥
KT	常驻终端密钥	KTR	交易密钥
PK	公开密钥密码体制中的公开密钥		
PKb	公开密钥密码体制中的银行公开密钥		
PKc	公开密钥密码体制中的顾客公开密钥		
PKu	公开密钥密码体制中的通用公开密钥		
SK	公开密钥密码体制中的秘密密钥		
SKb	公开密钥密码体制中的银行秘密密钥		
SKc	公开密钥密码体制中的顾客秘密密钥		
SKu	公开密钥密码体制中的通用秘密密钥		

密 码 操 作

AF	正向鉴别 (主机)	AR	反向鉴别 (主机)
ECPH	加密数据 (主机)	EMK	用主密钥加密 (主机)
ENC	加密 (终端)	ENCO	只加密 (主机)
DCPH	脱密数据 (主机)	DEC	脱密 (终端)
DECK	脱密密钥 (终端)	DECO	只脱密 (主机)
GKEY	产生密钥 (主机)	GSK1	产生会话密钥 1 (主机)

GSK2	产生会话密钥 2 (主机)	LKD	直接装入密钥 (终端)
MGK	组合密钥 (主机)		
RFMK	对主密钥加密的密钥重新加密 (主机)		
RTMK	用主密钥重新加密 (主机)	SMK	置主密钥 (主机)
WMK	写主密钥 (终端)		

密 码 宏 指 令

CIPHER	密码	GENKEY	产生密钥
RETKEY	还原密钥		

系 统 术 语

ATM	自动出纳机	BSC	二元同步通信
CC	通信控制器	HPC	主处理中心
KDC	密钥分配中心	LU	逻辑单元
PLU	一级逻辑单元	PU	物理单元
RU	请求/响应单元	RH	请求/响应报头
SLU	二级逻辑单元	SDLC	同步数据链路控制协议
SSCP	系统服务控制点	SNA	系统网络结构

机 构 名 称

ANSI	美国国家标准协会	CCITT	国际电报电话咨询委员会
ISO	国际标准化组织	NBS	国家标准局
NSA	国家保密局		

验 证 和 鉴 别 的 有 关 参 数

AP	鉴别参数	BID	银行识别符
CRV	密码验证	DGS	数字签名
ID	用户识别符	MAC	报文鉴别码
PAC	个人鉴别码	PAN	原始帐号
PIN	个人识别号	RN	随机数
Tcard	由银行卡产生的时变信息	TID	终端识别符
TOD	日时钟	TR	交易请求
Tterm	由终端产生的时变信息	Rf	参考值
Z	初始化向量		

目 录

第一章 密码术在电子数据处理中的作用	(1)
第一节 密码术、保密与数据安全	(1)
一、攻击方法	(1)
二、私人保密法的技术含义	(3)
第二节 数据加密标准	(5)
第三节 有效的密码保密性的论证	(6)
第四节 密码术的展望	(7)
第二章 分组密码和序列密码	(11)
第一节 密码算法	(11)
一、加密和脱密	(12)
二、工作因子	(15)
三、攻击的类型	(16)
四、算法设计	(16)
第二节 分组密码	(18)
一、传统算法	(20)
二、公开密钥算法	(25)
三、RSA 算法	(26)
四、陷门渐缩算法	(36)
第三节 序列密码	(40)
第四节 带链接的分组密码	(47)
一、数据内部的模式	(47)
二、使用可变密钥的分组链接	(50)
三、使用明文与密文反馈的分组链接	(53)
四、使用密文反馈的自同步方案	(53)
五、分组链接举例	(56)
六、短块加密	(56)
第五节 带链接的序列密码	(65)
一、带有错误传播特性的链接方法	(65)
二、带有自同步特性的链接方法	(68)
三、密码反馈的序列密码	(70)
第六节 填充和初始化向量的影响	(74)
第七节 使用链接技术的密码报文的鉴别	(76)

第八节 分组密码与序列密码的比较	(80)
第三章 数据加密标准	(87)
第一节 密码分类	(87)
第二节 设计标准	(91)
一、破译具有两条密钥带的体制	(91)
二、破译用线性移位寄存器实现的密钥自身密钥密码	(93)
三、破译一种用线性移位寄存器实现的明文自身密钥密码	(99)
四、一种密码的设计	(105)
第三节 数据加密标准的说明	(108)
一、DES每圈密钥向量的产生	(110)
二、弱密钥和半弱密钥	(114)
三、DES算法的详细说明	(118)
四、DES操作过程的总结	(121)
五、数字举例	(122)
六、关于DES方案的某些注释	(123)
七、S盒设计方案的考虑	(123)
第四节 数据加密标准码间相关性的分析	(125)
一、明文与密文之间的相关性	(128)
二、密文与密钥之间的相关性	(138)
三、小结和结论	(147)
第四章 使用密码术的通信保密和文件保密	(150)
第一节 网络	(150)
第二节 网络加密方式	(152)
第三节 链路加密的基本原理	(155)
一、异步	(157)
二、字节同步	(158)
三、位同步	(158)
第四节 端对端加密概述	(159)
第五节 密钥分配	(161)
一、密钥的说明	(161)
二、对发送的数据加密举例	(169)
三、对数据文件加密举例	(171)
第六节 密码装置	(173)
第七节 密钥保护	(175)
一、终端密钥的保护	(175)
二、主机密钥的保护	(175)
三、密钥的分级结构	(179)
第八节 主机密码系统	(181)

第九节	基本密码操作.....	(183)
一、	终端的密码操作.....	(184)
二、	主机的密码操作.....	(188)
三、	密钥奇偶性.....	(193)
四、	密钥的分割.....	(193)
第十节	密码宏指令.....	(196)
第十一节	密钥管理宏指令.....	(201)
一、	GENKEY和RETKEY 宏 指令.....	(201)
二、	GENKEY和RETKEY宏 指令的使用.....	(205)
第十二节	密钥数据集.....	(206)
第十三节	小结.....	(208)
第五章	主机系统的密码操作.....	(211)
第一节	使用预制初级密钥的单域通信保密.....	(211)
第二节	使用动态产生初级密钥的单域通信保密.....	(213)
一、	两个主密钥.....	(214)
二、	要求.....	(215)
第三节	使用动态产生初级密钥的单域通信和文件保密.....	(216)
一、	存贮加密数据所带来的问题.....	(216)
二、	三个主密钥.....	(217)
三、	文件加密一例.....	(219)
四、	要求.....	(220)
第四节	多域加密.....	(221)
一、	通信保密的协议.....	(221)
二、	文件保密的协议.....	(222)
三、	传送一份新文件.....	(224)
四、	传送一份现有文件.....	(226)
第五节	附带的保密问题.....	(226)
第六节	密码操作的扩展.....	(227)
一、	使用合成密钥的密钥分配.....	(228)
二、	合成密钥协议.....	(228)
第七节	小结.....	(232)
第六章	密钥的产生、分配和安装.....	(234)
第一节	主机主密钥的产生.....	(234)
一、	掷币法.....	(235)
二、	投骰法.....	(235)
三、	随机数表法.....	(235)
第二节	密钥加密密钥的产生.....	(236)
一、	一种弱的密钥产生程序.....	(237)

二、	一种强的密钥产生程序	(237)
三、	产生密钥加密密钥的另一种方法	(239)
四、	用主密钥变量来加密密钥	(241)
五、	密钥的更换	(241)
第三节	数据加密密钥的产生	(245)
一、	用密码装置来产生密钥的一种方法	(246)
二、	产生数据加密密钥的另一种方法	(246)
第四节	在主机处理器输入主密钥	(247)
一、	硬线连接输入	(248)
二、	间接输入	(250)
第五节	通过外部操作进行攻击	(251)
第六节	终端主密钥的输入	(251)
一、	联机检测	(251)
二、	脱机检测	(252)
第七节	密钥的分配	(254)
第八节	密钥的丢失	(255)
第九节	密钥还原技术	(256)
第十节	小结	(257)
第七章	密码术与通信体系结构的结合	(259)
第一节	单域网络中的会话级密码术	(260)
一、	透明的操作方式	(260)
二、	非透明的操作方式	(265)
第二节	单域网络中的私人秘密密码术	(269)
第三节	多域网络中的会话级密码术	(269)
第四节	应用程序对应用程序密码术	(273)
第五节	填充字符的考虑	(273)
第八章	采用密码术的鉴别技术	(276)
第一节	基本概念	(276)
第二节	符号交换	(276)
第三节	报文鉴别	(278)
一、	报文源的鉴别	(279)
二、	报文时间性的鉴别	(282)
三、	报文内容的鉴别	(283)
四、	报文收方的鉴别	(287)
五、	报文鉴别的方法	(287)
第四节	非时变量数据的鉴别	(289)
一、	通行字的鉴别	(289)
二、	采用主机主密钥产生的测试码模式的鉴别	(292)

三、 密钥鉴别的方法.....	(300)
四、 采用主机主密钥产生的测试码模式的另一种鉴别方法.....	(300)
第九章 数字签名	(305)
第一节 签名的意义.....	(305)
一、 认可法.....	(306)
二、 代理法.....	(306)
三、 统一商业法.....	(306)
四、 造成意外事件的疏忽.....	(307)
第二节 数字签名的获得.....	(308)
第三节 通用签名.....	(309)
一、 采用公开密钥算法的方法.....	(309)
二、 采用传统算法的方法.....	(312)
第四节 仲裁签名.....	(321)
一、 一种采用DES算法的方法.....	(322)
二、 仲裁签名举例.....	(323)
三、 弱的方法.....	(324)
四、 其它的弱方法.....	(325)
第五节 用 DES 来得到公开密钥的特性.....	(326)
一、 计算机网络的密钥公证系统.....	(327)
二、 一种采用主机主密钥变量的方法.....	(330)
第六节 数字签名的合法化.....	(331)
一、 原始书面协定.....	(332)
二、 法律的选择.....	(332)
三、 法庭公告的承认.....	(333)
第十章 密码术在以个人识别号为基础的电子资金传送系统中的应用	(337)
引 言.....	(337)
第一节 PIN的基本概念.....	(338)
一、 为什么要使用PIN.....	(338)
二、 PIN的保密.....	(338)
三、 PIN的长度.....	(339)
四、 可容许的PIN输入尝试次数.....	(340)
五、 PIN的发行.....	(341)
六、 本地交易的PIN证实.....	(346)
七、 交换交易的PIN证实.....	(347)
八、 小 结.....	(349)
第二节 EFT的欺 诈 威 胁.....	(349)
一、 EFT的 欺 诈 种 类.....	(350)
二、 被动欺 诈 威 胁.....	(351)

三、	有关的危险	(353)
四、	主动欺诈威胁	(353)
五、	欺诈与责任	(355)
六、	小结	(357)
第三节	防欺诈的原则	(358)
一、	密码术——防欺诈的工具	(358)
二、	防被动欺诈威胁	(358)
三、	防主动欺诈威胁	(359)
四、	交换环境中的防欺诈	(363)
五、	小结	(365)
第四节	防欺诈方法的实现	(365)
一、	建议硬件实现的保密组件应具有某些特性	(366)
二、	建议保密组件应具有某些功能	(366)
三、	PIN的证实	(368)
四、	密钥的管理	(368)
五、	MAC 的产生	(369)
六、	应用	(370)
七、	小结	(372)
第十一章	密码术在电子资金传送系统中的应用	
	——个人识别号和个人密钥	(374)
第一节	基础知识	(374)
第二节	关于 EFT 系统中的泄密问题	(376)
一、	通信线路保密	(377)
二、	计算机保密	(377)
三、	终端保密	(377)
四、	银行卡的保密	(379)
第三节	系统用户的识别和鉴别	(380)
一、	可变的用户特征	(380)
二、	不可变的用户特征	(380)
第四节	个人验证和报文鉴别的要求	(380)
一、	鉴别参数	(381)
二、	个人鉴别码	(383)
三、	只用AP 的个人验证	(383)
四、	使用AP和PAC的个人验证	(384)
五、	使用MAC 的报文鉴别	(385)
六、	EFT 的保密要求	(386)
七、	对 EFT 保密要求的评论	(391)
第五节	在联机方式下的个人验证	(391)

一、	用相关的PIN和相关的个人密钥来进行个人验证	(391)
二、	用独立的PIN和独立的个人密钥来进行个人验证	(393)
三、	减少卡片存贮要求	(398)
第六节	脱机方式和无主机方式的个人验证	(401)
一、	使用PIN产生密钥由系统选择PIN的个人验证	(402)
二、	使用偏移量由用户选择PIN的个人验证	(403)
三、	使用 PAC 由用户选择PIN的个人验证	(403)
第七节	密码设计指南	(405)
一、	PIN保密的主要威胁	(409)
二、	密钥管理的要求	(410)
三、	对磁卡上存贮的密钥保密的威胁	(414)
第八节	PIN/系统密钥方法	(416)
一、	关于PIN/系统密钥方法的密钥管理的考虑	(418)
二、	防止误传的攻击	(419)
三、	用于非交换环境的PIN/系统密钥方法	(423)
四、	用于交换环境的PIN/系统密钥方法	(425)
五、	PIN/系统密钥方法的缺点	(425)
六、	PIN/系统密钥方法的优点	(426)
第九节	PIN/个人密钥方法	(427)
一、	关于应用磁卡的PIN/个人密钥方法的说明	(427)
二、	关于PIN/个人密钥方法的密钥管理的考虑	(428)
三、	PIN/个人密钥方法的优点	(428)
四、	采用磁卡的PIN/个人密钥方法的缺点	(429)
五、	采用智能保密卡的个人密钥方法	(430)
第十节	使用智能保密卡的PIN/个人密钥/系统密钥 (混合密钥管理)方法	(434)
一、	关于混合密钥管理方法的说明	(435)
二、	混合密钥管理方法的设想	(438)
三、	非交换环境中的混合密钥管理方法	(438)
四、	交换环境中的混合密钥管理方法	(442)
五、	智能保密卡的密码考虑	(444)
六、	用数字签名来增强保密性	(445)
七、	优点	(446)
第十一节	密钥管理的设想—对称算法与非对称算法	(447)
一、	保密鉴别和非保密鉴别	(448)
二、	不要鉴别的保密	(452)
第十二节	使用智能保密卡和公开密钥算法的密码系统	(455)
一、	公开密钥管理方法的说明	(456)

二、	关于非对称算法的密钥管理问题.....	(459)
三、	脱机应用.....	(460)
四、	在交换和非交换环境中的联机应用.....	(461)
第十三节	小结.....	(466)
第十四节	术语汇编.....	(466)
第十二章	密码系统的保密测度.....	(472)
第一节	数学密码学的元素.....	(473)
一、	传统密码体制中的信息流.....	(473)
二、	具有报文概率和密钥概率的密码.....	(474)
三、	随机密码.....	(477)
四、	在有多余度的语言中的有意义报文的数量.....	(478)
第二节	随机密码保密性的概率测度.....	(479)
一、	仅用密文进行密码分析时获得密钥的概率.....	(479)
二、	英语简单代替举例 (仅知密文)	(482)
三、	当明文和对应的密文可供密码分析使用时获得密钥的概率.....	(484)
四、	获得明文的概率.....	(484)
第三节	香农信息论方法的一种推广.....	(486)
一、	信息测度.....	(487)
二、	只有密文进行密码分析时密码的唯一解码量.....	(488)
三、	当明文和对应密文可用于分析时密码的唯一解码量.....	(489)
四、	$H(X Y)$ 、 $H(K Y)$ 和 $H(K X, Y)$ 之间的关系.....	(490)
五、	数据加密标准的唯一解码量.....	(491)
第四节	作为保密测度的工作因子.....	(492)
一、	破译密码的代价和时间.....	(493)
二、	英语简单代替—某些预备知识.....	(493)
三、	对英语简单代替进行双字母频率分析的实验结果.....	(495)
四、	对英语简单代替进行单字母频率分析的实验结果.....	(497)
五、	结果的比较.....	(498)
附录 A	FIPS 出版物 第 46 号.....	(502)
附录 B	有关的补充计算.....	(510)
	时间—存贮空间权衡法.....	(510)
	生日悖论.....	(511)
附录 C	塑料卡片的编码方法及标准.....	(513)
	一般的物理特性.....	(513)
	磁道 1.....	(513)
	磁道 2.....	(514)
	磁道 3.....	(515)
附录 D	某些密码原理及其攻击方法.....	(517)