〔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
保密系統設計与实現指南

卡 尔·H·迈 耶
斯 蒂 芬·M·马 特 斯 著

黄朝载 杜银山 陈蔚文 王 宪
付爭少 吴兴龙 何如賢 卢起骏 译

卢 起 骏 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詳细的闡述。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闡述密码基础理论，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闡述。

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，后来又在美国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。

譯 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与实现指南》。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
CFB	密码反馈
ICV	初始链接值
OFB	输出反馈(参见密钥自身密钥密码)
Y	密文
DEA	数据加密算法(ANSI，与DES同义)
PKC	公开密钥密码体制
CE	压縮编码
ECB	电子密本（参见分组密码）
OCV	输出链接值
X	明文
Z	初始化向量（与ICV同义）
DES	数据加密标准（NBS）
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
KC	初级通信密钥（与会话密钥同义）
KI	交换密钥
KN	二级密钥
KNF	二级节点文件密钥
KPG	个人密钥产生密钥，用来从ID产生KP
KS	会话密钥
KT	常驻终端密钥
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
KA	鉴别密钥
KF	初级文件密钥
KMT	终端主密钥
KNC	二级（节点）通信密钥
KP	个人密钥
KPN	PIN产生密钥，用来从ID产生PIN
KSTR	交易会话密钥
KTR	交易密钥

密 码 操 作

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

GSK2 产生会话密钥2（主机）
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）
WMK 写主密钥（终端）
LKD 直接装入密钥（终端）
SMK 置主密钥（主机）

密码宏指令

CIPHER 密码
RETKEY 还原密钥
GENKEY 产生密钥

系统术语

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

机构名称

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

验证和鉴别的有关参数

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

目　录