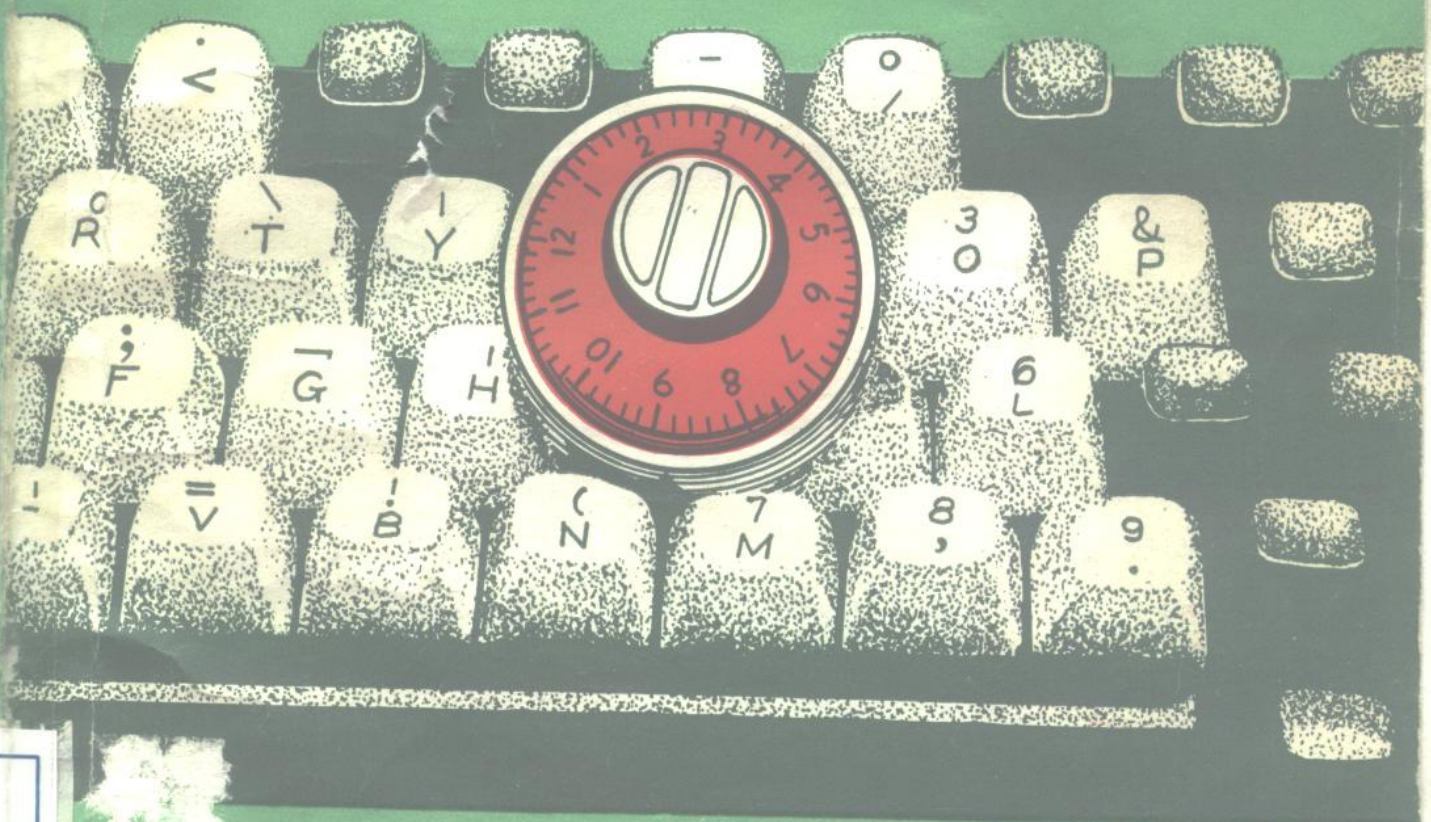
密码学

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的教材或参考书。

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）

〔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
责任编辑 王绍李 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33 1/2 766千字
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。

第六章的主要内容为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黾黾逼人的挑战，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和困难。

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