普通高等院校电子信息类系列教材

XIANDAI MIMAXUE

现代密码学

（第2版）

任伟◎编著

北京邮电大学出版社
www.buptpress.com

普通高等院校电子信息类系列教材

现代密码学

（第2版）

任伟 编著

北京邮电大学出版社
www. buptpress. com

内 容 简 介

本书内容包括密码学概述、古典密码体制、信息理论安全、序列密码、分组密码、Hash 函数和消息鉴别、公钥加密(基础)、公钥加密(扩展)、数字签名、实体认证与身份识别、密钥管理。本书的特点是注重介绍知识的内在逻辑性,展现密码学方案设计的内在规律和基本原理,注重使用比较和类比的方式探究一般规律和方法论,使学习者"知其所以然"。在给出方案的同时,还给出具有启发性的解释和讨论,解释方案的设计机理、来源和思路,试图培养学习者的逻辑推理能力和设计密码学方案的创造性思维方式。

本书面向的主要对象包括高等学校信息安全、密码学、电子对抗、应用数学、计算机科学、通信工程、信息工程、软件工程等专业本科高年级学生和研究生。对具有密码学基础的研究人员也有启发作用和参考价值。

图书在版编目(CIP)数据

现代密码学 / 任伟编著. --2 版. --北京: 北京邮电大学出版社, 2014.1
ISBN 978-7-5635-2294-1

Ⅰ.①现… Ⅱ.①任… Ⅲ.①密码—理论 Ⅳ.①TN918.1

中国版本图书馆 CIP 数据核字 (2013) 第 296116 号

书　　名: 现代密码学(第 2 版)
著作责任者: 任　伟　编著
责 任 编 辑: 刘　颖
出 版 发 行: 北京邮电大学出版社
社　　址: 北京市海淀区西土城路 10 号(邮编:100876)
发 行 部: 电话: 010-62282185　传真: 010-62283578
E-mail: publish@bupt.edu.cn
经　　销: 各地新华书店
印　　刷: 北京源海印刷有限责任公司
开　　本: 787 mm×1 092 mm　1/16
印　　张: 15.5
字　　数: 373 千字
印　　数: 1—3 000 册
版　　次: 2011 年 4 月第 1 版　2014 年 1 月第 2 版　2014 年 1 月第 1 次印刷

ISBN 978-7-5635-2294-1　　定　价: 32.00 元

序言

一本好的教材不仅要教给读者知识，更重要的是要给读者以启迪。任伟博士的新著《现代密码学》不但“授人鱼”而且更“授人以渔”。

“现代密码学”是一门既难学，更难讲的重要基础课程。它既要求学生具备良好的数学基础，更要求教师的讲解要深入、透彻，如果没有一本很好的教材，那么，无论是老师还是学生都将在它面前一筹莫展。

为了向读者展示现代密码学中的逻辑思维过程，启发读者的创造性，尽可能地让读者真正学懂现代密码学的精髓，本书作者可谓是使尽了浑身解数：演绎法、归纳法、关联法、典型示例法、方案比较法、特征和规律提炼法等方法层出不穷；浅显的解释、历史的回顾、现状的综述、前景的展望等尽情发挥；内在基本原理的揭示、理论与技术的推广讨论、全面的扩展思维等无所不包。

作为一本专著，本书取材独具一格，内容翔实，覆盖面广，组织结构由浅入深，思维周到严谨，富有逻辑性。作为一本教材，本书讲解通俗易懂，举例丰富，分析透彻，可读性强。本书的特别之处还在于它论述的视角独特，注重对一般规律和基本原理的论述，包含了大量的知识归纳和前后逻辑的关联和比较，颇具启发性。本书对深入理解现代密码设计的内在机制，提高应用密码学知识的创新能力是一次有益的尝试，对现有密码学书籍是有益的开拓和补充。该书的出版必将有助于推动我国现代密码学的教学和科研工作。

灵创团队带头人

北京邮电大学信息安全中心主任

灾备技术国家重点实验室主任

国家级精品课程“现代密码学”负责人

国家级教学名师、博士导师、长江学者

前言

目前市场上已经有很多密码学书籍，但普遍存在的一个问题就是大部分书中对原理、原则和设计机理等内在机制的讲解仍不充分，学生在学习了各种方案后，不理解这些方案是如何设计出来的，特别是不知道这些方案是如何想出来的，不知道其来龙去脉，没有理解方案设计中内在的逻辑性，没有“真正学懂”，以至于疲于死记硬背方案本身，导致学生无法学以致用，尤其缺乏设计安全方案的能力。同时，目前的教材在思维的启发性方面、学生创造性能力培养方面仍然有待完善。本书有意识地引导学生思考，培养他们的逻辑推理能力，发散性思维能力，知识的归纳能力，以及灵活运用所学知识的能力。

本书也是一本旨在让学习者能够“真正学懂密码学”的密码学教材。“密码学”是信息安全专业、密码学专业、电子对抗等专业中一门最重要的专业课，在学科知识体系中占据重要的地位。但是，多年的教学实践以及学生的体会表明，它也是一门非常难学（和难讲授）的一门综合课程，其数学基础涉及算法数论、计算复杂性、抽象代数、信息论、概率论等，讲授的内容覆盖面广，各知识点均具有一定难度和深度。因此，“真正讲透或学懂密码学”对于教与学双方都是一个挑战。

“真正学懂”意味着对知识的深刻理解、对一般规律的认识，甚至是融会贯通、应用自如。本书在这个方面可能是一次有益的尝试。每章内容的组织是从整体全貌到局部细节，从一般模型到具体方案（先讲模型、分类，再介绍具体构造方案）。介绍具体内容时遵照学习规律，从易到难，从简单方案到改进方案，还原历史发展的原貌和变迁，突出来龙去脉（如在介绍公钥方案的提出时，先介绍 Merkle 谜题，Pohlig-Hellman 对称密钥分组加密，Merkle-Hellman 背包公钥密码方案，最后介绍 RSA 方案）。讲解内容时深入浅出，简洁、直观、易懂，使用浅显的语言表述深奥的内在规律。在介绍完多个具体方案后，再归纳一般规律，从具体到抽象，从具体方案中提炼出一般规律和原理（如从 ElGamal 签名、DSA 等到一般 ElGamal 签名，从基于身份识别协议到知识签名）。大部分方案给出实例（如实际数据）进行直观地讲解。此外，本书还大量采用类比法、比较法、归纳法、图示法，试图使读者对所学内容能够反复巩固，前后联系。

写作本书时还特别遵循了以下思路：

（1）注重启发性。改变了目前教材中以罗列密码学方案为主，缺乏对设计原理的分析，对设计的动机和逻辑性的解释的局面。让学习者知其然，也知其所以然。

（2）注重知识点的逻辑联系和类比。章节间和章节中前后各个分离的知识点间的联系和类比关系，明确给出各知识点间的关联并加以强调，便于读者体会密码算法或协议设计的奥妙。

（3）注重原理的总结和推广。在具体构造方案介绍后，给出一般性构造方案，或者加以讨论和提炼总结，有利于知识的理解，举一反三。

（4）广度和深度兼具。基本原理，基本概念的讲解力求透彻，有深度。通过扩展阅读提高广度，便于回顾经典论文或者了解最新的国际国内发展动态。

（5）内容新颖。给出了基于计算复杂性的现代密码学的基本概念、原则。论述了可证明安全性理论的基础知识，如随机预言模型、安全定义、规约证明方法。解决了学生学完密码学课程后，无法看懂现代密码学论文的一个窘境。

全书共分 11 章：第 1 章对密码学做一个概述；第 2 章介绍古典密码体制；第 3 章介绍信息理论安全；第 4 章介绍序列密码；第 5 章介绍分组密码；第 6 章介绍 Hash 函数和消息鉴别；第 7 章介绍公钥加密（基础）；第 8 章介绍公钥加密（扩展）；第 9 章介绍数字签名；第 10 章介绍实体认证与身份识别；第 11 章介绍密钥管理。

全书精心安排了示例。为帮助读者进一步对内容的拓展研究，还有针对性地提供了进一步阅读建议，用于开展课外学习和论文研读讨论。每章小结归纳了本章知识点，并指出重点和难点，便于复习。打 * 号的章节可选学。

本书面向的主要对象包括高等学校信息安全、密码学、电子对抗、应用数学、计算机科学、通信工程、信息工程、软件工程等专业本科高年级学生和研究生。对具有密码学基础的研究人员也有启发作用和参考价值。

第 2 版中更新了参考文献以及对文献的阅读建议，并对书中内容作了较多增删调整。

本书受到国家自然科学基金资助（No. 61170217），湖北省教育厅高等学校教学研究项目资助（No. 2011123）以及中国地质大学（武汉）实验技术研究经费（SJC-201214）的资助，在此表示感谢。

特别感谢长江学者北京邮电大学杨义先教授为本书第 1 版作序。由于作者水平有限，在此衷心希望读者提出意见和建议，便于本书进一步改进，我的 E-mail 是：weirencs@cug.edu.cn。

作者

2013 年 8 月

目 录

第1章 密码学概述

1.1 密码学的目标与知识构成

随着信息社会的发展，信息安全成为一个需要解决的关键问题。针对信息安全的攻击，主要包括主动攻击和被动攻击。被动攻击主要是信息的截取(interception)，指未授权地窃听传输的信息，企图分析出消息内容或者是通信模式。主动攻击包括：(1)中断(interruption)，阻止通信设施的正常工作，破坏可用性；(2)篡改(modification)，更改数据流；(3)伪造(fabrication)，将一个非法实体伪装成一个合法的实体；(4)重放(replay)攻击，将一个数据单元截获后进行重传。

信息安全的目标是确保信息的安全性。安全目标通常包括如下几项。

(1) 机密性(confidentiality)。指保证信息不泄露给非授权的用户或者实体，确保保存的信息和被传输的信息仅能被授权的各方得到，而非授权用户即使得到信息也无法知晓信息的内容。通常通过访问控制机制阻止非授权的访问，通过加密机制阻止非授权用户知晓信息的内容。

(2) 完整性(integrity)。指消息未经授权不能进行篡改，要保证消息的一致性。即消息在生成、传输、存储和使用过程中不应发生人为或者非人为地非授权篡改(插入、修改、删除、重排序等)。一般通过访问控制阻止篡改行为，同时通过消息摘要算法来检测信息是否被篡改。

(3) 认证性(authentication)。指确保一个消息的来源或者消息本身被正确地标识，同时确保该标识没有被伪造，认证分为消息鉴别和实体认证。消息鉴别是指接收方保证消息确实来自于所声称的源；实体认证指能确保被认证实体是所声称的实体。

(4) 不可否认性(non-repudiation)。指能保证用户无法事后否认曾经对信息进行的生成、签发、接收等行为。当发送一个消息时，接收方能证实该消息确实是由既定的发送方发来的，称为源不可否认性；同样，当接收方收到一个消息时，发送方能够证实该消息确实已经送到了指定的接收方，称为宿不可否认性。一般通过数字签名来提供不可否认服务。

(5) 可用性(availability)。指保障信息资源随时可提供服务的能力。即授权用户根据需要可以随时访问所需信息，保证合法用户对信息资源的使用不被非法拒绝。典型的对可用性的攻击是拒绝服务攻击。

除了以上一些主要目标外，还有隐私性(privacy)、匿名性(anonymity)等。

为达到上述目标，信息安全采用了信息论、计算机科学和密码学等方面的知识，形成了一门综合学科，其主要任务是研究计算机系统和通信网络中信息的保护方法，以及实现系统和网络中信息的机密性、完整性、认证性、不可否认性、可用性等目标，其中密码学是实现信

息安全目标的核心技术。

密码学(cryptology)研究实现信息安全各目标的相关的数学、方法和技术。密码学不是提供信息安全的唯一方式。其研究的目标是信息安全目标的一个子集，主要包括机密性、完整性、认证性、不可否认性。为实现上述目标，密码学结合数学、计算机科学、电子与通信等诸多学科的方法于一体，是一门交叉学科。从大的方面可分为密码编码学和密码分析学两类，对应于密码方案的设计学科和密码方案的分析学科。

密码学在设计方案的时候，首先需要考虑方案所能达到的安全性。通常，衡量密码体制安全性的基本准则有以下几种。

(1) 计算安全(computational security)。如果攻破一个密码体制所需要的计算能力和计算时间是现实条件所不具备的，就认为相应的密码体制满足计算安全。

(2) 可证明安全(provable security)。如果攻破一个密码体制意味着可以解决某一个经过深入研究的数学难题，就认为相应的密码体制满足可证明安全。

(3) 无条件安全(unconditional security)。如果假设攻击者在无限计算能力和计算时间的前提下，也无法攻破该体制，则认为相应的密码体制满足无条件安全。

通常现代密码学强调达到可证明安全性，这通常是计算安全的。即安全具有一定的等级，这种等级通常通过攻破方案所需要的工作量来衡量。

除了安全性外，还需要考虑到如下几个方面。

(1) 功能性。方案能够满足安全需求。

(2) 性能。方案的计算、存储、传输等各方面的效率。

(3) 容易实现性。在实际中实施方案的难易程度。包括在软件和硬件环境中实现密码要素的复杂度。

上述方面往往在实际应用中需要权衡，如在一个计算能力有限的环境中，为了系统整体上具有良好的性能，可能不得不割舍高级别的安全性。

围绕着密码学要达到的目标，可以将密码学的实现方案分类成各种工具。图 1.1 给出了密码学内容的构成，图 1.2 围绕着安全目标给出了各内容间的联系。

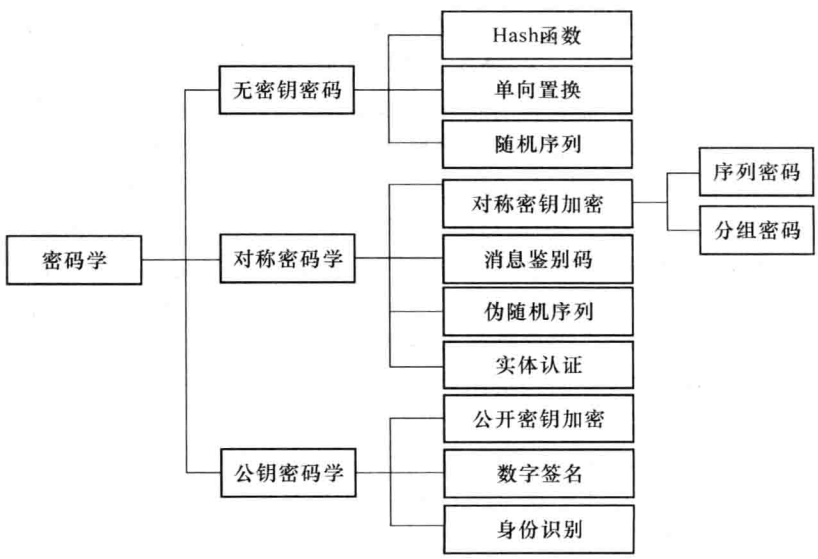

图 1.1　密码学的内容构成

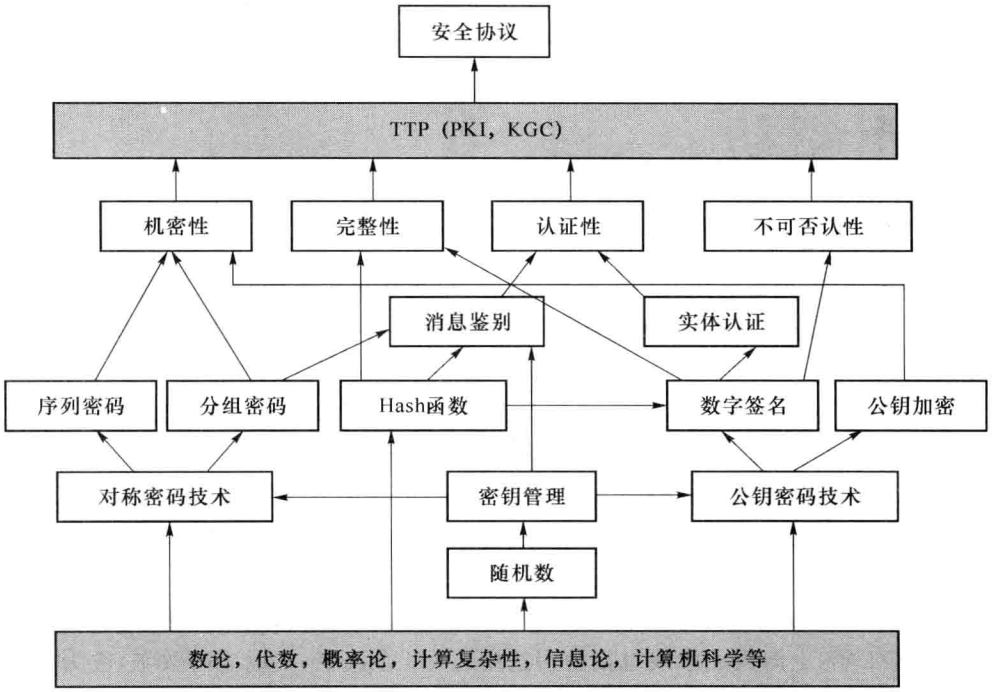

图 1.2 密码学研究内容间的联系

1.2 密码学的发展简史

从整体上来说，密码学经过了人工密码，到机械密码，到电子计算机密码的发展历程。下面按年代顺序列出密码学发展中的重要事件。

1. 古典密码时期

(1) 公元前 1900 年左右，一位佚名的埃及书吏在碑文中使用了非标准的象形文字，或许是目前已知最早的密码术实例。

(2) 公元前 400 多年，古希腊斯巴达军队中使用的 Scytale 密码，是一种置换密码。

(3) 公元前 1 世纪，古罗马帝国皇帝 Caesar 曾经使用有序的单表代换密码，即 Caesar 密码，是单表代换密码的代表。

(4) 我国宋代曾公亮、丁度等编撰的《武经总要·字验》中记载，北宋前期，在作战中曾用一首五言律诗的 40 个汉字，分别代表 40 种情况或要求，这种方式已具备了密码本的特点。

(5) 欧洲的密码学起源于中世纪的罗马和意大利。约在 1379 年，欧洲第一本关于密码学的手册由生活在意大利北部城市 Parma 的 Gabriela de Lavinde 写成，它由几个加密算法组成，且为罗马教皇 Clement 七世服务。

(6) 阿拉伯人是第一个清晰地理解密码学原理的人，他们设计并使用代换和换位加密，并且发现了密码分析中的字母频率分布关系。大约在 1412 年，波斯人 al-Qalqashandi 所编的百科全书中的第 14 卷载有破译简单代换密码的方法。这是密码分析法最早的著作之一。

(7) 大约在1467年左右,意大利佛罗伦萨的建筑师Alberti发明了多字母表替代密码,他设计了一个密码盘,该盘有一个大一些的外轮和一个小一些的内轮,并各自以明文字符和密文字符做索引。字母的排列确定了一个简单替代并且可在加密一些字之后通过转动盘来修改替代方式。

(8) 1508年,密码学的第一本印刷书籍 *Polygraphic* 由德国的僧侣Trithemius写成,并在1518年出版,其中包含了第一个基于24个字符的方形表,该表列出了明文字母表字符在一个固定次序下的所有移位替代。

(9) 17世纪,英国著名的哲学家弗朗西斯·培根在他所著的《学问的发展》一书中最早给密码下了定义,他说:"所谓密码应具备三个条件,即易于翻译、第三者无法理解、在一定场合下不易引人注意。"

(10) 1854年,Playfair密码(Playfair Cipher)由C. Wheatstone提出的,此后由他的朋友L. Playfair将该密码公布,所以就称为Playfair密码。

(11) 1858年,维吉尼亚密码(Vigenere Cipher)由法国密码学家B. D. Vigenere提出。

(12) 1860年,密码系统在外交通信中已得到普遍使用。如在美国国内战争中,联邦军广泛地使用换位加密,主要是使用Vigenere密码。

(13) 1863年Kasiki测试法由普鲁士军官F. Kasiski提出,用于分析多表代换的周期。

(14) 1871年,上海大北水线电报公司选用6 899个汉字,代以4码数字,成为中国最初的商用密码本,同时也设计了由明码本改编成密码本并进行混淆的方法。

(15) 1883年,A. Kerckhoffs在《军事密码学》一书中提出了密码系统的安全性的一个基本假设,称为Kerckhoffs假设(原则),即密码分析者知道所使用的密码算法。

(16) 1917年,Vernam密码由美国AT&T公司的G. Vernam为电报通信设计的非常简单方便的密码。它奠定了序列密码的基础。

(17) 1918年,W. F. Friedman的论文《重合指数及其在密码学中的应用》(*The Index of Coincidence and Its Applications in Cryptography*),给出了多表代换密码的破译方法,是1949年之前最重要的密码文献。

(18) 1929年,希尔密码(Hill Cipher)由数学家L. Hill提出。

古典密码时期密码技术仅是一门文字变换艺术,其研究和应用远没有形成一门科学,最多只能称其为密码术。

2. 近代密码时期

(1) 20世纪20年代,随着机械和机电技术的成熟,以及电报和无线电需求的出现,引起了密码设备方面的一场革命——发明了转轮密码机(Rotor),转轮机的出现是密码学发展的重要标志之一,从此出现了商业密码机的公司和市场。

(2) 从1921年开始的接下来的十多年里,美国加州奥克兰的一个名叫Edward Hebern的人构造了一系列改进的转轮机,并应用于美国海军的试用评估,他申请了第一个转轮机的专利,这种装置在差不多50年内被指定为美军的主要密码设备,奠定了第二次世界大战中,美国在密码学方面的超级地位。

(3) 在美国的Herbern发明转轮密码机的同时,欧洲的工程师们如荷兰的Hugo Koch、德国的Arthur Scherbius都独立地提出了转轮机的概念。Authur Scherbius于1919年设计出了历史上著名的密码机——德国的Enigma机(意思是"谜")。1930年,日本的第一转

轮密码机(美国分析家称之为RED)开始为外交部服务。1939年,日本人引入了一个新的加密机(美国分析家称之为PURPLE),其中的转轮机用电话步进交换机取代。

(4) 第二次世界大战是人工加密时代转变为机械加密时代的转折点。转轮密码机的大量使用极大提高了加解密速度,同时抗攻击性能有很大的提高,是密码学发展史上的一个里程碑。同时,密码分析最伟大的成功发生在"二次大战"期间,波兰人和英国人破译了Enigma密码,美国人攻破了日本的RED、ORANGE和PURPLE密码,对盟军在二次大战中获胜起到了关键性作用。

近代密码时期可以看作是科学密码学的前夜,这阶段的密码技术可以说是一种艺术,是一种技巧和经验的综合体,但还不是一种科学,密码专家常常是凭直觉和信念来进行密码设计和分析,而不是推理和证明。因此,也有学者将古典、近代密码时期划分为一个阶段。

3. 现代密码时期

(1) 1949年,Shannon在*Bell Systems Technical Journal*上发表了《保密系统的通信理论》(*Communication Theory of Secrecy Systems*)一文,用概率和统计等科学工具研究加密系统,为密码学奠定了坚实的理论基础,从此密码学从艺术变为科学。

(2) 1967年,Kahn出版了《破译者》(*The Codebreakers*)一书,对密码学的历史进行了相当完整的记述,使成千上万原本不知道密码学的人了解了密码学。从此,密码学研究引起了民间的兴趣。他认为是阿拉伯人创造了"加密法(cipher)"一词。

(3) 1973年,美国国家标准局(NBS,现在是美国国家标准技术研究所NIST)在全世界范围征求国际密码标准方案(DES)。4年后,发布正式的标准DES。该方案的公布极大地促进了密码学在民间的研究。

(4) 1976年,W. Diffie和M. Hellman在《密码学的新方向》一文中提出公钥密码体制。这是密码学发展史上最伟大的一次革命,是现代密码学诞生的标志。

(5) Merkle和Hellman于1978年提出了第一个公钥密码系统——背包(knapsack)公钥密码系统,安全性基于NP完全问题背包问题。

(6) 1978年,美国麻省理工学院(MIT)的Rivest、Shamir和Adleman提出RSA加密机制,这是第一个实用的公钥方案,开创了密码学的新纪元。

(7) 1979年,MIT的M. O. Rabin的Rabin提出第一个可证明安全的公钥密码体制。

(8) 1979年,L. Lamport提出基于任意单向函数的一次签名方案。

(9) 1984年,S. Goldwasser与S. Micali提出了概率公钥密码系统的概念,并提出Goldwasser-Micali概率公钥密码系统。

(10) 1984年,IBM公司的Benett和Montreal大学的Brassard,提出第一个量子密码学方案,称为BB84协议。它是以量子力学基本理论为基础的量子信息理论领域的第一个应用,并提出了一个量子密钥交换的安全协议,由此迎来了量子密码学的新时期。

(11) 1985年,ElGamal密码体制由T. ElGamal提出,基于的困难问题是群中的离散对数问题。

(12) 1985年,T. ElGamal提出一个基于离散对数问题的数字签名体制,称为ElGamal数字签名体制。

(13) 1985年,N. Koblitz和V. Miller提出了椭圆曲线密码系统(Elliptic Curve Cryptography,ECC),实现了公钥密码体制在效率上的重大突破。