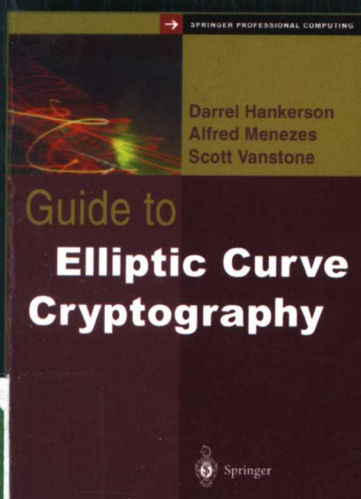


椭圆曲线密码学导论

Guide to Elliptic Curve Cryptography



Darrel Hankerson

[加] Alfred Menezes 著

Scott Vanstone

张焕国 等译



电子工业出版社

Publishing House of Electronics Industry

<http://www.phei.com.cn>

国外计算机科学教材系列

椭圆曲线密码学导论

Guide to Elliptic Curve Cryptography

Darrel Hankerson

[加] Alfred Menezes 著

Scott Vanstone

张焕国 等译

电子工业出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

自 1984 年 Hendrik Lenstra 给出基于椭圆曲线的整数因子分解算法后, 椭圆曲线在密码学和计算机数论中的应用已得到了很大的发展。椭圆曲线密码属于公钥密码体制, 它可以提供与 RSA 密码体制同样的功能, 其安全性建立在椭圆曲线离散对数问题的困难性之上。本书主要是为安全专业人员、技术开发人员和致力于椭圆曲线密码应用的人员提供的, 介绍了有限域算法, 椭圆曲线算术, 针对椭圆曲线离散对数问题的攻击, 椭圆曲线参数组和密钥对的生成与确认, 数字签名、公钥加密和密钥协商的椭圆曲线协议选择, 椭圆曲线密码的软件和硬件实现, 旁门攻击技术及其预防对策, 等等。此外, 本书还为读者提供了大量的算法与参考文献。

本书自成体系, 适用于计算机科学、计算机工程、网络设计和网络数据安全领域的工程技术人员、专家以及研究人员, 也可供大专院校高年级本科生和研究生作为教材使用。

Translation from the English language edition: Guide to Elliptic Curve Cryptography by Darrel Hankerson, Alfred Menezes, and Scott Vanstone.

Copyright © 2004 Springer-Verlag New York, Inc.

Springer-Verlag is a company in the BertelsmannSpringer Publishing group.

All Rights Reserved.

Authorized Simplified Chinese language edition by Publishing House of Electronics Industry. Copyright © 2005.

本书中文简体字翻译版由斯普林格出版公司授予电子工业出版社。未经出版者预先书面许可, 不得以任何方式复制或抄袭本书的任何部分。

版权贸易合同登记号 图字: 01-2004-6032

图书在版编目 (CIP) 数据

椭圆曲线密码学导论 / (加) 汉克森 (Hankerson, D.) 等著; 张焕国等译. - 北京: 电子工业出版社, 2005.8
(国外计算机科学教材系列)

书名原文: Guide to Elliptic Curve Cryptography

ISBN 7-121-01602-8

I. 椭... II. ①汉... ②张... III. 密码 - 理论 - 教材 IV. TN918.1

中国版本图书馆 CIP 数据核字 (2005) 第 085074 号

责任编辑: 谭海平

印 刷: 北京市顺义兴华印刷厂

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编: 100036

经 销: 各地新华书店

开 本: 787 × 980 1/16 印张: 19 字数: 425 千字

印 次: 2005 年 8 月第 1 次印刷

定 价: 38.00 元

凡购买电子工业出版社的图书, 如有缺损问题, 请向购买书店调换; 若书店售缺, 请与本社发行部联系。联系电话: (010) 68279077。质量投诉请发邮件至 zltts@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

出版说明

21世纪初的5至10年是我国国民经济和社会发展的关键时期,也是信息产业快速发展的关键时期。在我国加入WTO后的今天,培养一支适应国际化竞争的一流IT人才队伍是我国高等教育的重要任务之一。信息科学和技术方面人才的优劣与多寡,是我国面对国际竞争时成败的关键因素。

当前,正值我国高等教育特别是信息科学领域的教育调整、变革的重大时期,为使我国教育体制与国际化接轨,有条件的高等院校正在为某些信息学科和技术课程使用国外优秀教材和优秀原版教材,以使我国在计算机教学上尽快赶上国际先进水平。

电子工业出版社秉承多年来引进国外优秀图书的经验,翻译出版了“国外计算机科学教材系列”丛书,这套教材覆盖学科范围广、领域宽、层次多,既有本科专业课程教材,也有研究生课程教材,以适应不同院系、不同专业、不同层次的师生对教材的需求,广大师生可自由选择 and 自由组合使用。这些教材涉及的学科方向包括网络与通信、操作系统、计算机组织与结构、算法与数据结构、数据库与信息处理、编程语言、图形图像与多媒体、软件工程等。同时,我们也适当引进了一些优秀英文原版教材,本着翻译版本和英文原版并重的原则,对重点图书既提供英文原版又提供相应的翻译版本。

在图书选题上,我们大都选择国外著名出版公司出版的高校教材,如Pearson Education培生教育出版集团、麦格劳-希尔教育出版集团、麻省理工学院出版社、剑桥大学出版社等。撰写教材的许多作者都是蜚声世界的教授、学者,如道格拉斯·科默(Douglas E. Comer)、威廉·斯托林斯(William Stallings)、哈维·戴特尔(Harvey M. Deitel)、尤利斯·布莱克(Uyless Black)等。

为确保教材的选题质量和翻译质量,我们约请了清华大学、北京大学、北京航空航天大学、复旦大学、上海交通大学、南京大学、浙江大学、哈尔滨工业大学、华中科技大学、西安交通大学、国防科学技术大学、解放军理工大学等著名高校的教授和骨干教师参与了本系列教材的选题、翻译和审校工作。他们中既有讲授同类教材的骨干教师、博士,也有积累了几十年教学经验的老教授和博士生导师。

在该系列教材的选题、翻译和编辑加工过程中,为提高教材质量,我们做了大量细致的工作,包括对所选教材进行全面论证;选择编辑时力求达到专业对口;对排版、印制质量进行严格把关。对于英文教材中出现的错误,我们通过与作者联络和网上下载勘误表等方式,逐一进行了修订。

此外,我们还将与国外著名出版公司合作,提供一些教材的教学支持资料,希望能为授课老师提供帮助。今后,我们将继续加强与各高校教师的密切联系,为广大师生引进更多的国外优秀教材和参考书,为我国计算机科学教学体系与国际教学体系的接轨做出努力。

电子工业出版社

教材出版委员会

- | | | |
|-----|-----|---|
| 主 任 | 杨芙清 | 北京大学教授
中国科学院院士
北京大学信息与工程学部主任
北京大学软件工程研究所所长 |
| 委 员 | 王 珊 | 中国人民大学信息学院院长、教授 |
| | 胡道元 | 清华大学计算机科学与技术系教授
国际信息处理联合会通信系统中国代表 |
| | 钟玉琢 | 清华大学计算机科学与技术系教授
中国计算机学会多媒体专业委员会主任 |
| | 谢希仁 | 中国人民解放军理工大学教授
全军网络技术研究中心主任、博士生导师 |
| | 尤晋元 | 上海交通大学计算机科学与工程系教授
上海分布计算技术中心主任 |
| | 施伯乐 | 上海国际数据库研究中心主任、复旦大学教授
中国计算机学会常务理事、上海市计算机学会理事长 |
| | 邹 鹏 | 国防科学技术大学计算机学院教授、博士生导师
教育部计算机基础课程教学指导委员会副主任委员 |
| | 张昆藏 | 青岛大学信息工程学院教授 |

译者序

随着计算机和网络技术的高速发展和广泛应用,社会的信息化程度越来越高,但社会对计算机和网络系统的依赖性也越来越大。若计算机和网络系统的安全受到危害,则会危及国家的安全,引起社会的混乱,从而造成重大损失。因此,确保计算机和网络系统的安全已成为世人关注的社会问题,并成为计算机科学技术的热点领域。

众所周知,确保信息系统的安全是一个系统工程,必须从整体考虑,从底层着手,综合采取措施,才能比较有效地确保信息系统的安全。硬件结构的安全和操作系统的安是信息系统安全的基础,而密码等则是关键技术。

密码技术是一门古老的技术,大概自人类社会出现战争便产生了密码。密码的发展经历了由简单到复杂、由古典到近代的发展历程,并且在它发展的各个阶段,都为确保信息安全发挥了重要作用。

1949年香农发表了题为《保密系统的通信理论》这一著名论文,该论文把密码置于坚实的数学基础之上,标志着密码学作为一门科学的形成。1976年 W. Diffie 和 M. E. Hellman 提出了公钥密码的概念,从此开创了一个密码新时代。公钥密码从根本上克服了传统密码在密钥分配上的困难,特别适合计算机网络应用,而且很容易实现数字签名,因而特别受到重视。目前,公钥密码已得到了广泛应用。

在国际上研究比较充分而且公认比较安全的公钥密码有,基于大整数因子分解困难性的 RSA 密码,基于离散对数问题困难性的 ELGamal 密码,以及基于椭圆曲线离散对数问题困难性的椭圆曲线密码等。

人们对椭圆曲线的研究已有 100 多年的历史,而椭圆曲线密码是 Neal Koblitz 和 Victor Miller 于 1985 年提出来的。目前,椭圆曲线密码已成为除 RSA 密码之外呼声最高的公钥密码之一。它可以提供同 RSA 密码体制同样的功能。然而它的安全性建立在椭圆曲线离散对数问题(ECDLP)的困难性之上。现在求解 ECDLP 的最好算法具有全指数时间复杂度,与此不同,整数因子分解问题却有亚指数时间算法。这意味着要达到期望的安全程度,椭圆曲线密码可以使用较 RSA 密码更短的密钥。普遍认为 160 位椭圆曲线密码可提供相当于 1024 位 RSA 密码的安全程度。由于密钥短,所以工程实现的

加解密速度较快,并且可节省能源、带宽和存储空间。正因为如此,一些国际标准化组织已把椭圆曲线密码作为新的信息安全标准。由于椭圆曲线密码具有上述优点,因此椭圆曲线密码特别适于在航空、航天、卫星及智能卡等系统中应用。

加拿大滑铁卢大学的应用密码学研究中心(CACR)是国际著名的椭圆曲线密码研究中心之一。他们在椭圆曲线密码理论与技术方面的研究成果享誉世界。本书的三位作者都是著名的椭圆曲线密码专家。其中Darrel Hankerson是Auburn大学的研究人员,2000年至2004年夏季到滑铁卢大学的应用密码学研究中心(CACR)做访问学者。Alfred Menezes和Scott Vanstone都是滑铁卢大学的教授。

本书全面地介绍了椭圆曲线密码的理论、技术与应用,试图为信息安全专业技术人员和椭圆曲线密码应用人员提供一本椭圆曲线密码的基础书籍。本书的一个显著特点是关键技术都给出了算法,从而为工程实现奠定了基础。内容的叙述是面向各种读者的,以使各类读者都能得到他们所需的知识。而且在每章的末尾给出了广泛的论述,为读者提供了有用的参考。

本书的第1章概述了密码和椭圆曲线密码。第2章介绍了有限域。第3章介绍了椭圆曲线算术。第4章介绍了椭圆曲线密码的各种协议。第5章详细介绍了椭圆曲线密码的软件和硬件实现技术。本书内容丰富,既有理论基础,又有工程实现技术。关键技术算法化,便于实现应用。讲述深入浅出,便于理解。本书是一本难得的好书,既可用做研究生和高年级本科生的教材,也可供从事信息安全、计算机、通信、电子等领域的科技人员参考。

本书的前言、第1章、第2章和第3章由张焕国翻译,第4章、第5章、第6章和附录由王张宜翻译。孟庆树、王邦菊等帮助整理译稿。全书由张焕国统稿和审校。由于译者的专业知识和外语水平有限,书中错误在所难免,敬请读者指正,译者在此先致感谢之意。

译者于武汉珞珈山

2005.8

前 言

代数、代数几何和数论学者对椭圆曲线的研究可追溯到 19 世纪中叶。现在已有大量描述椭圆曲线美好和优雅特性的论著。1984 年, Hendrik Lenstra 给出了一个独具创意的基于椭圆曲线的整数因子分解算法。这一成功推动了研究工作者去开拓椭圆曲线在密码学和计算数论中的其他应用。

公钥密码的概念是由 W. Diffie 和 M. Hellman 于 1976 年提出的。第一个实际的公钥密码是 1977 年 R. Rivest, A. Shamir 和 L. Adleman 提出的 RSA 公钥密码体制。RSA 密码是现在最著名的公钥密码之一, 它的安全性建立在整数因子分解的困难性之上。椭圆曲线密码(ECC)是 1985 年由 N. Koblitz 和 V. Miller 提出的。椭圆曲线密码属于公钥密码体制, 它可以提供同 RSA 密码体制同样的功能。然而它的安全性建立在椭圆曲线离散对数问题(ECDLP)的困难性之上。现在求解 ECDLP 最好的算法具有全指数时间复杂度, 与此不同, 整数因子分解问题却有亚指数时间算法。这意味着对于达到期望的安全程度, 椭圆曲线密码可以使用较 RSA 密码更短的密钥。例如, 普遍认为 160 位的椭圆曲线密码可提供相当于 1024 位 RSA 密码的安全程度。由于密钥短而获得的优点包括加解密速度快、节省能源、节省带宽和节省存储空间。

受众 本书试图为安全专业人员、技术开发人员和致力于椭圆曲线密码应用的人员提供一本基础书籍。内容的叙述是面向各种读者的, 并且假设读者具有不高于大学程度的计算机科学、工程和数学的基础。本书不是写给理论专家的, 它明显缺少数学证明。本书的覆盖面相当宽, 并在每章的末尾给出了大量的文献, 为读者提供了有用的参考。

总体介绍 本书第 2 章集中介绍有限域算术, 第 3 章集中介绍椭圆曲线算术。第 4 章首先介绍针对 ECDLP 的各种攻击方法, 然后介绍椭圆曲线参数组和密钥对的生成与确认, 以及数字签名、公钥加密和密钥协商的椭圆曲线协议选择。本书没有介绍针对 ECDLP 的各种攻击的数学细节, 也没有论述椭圆曲线点的计数算法, 因为许多数学工作者对此已经非常熟悉(以简明易读的形式阐述这些内容本身就是一种极大的挑战)。第 2 章、第 3 章和第 4 章的内容选取主要考虑了 ECC 的标准, 这些标准由公认的标准机构所

制定,如椭圆曲线数字签名算法(ECDSA)的标准 FIPS 186-2 就是由美国国家标准与技术研究所(NIST)制定的。第 5 章详细介绍了椭圆曲线密码的软件和硬件的有效实现技术,并且还介绍了“旁门攻击”技术及其预防对策。虽然第 5 章的内容是有限的,但是我们希望它能给软件开发人员和硬件设计人员提供一些有益的工程借鉴。

致谢 非常感谢曾给过我们有益的建议和帮助的人们。他们是 Mike Brown, Eric Fung, John Goyo, Rick Hite, Rob Lambert, Laurie Law, James Muir, Arash Reyhani-Masoleh, Paul Schellenberg, Adrian Tang, Edlyn Teske 和 Christof Zalka。特别感谢 Helen D'Souza, 他为本书设计了精美的艺术插图。还要感谢 Cindy Hankerson 和 Sherry Shannon-Vanstone, 是他们建议在书的插图中采用自然曲线的图案。最后我们感谢 Springer 出版社的编辑 Wayne Wheeler 和 Wayne Yuhasz, 感谢他们所给予的不断鼓励和支持。

读者可以通过我们的网站获得本书的更新和勘误信息,以及我们的联系信息。我们的网址是 <http://www.cacr.math.uwaterloo.ca/ecc/>。我们非常感激读者能够发现并告诉我们书中的错误和缺陷。

Darrel R. Hankerson, Alfred J. Menezes, Scott A. Vanstone
Auburn & Waterloo
2003.6

目 录

第 1 章 概论	1
1.1 密码学基础	1
1.2 公钥密码	5
1.3 为什么需要椭圆曲线密码	13
1.4 导读	18
1.5 注释和进一步参考	19
第 2 章 有限域算术	22
2.1 有限域介绍	22
2.2 素域算术	26
2.3 二进制域算术	44
2.4 最佳扩域算术	58
2.5 注释和进一步参考	66
第 3 章 椭圆曲线算术	70
3.1 椭圆曲线的概念	71
3.2 点的表示与群的运算法则	81
3.3 点乘	90
3.4 Koblitz 曲线	108
3.5 具有有效可计算自同态的曲线	118
3.6 用折半进行点乘	124
3.7 点乘的开销	136
3.8 注释和进一步参考	142
第 4 章 密码协议	147
4.1 椭圆曲线离散对数问题	147

4.2	参数组	164
4.3	密钥对	172
4.4	签名方案	175
4.5	公钥加密方案	180
4.6	密钥建立	184
4.7	注释和进一步参考	188
第 5 章	实现问题	196
5.1	软件实现	196
5.2	硬件实现	213
5.3	实现的安全	225
5.4	注释和进一步参考	235
附录 A	参数举例	242
附录 B	ECC 标准	251
附录 C	软件工具	254
参考文献		258
索引		286

第 1 章 概 论

椭圆曲线具有丰富多彩的历史，数学家对它的研究已经有一百多年。人们利用椭圆曲线来解决各种不同的问题。一个例子是用来解决同余数问题，这个问题要求把表示某些直角三角形面积的正整数进行分类，而这些直角三角形的边长是有理数。另一个例子是用来证明 Fermat 大定理。Fermat 大定理叙述的是，当 n 是大于 2 的整数时，方程 $x^n + y^n = z^n$ 对于 x, y, z 无非零整数解。

1985 年，Neal Koblitz 和 Victor Miller 分别独立地提出了利用椭圆曲线设计公钥密码体制的问题。从此以后关于椭圆曲线密码安全性和有效实现的大批研究成果被发表出来。1990 年以后，椭圆曲线密码开始得到商业界的认可，公认的标准化组织制定了椭圆曲线密码协议，一些公司在他们的安全产品中也采用了这些协议。

本章的目的是要讲述公钥密码体制相对于对称密码体制的优点，特别是要详细讲述各种椭圆曲线密码。但是，这里的讲述只是介绍性的。关于椭圆曲线密码的安全性及其有效实现将在后面几章讲述。

1.1 节将讲述密码学的基本目的以及对称密码与公钥密码的本质差别。1.2 节将讲述 RSA 密码、离散对数以及椭圆曲线密码族。1.3 节将对这些密码体制进行比较，以说明椭圆曲线密码的优点。1.4 节是本书的导读。最后，1.5 节给出进一步的密码学参考文献。

1.1 密码学基础

密码学是设计和分析确保在不安全信道上的通信安全的数学技术。

1.1.1 基本的通信模型

在图 1.1 中，实体 A (Alice) 和 B (Bob) 在不安全的信道上进行通信。我们假设在通信中存在一个敌手 E (Eve)，他要攻击 A 和 B 之间的各种安全服务。例如， A 和 B 利用移动通信电话网络进行通信，而 E 企图偷听他们的会话。或者，设 A 是个体 $\tilde{A}$ 的一个网站浏览器， B 是在线商店 $\tilde{B}$ 的网站，个体 $\tilde{A}$ 想通过网络在网站 B 购买 $\tilde{B}$ 的产品。在这种情况下信道就是

互联网。敌手 E 企图阅读 A 和 B 的交易信息, 以便得到 $\tilde{A}$ 的信用卡信息, 或假冒 A 或 B 与对方进行交易。第三个例子是考虑这样一种情况, A 通过互联网发送一封电子邮件给 B 。敌手 E 企图阅读这一消息, 或篡改其中的某一部分, 或冒充 A 给 B 发送自己的消息。最后, 考虑这样一种情况, 设 A 是一个智能卡, 它正在认证位于银行总部的主机 B 的读卡器 $\tilde{A}$ 。而敌手 E 监视通信, 企图获得 $\tilde{A}$ 的账号信息, 或者冒充 $\tilde{A}$, 以便从 $\tilde{A}$ 的账号取走资金。显然, 从这些例子可以看出通信的实体不一定是人, 可以是计算机、智能卡, 或涉及个人、组织 (如商店、银行等) 利益的软件模块。

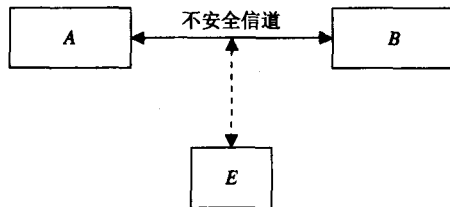


图 1.1 基本的通信模型

1.1.2 安全目标

认真考虑上述实例所揭示的保密通信的下列基本目标:

1. 秘密性: 对除授权者外的任何人保持数据的秘密。即除授权者可读外, 敌手 E 不可读 A 和 B 的通信消息。
2. 完整性: 确保数据不被未授权者所篡改。即 B 能检测 A 发来的数据是否被 E 篡改。
3. 数据源认证: 确认数据的来源。 B 应能验证声称是 A 发来的数据确实是 A 发的。
4. 实体认证: 确认实体的身份。即 B 应能认证通信对方的身份。
5. 不可否认性: 阻止一个实体否认以前的通信或行为。即当 B 收到一个 A 发来的消息时, B 不仅能确认该消息确实为 A 所发, 而且能够使公正的第三方也相信这一点。因此, A 就不能抵赖自己发给 B 的消息。

某些应用可能还有其他的安全要求, 如通信实体的匿名性、访问控制 (控制实体对资源的访问) 等。

1.1.3 敌手模型

为了能够用模型描述 A 和 B 所面临的威胁, 通常假设敌手 E 具有相当大的能力。除了能够获得信道传输的所有数据外, 他还能够篡改所传输的数据并注入自己的数据。 E 能够

支配相当大的计算资源。最后,除了秘密密钥以外, E 知道密码算法和通信协议的全部细节。密码工作者的挑战是面对如此强大的敌手,如何设计好的密码体制以确保通信的安全。

1.1.4 对称密码

密码体制一般可以划分为两种类型。图 1.2(a)描述了对称密码体制。对于对称密码体制,通信的双方必须就密钥的秘密性和真实性达成一致。然后,他们便可以利用对称密码,诸如数据加密标准(DES)、RC4、高级数据加密标准(AES),来确保通信数据的秘密性。他们还可以使用消息认证码(MAC),诸如 HMAC,确保通信数据和数据源的真实性。

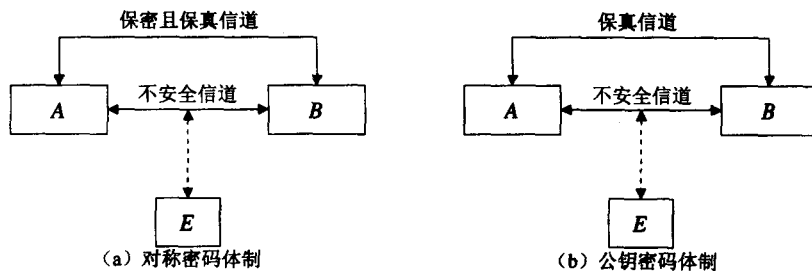


图 1.2 对称与公钥密码体制

例如,若要确保数据的秘密性,假设 A 和 B 共享密钥 k ,则 A 可以用加密函数 ENC 和密钥 k 将消息 m 加密成密文 $c = ENC_k(m)$,并发给 B 。 B 接收到 c 后用解密函数 DEC 和相同的密钥 k 解密密文 c ,还原出消息 $m = DEC_k(c)$ 。若要确保数据的完整性和数据源的真实性,则 A 和 B 首先就要协商共享一个密钥 k 。然后 A 利用密钥 k 和 MAC 算法对明文消息计算认证标记 $t = MAC_k(m)$ 。 B 收到 m 和 t 后,利用 MAC 算法和同一密钥 k ,对接收到的 m 重新计算认证标记 $t' = MAC_k(m)$,若 $t = t'$,则认为这一消息确实是 A 所发。

密钥分发与管理 对称密码体制的最大优点是效率高,但它却存在严重的缺点。一个主要的缺点是密钥分发问题,即要求分发密钥的信道既是保密的又是保真的。在某些应用情况下,通过一个物理安全的信道,如利用可靠的信使作为安全的信道,很容易实现密钥分发。另一种方法是利用一个在线的可信第三方。开始时它为所有网络实体建立一个保密的密钥,然后利用这些保密的密钥进行通信密钥的分发^①。这种方案特别适合具有中央权威机构的应用环境,然而这显然不适用于互联网环境下的电子邮件应用。

第二个缺点是密钥管理问题,即在有 N 个实体的网络中,每个实体都必须保存其他

^① 这种方法采用一个权威的第三方分发对称密码的密钥,它已用于针对客户机/服务器系统的 Kerberos 网络认证协议中。

$N-1$ 个实体的密钥。利用一个在线的可信第三方, 这一问题可以得到缓解。在需要密钥时由这一在线的可信第三方分发密钥, 因此可以减小实体存储大量密钥的压力。然而, 这种解决方案对有些应用情况却不适用。最后指出, 因为由两个(或更多个)实体共享密钥, 所以对称密码体制不能实现用于不可否认服务的数字签名, 这是因为无法区分共享密钥的不同实体的行为^①。

1.1.5 公钥密码

图 1.2(b)所示的公钥密码是 Diffie, Hellman 和 Merkle 针对对称密码体制的上述缺点, 于 1975 年提出的。与对称密码不同, 公钥密码仅要求密钥的交换是保真的, 而不要求其是保密的。每个实体选择一个密钥对 (e, d) , 其中 e 是公钥, 而 d 是私钥, 私钥需要保密。这种密钥具有如下特性, 且仅由公钥不能计算出私钥。

秘密性 如果实体 A 希望发送一个秘密消息 m 给 B , 他首先获得 B 的公钥 e_B , 并利用公钥密码体制的加密函数 ENC , 计算出密文 $c = ENC_{e_B}(m)$ 。然后 A 将 c 发给 B 。 B 利用自己的私钥和公钥密码体制的解密函数 DEC , 解密恢复出明文 $m = DEC_{d_B}(c)$ 。这里假设敌手只知公钥 e_B 而不知私钥 d_B , 因此不能解密密文 c 。可以看出, 其中不需要对 e_B 保密。重要的是 A 必须获得真实的 e_B ; 否则, 若 A 得到的是冒充 B 的另一实体 E 的公钥 e_E , 则 E 就可以恢复消息 m 。

不可否认性 数字签名可用于数据源和数据完整性认证, 提供不可否认服务。实体 A 应用数字签名产生算法 $SIGN$ 和自己的私钥 d_A , 计算产生消息的签名: $s = SIGN_{d_A}(m)$ 。实体 B 接收到 s 和 m 后, 利用 A 的真实公钥 e_A 和数字签名验证算法来验证 s 是否是从 m 和 d_A 产生的签名。因为假定只有 A 知道 d_A , 所以 B 可以断定消息 m 确实是 A 所发。此外, 因为签名验证只需要公开的 m 和 e_A , 因此 m 的签名 s 也可由第三方验证。若 A 企图抵赖自己对消息 m 的签名, 则第三方可以仲裁。与手写签名不一样, A 的签名 s 与所签的消息 m 相关, 因此可以阻止简单地将 s 附加到其他消息 m' 之后冒充 A 对 m' 签名的伪造行为。虽然公钥 e_A 不需要保密, 但是验证 A 的签名时需要使用 A 的真实公钥 e_A 。

这样, 公钥密码圆满地解决了对称密码面临的三个难题: 密钥分发、密钥管理和提供不可否认性。应当指出, 虽然公钥密码不需要使用保密信道分发公钥, 但是用于分发和管理公钥的公钥基础设施(PKI)的实施在实践上可能会遇到极大的挑战。另外, 公钥密码的运

^① 也可以使用对称密码设计数字签名方案, 但是这种方案不实用, 因为这种方案需要使用在线的可信第三方, 而且还必须在每次签名时都要换用新的密钥。

算通常比对称密码慢得多。因此,通常采用对称密码和公钥密码的混合系统,将对称密码的高效性和公钥密码的功能方便性结合起来。

下一节将介绍三种著名的公钥密码体制。

1.2 公钥密码

在公钥密码体制中,密钥对的选择要保证从公钥求出私钥等价于要求解一个困难的计算问题。构成常用公钥密码基础的困难问题有如下的数论问题:

1. 整数的因子分解问题,其困难性是 RSA 公钥密码安全性的基础。
2. 离散对数问题,其困难性是 ElGamal 公钥密码及其变体(如数字签名算法)安全性的基础。
3. 椭圆曲线离散对数问题,其困难性是椭圆曲线公钥密码安全性的基础。

本节介绍 RSA 公钥密码、ElGamal 公钥密码和椭圆曲线公钥密码的基本方案。我们强调指出,本节的介绍是教科书式的,而对于实际应用,要能抵抗各种实际攻击,还需要对这些方案进行加强,例如在加密之前用随机数进行明文填充。然而,这些基本方案描述了 RSA、离散对数和椭圆曲线公钥密码的基本思想。第4章将介绍椭圆曲线密码的更深入内容。

1.2.1 RSA 体制

RSA 密码以发明者 Rivest, Shamir 和 Adleman 的名字的首字母命名,他们在公钥密码的概念提出之后不久,于 1977 年提出了这种公钥密码。

RSA 密钥生成

RSA 密钥对用算法 1.1 生成。其公钥由一对整数 (n, e) 组成,其中 n 是 RSA 的运算模,它是两个同样长度的保密随机素数 p 和 q 的乘积。加密指数 e 是满足 $1 < e < \phi$ 且 $\gcd(e, \phi) = 1$ 的整数,其中 $\phi = (p-1)(q-1)$ 。私钥 d 也称为解密指数。它是满足 $1 < d < \phi$ 且 $ed \equiv 1 \pmod{\phi}$ 的整数。已经证明,从公钥对 (n, e) 计算出私钥 d 等价于从 n 分解出因子 p 和 q 。这一问题被称为整数的因子分解问题(IFP)。

算法 1.1 RSA 密钥对生成

输入: 安全参数 l 。

输出: RSA 公钥 (n, e) 和私钥 d 。

1. 随机选择两个素数 p 和 q , p 和 q 的长度同为 $l/2$ 。
2. 计算 $n = pq$ 和 $\phi = (p-1)(q-1)$ 。
3. 任意选择整数 e , e 满足 $1 < e < \phi$ 且 $\gcd(e, \phi) = 1$ 。
4. 计算整数 d , d 满足 $1 < d < \phi$ 且 $ed \equiv 1 \pmod{\phi}$ 。
5. 返回 (n, e, d) 。

RSA 加密方案

RSA 加密和签名方案基于以下理论依据, 即对于所有的整数 m , 都有

$$m^{ed} \equiv m \pmod{n}. \quad (1.1)$$

RSA 公钥密码的基本加密和解密过程分别如算法 1.2 和算法 1.3 所示。解密的原理是根据式(1.1)导出的 $c^d \equiv (m^e)^d \equiv m \pmod{n}$ 。安全性建立在从密文 $c = m^e \bmod n$ 和公钥 (e, n) 计算明文 m 的困难性之上。这个问题就是求 c 的 $\bmod n$ 的 e 次根, 被认为与整数分解一样困难(尚未证明)。

算法 1.2 基本 RSA 加密

输入: RSA 公钥 (n, e) , 明文 $m \in [0, n-1]$ 。

输出: 密文 c 。

1. 计算 $c = m^e \bmod n$ 。
2. 返回 (c) 。

算法 1.3 基本 RSA 解密

输入: RSA 公钥 (n, e) , RSA 私钥 d , 密文 c 。

输出: 明文 m 。

1. 计算 $m = c^d \bmod n$ 。
2. 返回 (m) 。

RSA 签名方案

RSA 公钥密码的签名和签名验证过程分别如算法 1.4 和算法 1.5 所示。签名者首先利用密码学杂凑函数 H , 计算消息 m 的摘要 $h = H(m)$, 摘要值 h 称为消息 m 的短指纹。然后, 签名者用自己的私钥 d 计算 $h \bmod n$ 的 e 次根 s , 即 $s = h^d \bmod n$ 。注意, 根据式(1.1)有 $s^e \equiv h \pmod{n}$ 。最后, 签名者把消息 m 和自己的签名 s 一起发给验证方。验证方根据收