中国计算机学会计算机安全专业委员会推荐参考书

信息与网络安全丛书

公开密钥基础设施

——概念、标准和实施

Carlisle Adams Steve Lloyd 著

冯登国 等 译

93.08

人民邮电出版社

www.pptph.com.cn

中国计算机学会计算机安全专业委员会推荐参考书

信息与网络安全丛书

公开密钥基础设施

—— 概念、标准和实施

Carlisle Adams　Steve Lloyd　著

冯登国　等　译

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

公开密钥基础设施：概念、标准和实施/（美）亚当斯（Adams,C.）著，（美）劳埃德（Lloyd,S.）著；冯登国等译.－北京：人民邮电出版社，2001.1
(信息与网络安全丛书)
ISBN 7-115-09024-6

I. 公… II.. ①亚… ②劳… ③冯… III. 计算机网络－安全技术 IV. TP393.08
中国版本图书馆 CIP 数据核字（2000）第 73225 号

中国计算机学会计算机安全专业委员会推荐参考书
信息与网络安全丛书
公开密钥基础设施
——概念、标准和实施

◆ 著　　Carlisle Adams　Steve Lloyd
译　　冯登国　等
责任编辑　李　际

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ pptph.com.cn
网址　http://www.pptph.com.cn
北京汉魂图文设计有限公司制作
北京朝阳展望印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：14.5
字数：333 千字　　2001 年 1 月第 1 版
印数：1－6 000 册　　2001 年 1 月北京第 1 次印刷

著作权合同登记　图字：01－2000－2861 号
ISBN 7-115-09024-6/TP·1998

定价：27.00 元

丛书前言

随着科学技术的飞速发展，人们已经生活在信息时代。计算机技术和网络技术深入到社会的各个领域，因特网把“地球村”的居民紧密地连在了一起。如果说“天涯若比邻”在过去只是描写人们心灵上的贴近，那么今天计算机网络已使这句话变成了生活现实。近年来因特网的迅速发展，给人们的日常生活带来了全新的感受，人类社会各种活动对信息网络的依赖程度已经越来越大。

然而，凡事“有一利必有一弊”。人们在得益于信息革命所带来的新的巨大机遇的同时，也不得不面对信息安全问题的严峻考验。1999 年好莱坞推出的以网络为主题的影片《黑客帝国》风靡全球，给人们提示了这个问题的严重性。在人们对网络技术的普及叫好声尚未消失的时候，黑客攻击战在现实生活中也愈演愈烈。国内外众多的网站相继被“黑”，病毒制造者们各显其能。从 CIH 噩梦难醒，到“爱虫”病毒狂吻全球，全球“中毒”者不计其数。这些给各行各业带来了巨大的经济和其他方面损失。除此之外，“电子战”、“信息战”已成为国与国之间、商家与商家之间的一种重要的攻击与防卫手段。因此，信息安全、网络安全的问题已经引起各国、各部门、各行、各业以及每个计算机用户的充分重视。

为了提高我国各级计算机信息网络主管部门的安全意识，普及计算机安全知识，进一步提高国内计算机安全的技术水平，帮助国内技术人员汲取国外计算机安全先进技术和经验，有效保护我国信息网络安全，在公安部公共信息网络安全监察局的大力支持下，我们策划且及时推出了这套《信息与网络安全丛书》。这套丛书采用开放式选题架构，全部是从国外著名出版公司出版的有关信息与网络安全类的权威著作和畅销书中精选而成。这套丛书内容涉及计算机硬件安全、操作系统安全、工作站和服务器的系统安全、网络安全设计、网络入侵检测、网络安全理论等各方面的内容。

由于本套丛书的原版书均是由国外权威人士编写而成，因此在观念上和技术上站在了该领域的前沿。也正因为此，本套丛书受到了有关部门领导和专家的高度重视。由公安部领导和公共信息网络安全监察局及部分计算机安全专家组成的审定委员会对图书进行了审阅，从而保证了丛书的权威性和准确性。当然，由于原版图书所涉及的网络及社会环境等与我国情况不尽相同，读者定会本着批评借鉴的态度结合工作实际进行阅读、参考和分析。

我们真诚希望本套丛书能够为信息与网络安全管理和技术人员提供帮助，为我国的信息安全建设做出贡献。

编者

2000 年 7 月

前言

毋庸置疑，公开密钥基础设施(PKI)技术的前景在过去的几年里引起了极大的重视。几乎每天的报纸、贸易杂志或大会文章中都报道有关 PKI 的内容，我们听到和看到通过使用数字签名技术进行认证和非否认服务，以及基于混合使用对称和非对称密码技术实施机密性和密钥管理服务的前景，而这些技术都是建立在了解与 PKI 相关的技术的基础之上的。事实上，许多人认为对 PKI 技术的介绍能促进全球的电子商务。

在 20 年前，随着公钥技术的产生，PKI 基础设施已经建立,但是也只在最近几年 PKI 技术才作为商用方面可行的解决方案。但是几年前开始出现的技术支持厂商已经从少数几家发展到了数百家，它们已经提供了多种与 PKI 有关的服务。此外，以 PKI 为基础的服务的商业需求正日益增加,越来越多的事实表明，PKI 的后动力也将更好地有助于未来的可持续发展。

当然,作为技术,PKI 是相当新的。对于许多人来说,PKI 技术在某种程度上被披上了一层神秘的色彩。这种情形似乎是由于令人混淆的文档、标准以及销售方式的剧增而加剧。而且还没有一本对 PKI 的关键概念和技术基础进行综合介绍的书。

因此，作者有写本书的共同愿望:提供与销售无关的信息来建立理解 PKI 的基础，在本书里我们解决许多与 PKI 相关的基础问题,包括:

- 究竟什么是 PKI?
- 数字签名由什么组成?
- 什么是证书?
- 什么是证书撤消?
- 什么是证书机构(CA)?
- 什么是管理标准?
- 在企业中实施大型 PKI 的相关问题是什么?

这些只是这本书所探讨的一部分问题。

PKI 的动力

PKI 不是一种没有实际效益的简单的纯技术，认识到这一点很重要。当正确地开发 PKI 时，PKI 能为组织提供一定的基本利益，包括节省大量费用的潜力。PKI 可以作为支持认证、完整性、机密性和不可否认性的技术基础。将对称和非对称密码技术结合来实现 PKI，这种结合采用了单一的易于管理的机构而不是多种安全方案（参见第 2 章 ~ 第 5 章）。PKI 采取了层次密钥管理，与单一采用对称密码体制相比，大大降低了将密钥信息分发给通信各方的费用（参见第 2 章有关对称和非对称密码技术的描述）。合理的实施一个统一的 PKI 技术有利于：

- 降低了管理的费用（与多点解决方案的实施相比）。
- 减少了端用户签名事件的数量。
- 通过更加自动（更安全）的流程减少了纸上工作，提高了工作效率。
- 优化工作生产率（通过让用户确信使用安全基础设施只需要花最少的时间，从而将更多的时间用于手头的工作）。
- 减少了端用户在使用安全服务前所需要的培训要求（因为只有一种安全方案而不是多种）。

PKI 技术不但能节省费用，而且在许多情况下还能成为一个组织创造收入的来源（通过支持也许还没有的新服务）。第三部分将进一步讨论与 PKI 技术相关的收益和考虑。

注释

需要强调的是我们将尽力确保这本书与销售无关。实际上该书的原稿按审阅人的要求已做了部分修改。作为作者，本书中我们描述了我们关于一个综合 PKI 的组成的观点。尽管该观点偶尔与某些环境和产品有关，但我们要说明我们并不知道哪些销售商提供了书中所描述的服务。

我们也意识到有一些环境必定更接近这里所描述的组成和服务(由于他们具有具体的要求和特定的用户群)的一部分。我们充分意识到这些环境可能永远不会完全与我们所指的 PKI 一致。本来就该是这样。本书尽可能描述 PKI 的方方面面，因而不是讲 "Internet PKI"，也不限于企业的 PKI —— 尽管企业的环境比起其他的实施环境更接近我们的关于综合 PKI 的概念。本书试图描述 PKI 的各个方面；特定的环境将作为需要的部分被实现。为澄清这些概念，第 5 章讨论了现在 PKI 的一些变种。

读者对象

本书的主要目的是提供一个较全面的概述来帮助读者更好地理解 PKI 技术后面的技术和操作的考虑。如果你计划/实施和操作一个企业公开密钥基础设施，本书会使你获益匪浅。

一些对 PKI 的基本概念有兴趣的人也会发现本书很有用。

我们希望本书成为大众的教育工具和一些人的参考指南。尽管对于最终更想知道详细的实现细节的人来说，本书是一个初级读物，但是本书并不旨在解决详细的实现问题。

组织结构

本书分为三部分。第一部分提供了基础知识，这些内容有利于更好地理解 PKI 的概念和原理。第二部分讲述与 PKI 相关的标准和活动(例如，业界倡议的互操作的初始化)。这一部分有两个基本目的。第一，提供了 PKI 包括的主要标准的概述，并讨论了每组的侧重点，给这些活动的一部分提供了路标。第二，展示该领域的相对稳定性和成熟性，突出了已有的实现和互操作所需的坚实基础。第三部分讨论实施 PKI 所要考虑的因素，为实施 PKI 前要做一些初始的决定提供了指导。

第一部分：概念

第一部分是关于基本的 PKI 概念。包括基础知识(例如，密码入门)以及有关公钥证书和证书撤消方案的细节。

第 1 章介绍第一部分，提供第一部分以章为基础的内容列表。

第 2 章对本书中所涉及到的公钥密码概念做一个简要的非数学的介绍。这些概念包括对称和公钥算法的区别、密钥对的概念、该技术的服务、术语和算法实例。

第 3 章讨论一个基础设施，着重说明它在一个应用中的用途、在一次安全登录中的作用、为端用户提供透明性及全面的安全性的能力。该章对 PKI 也给出一个可行定义。

第 4 章讨论核心 PKI 服务，如认证、完整性和机密性等。

第 5 章讨论 PKI 可提供的服务。主要讨论 PKI 可提供的一些服务，例如数字时间戳、公证、不可否认和特权管理。

第 6 章介绍证书的概念，并讨论认证的过程。描述证书的内容和格式，以及证书机构（CA）和注册机构（RA）的作用。

第 7 章讲述密钥/证书在整个生命期的管理，包括产生、公布、更新、结束、密钥的变化、密钥的备份、密钥的恢复。

第 8 章讨论证书撤消的一般技术，包括定期公布和在线查询。还讨论了与该技术有关的其他方面：范围、时间和实现。

第 9 章介绍信任模型的概念。提出并比较了严格的层次结构、分布式体系结构、Web 模型、以用户为中心的信任，以及交叉认证。

第 10 章介绍密钥对的使用、不可否认的支持、独立证书的管理。

第 11 章考察证书的分发和资料库。本章讨论证书公布、规模、复制、时间、信任和不

信任的存储/访问。

第 12 章讨论客户端软件、在线请求、物理安全、灾难的考虑和恢复，以及系统安全与使用的平衡。

第 13 章简要讨论与 PKI 有关的法律问题，包括数字签名的合法状态、角色、职责、可靠性、缓解危险等主题。

第 14 章总结第一部分，并建议需进一步阅读的材料。

第二部分：标准

第二部分讲述标准活动和互操作初始化。

第 15 章介绍第二部分以及各章内容的列表。

第 16 章讨论正式的标准组织中一些最重要的活动，以及组织以外所做的其他相关的努力。

第 17 章提供一些最著名规范的当前和计划中近期的标准化情况。

第 18 章探讨有些标准，无论是正式或非正式的标准组织的产品，这些标准有必要但还不能充分地保证不同厂商的产品能互操作，在本章将给出部分原因。另外，本章还讨论了描述和互操作性测试的效用。

第 19 章提供了结论性的评论和进一步阅读的建议。

第三部分：实施 PKI 应考虑的若干因素

本书的第三部分讨论实施。尽管不是一个实施手册，这部分的基本目的是阐明当考虑一些大规模企业的 PKI 实施时，如何提出并解决问题。

第 20 章介绍第三部分，并提供各章的内容列表。

第 21 章讨论实施 PKI 带来的益处、费用的问题。本章有助于说明在企业环境中实施 PKI 的合理的商业原因。

第 22 章讨论在实施开始前要解决的问题，本章提供了产品选择的基础。

第 23 章讲述实施时的一些障碍和从长远策略出发需要考虑的问题。

第 24 章考察一些可实现的常见商务模型，并对一些全球可信模型做了简单的讨论。

第 25 章对第三部分进行总结并为进一步阅读提出建议。

1. 概述
2. 公钥密码学
3. 基础设施的概念
4. 核心 PKI 服务：认证、完整性和机密性
5. PKI 支撑的服务
6. 证书和认证
7. 密钥和证书管理
8. 证书撤消
9. 信任模型
10. 单实体多证书
11. PKI 信息的分发：资料库和其他技术
12. PKI 的运作考虑
13. 法律框架
14. 结论与进一步阅读的材料

第一部分

概念

概述 第1章

本书是关于理解公开密钥基础设施（Public Key Infrastructure，简称 PKI）的。理解的第一步要使用头脑：理解概念、熟悉术语并且对于与主题有限定作用的因素、主题的范畴及界限要有一定的认识。这使我们能够对关于这个问题的其他内容逐渐变得比较熟悉，能够以敏锐的、批判的眼光来阅读和理解相关的文献。

理解的第二步要使用手：我们要通过实践来学习。为了使这些概念的具体实现成为可能，我们要了解其他人已经做（和正在做）的技术工作，然后我们开始在自己的环境下自行实现这些概念。这样做也使得我们可以和其他人交流以及公正地评价文献。

“实践”能够导致更深刻的“了解”，“了解”反过来又可以产生更成功的“实践”，如此进行下去，最终的结果是对所研究的主题有相当深刻的理解。

本书的主要目的是想成为理解 PKI 过程的一本工具书。假如一定程度的“了解”是必须的，那么第一部分阐述的就是这方面的内容，它讨论了基本的概念和术语，解释了任何地方都会出现的技术选项，提出了这项技术所固有的优点及局限。

第二部分集中在“实践”，它描述了由标准化组织所着手做的相关工作和使 PKI 的实现和互操作成为可能的最初努力。第三部分也集中在“实践”，它讨论了具体实现的许多问题和在现实世界里实施 PKI 所要做的决策。

第一部分占据了本书的大半部分。第二部分和第三部分是使读者开始他或她自己的 PKI 实施的基本指导方针。

第一部分中介绍的主要内容如下：

- 第 2 章对贯穿本书其余部分的公钥密码学概念做了简要的非数学方式的介绍，包括对称密码和公钥密码的区别，密钥对的概念，这项技术所提供的服务，术语和示例算法等。
- 第 3 章讨论了关于基础设施的概念，突出了它作为应用支撑的用处，它在安全的单点登录中的作用和它对终端用户提供透明性和综合安全的能力。这一章还给出了一个有指导意义的 PKI 的定义。
- 第 4 章和第 5 章探讨了 PKI 能提供的服务。第 4 章讨论了核心服务：认证、完整性和机密性；第 5 章着眼于 PKI 能提供的服务，如数字时间戳，公证，不可否认性和特权管理。
- 第 6 章介绍了证书的概念并讨论了认证的过程。这一章描述了证书的内容和格式以及认证机构（Certification Authority，简称 CA）和注册机构（Registration Authority，简称 RA）的职责。

- 第 7 章着眼于密钥和证书生命周期管理的整个领域，涉及产生，发布，更新，终止，密钥历史，密钥备份和密钥恢复。
- 第 8 章讨论了证书撤消的常见技术——定期发布机制和在线查询机制。这一章讨论了这些技术的可扩展性、及时性和实现中要考虑的事项。
- 第 9 章探讨了信任模型的概念，提出并比较了严格层次结构、分布式结构、Web 模型、以用户为中心的信任等四种模型并讨论了交叉认证。
- 第 10 章讨论了单实体多证书的概念，还包括密钥对使用的检查，对不可否认性的支持和独立的证书管理。
- 第 11 章着眼于证书的分发和资料库。它讨论了证书发布的得失以及可扩展性、复制、及时性以及可信和不可信存储/访问等问题。
- 第 12 章探讨了 PKI 运作要考虑的事项并且讨论了客户端软件，在线请求，物理安全和灾难计划/恢复，以及在系统安全和易用性间的权衡。
- 第 13 章简短讨论了关于 PKI 的法律框架，并包括了如数字签名的法律状况、认证惯例陈述（Certification Practice Statement，简称 CPS）、责任和降低风险等话题。
- 第 14 章总结了第一部分并给出了在这个领域进一步学习可用的一些资源。

下面我们从公钥密码学的一个简短介绍开始本书的学习。

公钥密码学 第2章

本章主要介绍公钥密码学的基本概念。叙述力求精练简短，只涉及理解与本书剩余部分直接相关的东西。如果要了解更深和更广的知识，请参阅《Handbook of Applied Cryptography》（A.Menezes，P.van Oorschot 和 S.Vanstone [MvOV97]），《Applied Cryptography: Protocols，Algorithms，and Source Code in C》（B.Schneier [Sch96]），《Cryptography and Network Security：Principles and Practice》(W.Stallings [Sta99])或《Cryptography：Theory and Practice》(D.Stinson [Sti95])。

2.1 对称和非对称密码

自从人类有了通信以来，人类就希望能够有一些秘密（或隐藏）的联系。几千年来，人们已经设计了无数的隐藏数据的方法来使用，其中一种方法就是把有用的信息转换成一些看起来毫无意义的文字，而授权接收者可以通过某种方法把这些文字转换成原来的信息，以获取发送者的消息，而非授权者从这些文字中获取不到任何有用的信息。

用来把信息转换成无用的文字又能转换回来的机制有两大类。下面这一节将定义和论述对称（私钥）密码；至于非对称（公钥）密码将在"新方向：公钥密码"这一节来描述。

2.1.1 私钥密码

直到 20 世纪 70 年代中期，在那些公开文献中所提到的用来把有用的信息转换成无意义的文字并转换回来的唯一机制只是着重于加密和解密过程是怎样实现的。

作为这方面一个众所周知的简单例子，一种将有用信息转换成无意义的文字的方法是指定在原始信息中的每一个字母由字母表中的前第 13 位字母代替，如 A 代替 N，B 代替 O，Z 代替 M，等等。在这个例子中，转换回来的过程也是完全相同的：N 的前第 13 位字母是 A，O 的前第 13 位是 B，M 的前第 13 位是 Z，等等。

用密码领域中的普通术语来讲，确保这两次转换过程能顺利进行的共享秘密信息（上一个例子中的 13）称为密钥。将有用信息转换成无意义的文字的过程称为加密，而将无意义的文字转换回原来信息的过程称为解密。原来的信息称为明文，转换后的无意义文字称为密文，密文可以被授权者解密成相应的明文。整个机密性机制（也就是加密和解密算法）称

为密码。更进一步来说，如果一个安全机制符合下面两条中的一条，就称为对称（私钥）密码：

① 加密密钥和解密密钥完全相同（在前面一例中都是 13）。

② 一个密钥很容易从另一个密钥中导出（把前面一例稍作改动，加密过程是前移 5 位，这样，解密过程就是后移 5 位）。

在一些简单和复杂的实例中都有应用的对称密码已经存在了好几千年，而且新的对称密码也不断地被发明。比较早的例子是众所周知的 ROT-13（更普遍的说法是简单替代密码），更现代的例子包括 DES[FIPS46]，IDEA[Lai92]，RC5[Rivest95],CAST-128[Adams97，RFC2144]，以及美国 NIST（国家标准技术研究所）发起的 AES 候选方案（如“Advanced Encryption Standard Development Effort”[AES]）。

注释

AES 方案是 NIST 发起的，以挑选一个对称密码来正式代替 DES，起初是准备给美国政府来使用的，但很有可能会有更广泛的应用前景。AES 将在 2000 年夏季从 15 个候选方案中选出，预期将为今后二三十年提供更高性能的密码安全。经过长时间的观察，NIST 要求 AES 的密钥长度要达到 256 比特（而现在密码的密钥长度只能达到 128 比特）。

尽管对称密码有一些很好的特性（如运行占用空间小，加/解密速度能达到数十兆/秒或更多），但它们在某些情况下也有明显的缺陷，包括：

① 需要进行密钥交换。

② 规模复杂。

③ 同以前未知的实体初次通信困难。

下面的几个部分主要讨论这几个缺陷。

一、需要进行私钥交换

为了安全，对称密码完全依赖于以下这样一个事实：在传送信息以前，信息的发送者和授权接收者必须共享一些秘密信息（密钥），因此，在进行通信以前，密钥必须先在一条安全的单独通道上进行传输，这附加的步骤，尽管在某些情况下是可行的，但在某些情况下会非常困难或极其不便。

二、规模复杂

举例来说，Alice 和 Bob 两人之间的密钥必须不同于 Alice 和 Catherine 两人之间的密钥，否则给 Bob 的消息的安全就会受到威胁。在有 1000 个用户的团体中，Alice 需要保持至少 999 个密钥（更确切的说是 1000 个，如果她需要留一个密钥给她自己加密数据），因为对其他的用户情况也是一样，这样这个团体一共需要有将近 50 万个不同的密钥！随着团体的不断增大，储存和管理这么大数量的密钥很快就会变得难以处理（n 个用户的团体需要 $n^2/2$ 个不同的密钥，包括那些用户留给自己的）。考虑到这些密钥还不是永久性的密钥，为了防止使用同一个密钥加密太多的数据，这些密钥将会在一段时间内更换，情况就变得更难以想象了。

三、未知实体间通信困难

当两个通信实体互不相识时（也就是两个实体以前没有任何接触），需要一个秘密的单独通道进行密钥交换这一步骤就会非常困难。Alice 知道有一个名叫 Bob 的律师，她需要和他进行一次秘密交谈，然而，如果她没有和 Bob 通信的历史，她怎么知道和谁共享密钥以使得秘密通信能顺利进行呢？也就是说，她怎么确认和她共享密钥的人是 Bob 而不是 David，如果 David 假装成 Bob 以获得 Alice 的秘密信息呢？

在两个以前没有任何接触的实体间需要一个“介绍人”这一基本问题，并不是对称密码技术所特有的，它也在非对称密码技术中出现。然而，你会发现，在这两种技术中，解决方案却是截然不同的（比较下两节：“对称中心服务结构”和“陌生人之间的安全”）。

四、对称中心服务结构

通过应用基于对称密码的中心服务结构，上面所提到的问题有所缓解。在这个体系中，团体中的任何一个实体与中心服务器（通常称作密钥分配中心，或 KDC）共享一个密钥。在这样的一个结构中，需要存储的密钥数量基本上和团体的人数数量差不多，而且中心服务器也可以给那些以前互不相识的实体充当“介绍人”。但是，这个与安全密切相关的中心服务器必须随时都是在线的（因为只要服务器一掉线，实体间的通信将不可能进行了）。这就意味着中心服务器是整个通信失败的关键和受攻击的焦点，也意味着它还是一个庞大组织服务通信的“瓶颈”。

2.1.2 新方向：公钥密码

20 世纪 70 年代中期，两个名叫 Whitfield Diffie 和 Martin Hellman 的研究者开辟了公钥密码这块新天地（最近的文献表明：早在 20 世纪 60 年代末，英国机构 GCHQ 中的一部分人就认识到了 Diffie 和 Hellman 所提出的概念；然而，这些消息并没有公开发表，当然 Diffie 和 Hellman 都不知道）。考虑到上面所讨论的一些对称密码中的问题，Diffie 和 Hellman 提出了非对称密码体制的假想：在这个体制中，加密密钥和解密密钥是有一定的关系的，但却是完全不同的，以至于可以公开其中的一个，而完全不用担心任何人会计算或推导出另一个。

这个观点全新而又有趣，但是否可行呢？Diffie 和 Hellman 没有给出一个明确的答复；他们的论文“New Directions in Cryptography”[DH76]中没有一个具体的例子能满足以上要求，它所讲述的只是这样的密码体制有可能建立的根据，并举了一个简单的例子：一个基于向量－矩阵乘法的密码体制，信息发送者和授权接收者只需用一个向量去乘一个矩阵来进行加密和解密，而其他的非授权者要想恢复明文，则需进行非常复杂的矩阵转置过程。他们建议：在非对称密码体制中，最好采用那些表面上很难，但如果有了一些附加信息就很简单的数学问题，“具有高计算复杂性的陷门函数（trapdoor functions with high computational complexity）”（参见 Merkle 这方面早期的独立作品[M78，M79]）就是这方面很好的例子。

Diffie 和 Hellman 论文中的观点在刚出现时，不可能去过分强调它是多么的先进。但一个密钥可以完全公开而不破坏通信安全，这在当时的公开文献中是前所未有的，而且多年来一直刺激着这方面的研究工作的发展。人们一直想找出非对称密码体制的具体例子，提出了不少方案（其中大部分后来被证明是不安全的）。这个问题变得越来越基础，也许越来越重

要，因此，许多数学家，计算机科学家和工程师一直致力于研究理论和实际复杂性，并试图了解一些数学难题的核心难点，如有限域上的因式分解和离散对数。自从 1976 年，经典的 Diffie-Hellman 论文发表以来，科学家在这方面取得了长足的进步，非对称密码体制以及相关领域研究的发展步伐也越来越快。

2.2 公钥和私钥对

从上一节知道，非对称密码采用两种相关的密钥，而这两个密钥又截然不同，知道其中一个，并不能推导或计算出另一个（即使敌手有很强的计算能力）。这就意味着一个密钥可以完全公开（如储存在一个公开的数据库中，列在电话本上，或打印在名片上），也不降低安全性 —— 只要另一个密钥保密。这种可以公开密钥的观念是如此的先进且吸引人，因而保密数据的方法立刻全发展成了众所周知的公钥密码学。

注释

在工业和学术文献中，一般用私钥来指代那个没有公开的密钥，而不是用密钥，以避免同对称密码中的密钥产生混淆，它来源于两个人共享一个秘密，而一个人保持某一秘密的观点。

一对密钥之间的关系

在公钥密码中，一对密钥中的两个密钥是不同的，但却是相关的（这完全有必要，因为一个人必须要解开别人加密的东西）。这种相关性必须是一种数学关系，可能依赖一些只有密钥对的创造者才知道的信息（如大整数的因式分解）。采用这种技术的安全性基于这样一个事实：除了密钥对的创造者，其他人想从公钥推导出私钥，在计算上是完全不可能的。理论上，私钥还是有可能被推导出来的，但实际上，推导所用的时间、存储量和计算能力是大得惊人的。

2.3 公钥密码的服务

公钥密码的发现也带来了一系列新的服务，这些服务在对称密码体制中有的是前所未闻，有的就根本不可能达到，这一节着重介绍几个很重要和/或很有趣的服务。

2.3.1 陌生人之间的安全

在对称密码环境下，陌生人之间进行安全通信十分困难，这就成了推动公钥密码体制发展的巨大动力之一。特别是在给出了密码的其他细节后，计算私钥仍然很困难的情况下，在这个体系中仍可获得公钥并把它传播得更广。例如，把这个公钥存放在一个公用数据库中（在某种意义上，公用数据库是一个电话本的等价物）。这样，即使 Alice 以前没有和 Bob 有过任何意义上的接触，她也能查阅到他的公钥（类似于在电话本上查找电话号码）并发送