Information Security

PUTONG GAODENG XUEXIAO XINXI ANQUAN "SHIYIWU" GUIHUA JIAOCAI
普通高等学校信息安全“十一五”规划教材

PKI 原理与技术

PKI YUANLI YU JISHU

佘堃 郑方伟 编著

电子科技大学出版社

PUTONG GAODENG XUEXIAO XINXI ANQUAN "SHIYIWU" GUIHUA JIAOCAI
普通高等学校信息安全“十一五”规划教材

PKI 原理与技术

佘 堃 郑方伟 编著

电子科技大学出版社

图书在版编目（CIP）数据

PKI 原理与技术/佘堃，郑方伟编著. —成都：电子科技大学出版社，2007.8

普通高等学校信息安全“十一五”规划教材

ISBN 978-7-81114-225-9

Ⅰ.P… Ⅱ.①佘… ②郑… Ⅲ.电子商务—安全技术—高等学校—教材 Ⅳ.F713.36

中国版本图书馆 CIP 数据核字（2007）第 124449 号

内 容 提 要

本书为普通高等学校信息安全“十一五”规划教材之一。全书共 10 章，主要讲述了 PKI（公钥基础设施）理论基础、标准、应用及前景等，从工程的角度介绍了 PKI 体制和各关键技术的实施。

本书既可作为信息安全或计算机专业本科生、专科生的教材，也可作为相关领域专业技术人员的参考用书。

普通高等学校信息安全“十一五”规划教材

PKI 原理与技术

佘 堃 郑方伟 编著

出 版： 电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦 **邮编：** 610051）
策划编辑： 曾 艺
责任编辑： 周元勋
主 页： www.uestcp.com.cn
电子邮箱： uestcp@uestcp.com.cn
发 行： 新华书店经销
印 刷： 成都蜀通印务有限责任公司
成品尺寸： 185mm×260mm **印张** 15.875 **字数** 386 千字
版 次： 2007 年 8 月第一版
印 次： 2007 年 8 月第一次印刷
书 号： ISBN 978-7-81114-225-9
定 价： 30.00 元

编委会名单

编委会主任

郝玉洁

编委（按姓氏笔画为序）

刘乃琦　许春香　李毅超　佘　堃

周世杰　秦　科　谌黔燕　鲁　珂

学术顾问

秦志光　李建平　周明天

序言

随着社会信息化的快速发展，信息已成为社会发展的重要资源，围绕着这一资源所展开的全球性的竞争日趋激烈。信息的安全已不再是个人和涉及少数人利益的问题，而是事关部门、公司、企业甚至国家、地区等政治和经济利益的十分重要的问题。信息安全正在作为一种产业快速发展，而与此相悖的是，信息安全人才匮乏，远远不能满足商业、金融、公安、军事和政府等部门的需求。因此，培养信息安全领域的高技术人才已成为我国高等工程教育领域的重要任务。

信息安全是集计算机、通信工程、数学等学科知识为一体的交叉型新学科，对于这一新兴学科的培养模式和课程设置，各高等院校普遍缺乏经验，为此，电子科技大学计算机科学与工程学院信息安全专业的专家、学者和工作在教学一线的老师们，以我国本科高等工程教育人才培养目标为宗旨，组织了一系列信息安全的研讨活动，认真研讨了国内外高等院校信息安全专业的教学体系和课程设置，在进行了大量前瞻性研究的基础上，启动了普通高等院校信息安全“十一五”规划教材的编写工作。该系列教材由 8 本理论教材和 2 本实验教材组成，全方位、多角度地阐述了信息安全技术的原理，反映了当代信息安全研究发展的趋势，突出了实践在高等工程教育人才培养中的重要性，弥补了目前该类教材理论教学内容丰富，而实践教学不成体系的缺点，使其成为该系列教材的特点，也是其成功所在。

感谢电子科技大学信息安全专业的老师们为促进我国高等院校信息安全专业建设所付出的辛勤劳动，相信这套教材一定会成为我国高等院校信息安全人才培养的优秀教材。同时希望电子科技大学的教师们继续努力，为培养更多、更好的信息安全人才，为我国的信息安全事业作出更大的贡献。

二〇〇七年三月十日于香港

唐远炎　国际电子电气工程学会会士（IEEE Fellow）
国际模式识别学会会士（IAPR Fellow）
国际 IEEE SMC 机器学习委员会主席（Machine Learning Committee, IEEE SMC）
《中国高等学校学术期刊》计算机科学分册（Frontiers of Computer Science in China）副主编
国际 SCI 检索刊物《International Journal on Wavelet, Multiresolution, and Information Processing（IJWMIP）》（小波、多尺度分辨及信息处理国际期刊）创办人、主编
国际 SCI 检索刊物《International Journal of Pattern Recognition and Artificial Intelligence（IJPRAI）》（模式识别与人工智能国际期刊）副主编

前言

全球经济发展正在进入信息经济时代，知识经济初见端倪。作为 21 世纪的主要经济增长方式——电子商务，将给世界经济带来巨大的变革，产生深远的影响。但如何保证 Internet 网上信息传输的安全，是发展电子商务的重要环节。

为解决 Internet 的安全问题，世界各国对其进行了多年的研究，初步形成了一套完整的 Internet 安全解决方案，即目前被广泛采用的 PKI 技术(Public Key Infrastructure，公钥基础设施)，PKI 是依托于 20 世纪 70 年代发展起来的公开密钥密码学技术，1988 年，标准化组织 CCITT（ITU 的前身）已经开始着手数字证书的标准化工作，诞生了 PKI 的基础标准 X.509，它实际上是 X.500 系列目录服务 30 多个标准中一个“小”规范，然而从目前的发展来看，这个“小”规范衍生出了决定全球电子商务健康发展的公钥基础设施（PKI），从更深层次的意义来讲，PKI 奠定了世界经济一体化的基础。

PKI 这个词汇并不是从公开密钥密码学诞生那天就有的，实际上它是 20 世纪 90 年代末期随着 Internet 的飞速发展、普及才出现的。从提出公开密钥密码学到 PKI 出现的整整 20 年的间隙实际上正折射出了 Internet 从学院走向“无边界”的大众世界的发展历程。

与传统的对称密码密码学相比，公开密钥密码学除了在效率上有所欠缺外，它在密钥交换、密钥管理、抗抵赖性上具有无可比拟的优势。电子商务的公平性建立在抗抵赖性上，分析目前的密码技术，只有公开密钥密码学才能真正有效地提供这种特性。为了解决公开密钥密码学的效率问题，人们提出了许多新的公开密钥系统，然而除了传统的 DH、RSA、DSA 等密码体制，大部分系统都因不够安全而消亡了。令人激动的发展来自于椭圆曲线密码体制方面的工作。2003 年 5 月 12 日中国颁布的无线局域网国家标准 GB15629.11 中，包含了全新的 WAPI(WLAN Authentication and Privacy Infrastructure)安全机制，采用了椭圆曲线密码（ECC）算法。

本书从 PKI 的发展历史入手，介绍了 PKI 的各种关键技术，然后针对各种关键技术，以独立的章节阐述。数学基础主要描述了 RSA 和椭圆曲线算法所需要的基础，便于感兴趣的学生更深入地研究。本书大部分章节出于工程角度介绍 PKI 体制和各关键技术的实施，第 9、10 章还给出了无线环境下 PKI 的实施案例，WAP 和 WTLS。

本书的工作来自于电子科技大学——卫士通信息安全联合实验室所有成员 3 年来集体智慧的结晶。在本书的编写过程中，李桂林同学、郭轶同学、代星科同学、刘金华、王先进同学查阅和整理了大量的第一手资料。特别感谢刘可老师、严洁老师、夏迁同学、李波同学几年工作的积累和科学的态度，这是本书智慧的源泉。

由于作者水平有限，书中失误、不当之处难免，欢迎大家批评指正。

作　者

2007.5

目录

第1章 PKI 概 论

第2章 数 学 准 备

第 3 章 数 字 证 书

第 4 章 PKI 的信任模型

第5章 CA（CERTIFICATE AUTHORITY）系统

第6章 CA 系统功能

第7章 注册机关（RA）

第 8 章 轻量级目录访问协议（LDAP）

第 9 章 无线 PKI（WPKI）

第 10 章 WTLS 协议

第1章

PKI 概 论

1.1 PKI 的历史背景

1.1.1 ⇒ PKI 在欧美的发展

自 1976 年第一个正式的公共密钥加密算法诞生后，20 世纪 80 年代初期出现了非对称密钥密码体制，即公钥基础设施（PKI），但是前期一直处于探索发展阶段，直到最近几年，国外的 PKI 应用才开始快速的发展。1976 年，美国的密码学专家 Diffie 和 Hellman 提出了著名的 D-H 密钥分发体制，第一次解决了不依赖秘密信道的密钥分发问题，允许在不安全的媒体上双方交换信息，安全地获取相同的用于对称加密的密钥，公钥则在电话簿中公布。1978 年 Kohnfelder 提出了 Certificate Agency（CA 认证机构）的概念，在 CA 集中式管理的模式下，公钥以 CA 证书形式公布于目录库，私钥仍以秘密（物理）信道分发。1991 年相继出现了 PGP、PEM，第一次提出密钥由个人生成的分散式体制，以不传递私钥的方式避开了秘密信道。1996 年出现 SPKI 解决方案。PKI 设立了 CA 认证中心，以第三方证明的方式将公钥和标识绑定，并创立了层次化 CA 架构。

美国作为最早提出 PKI 概念的国家，于 1996 年成立了美国联邦 PKI 筹委会，其 PKI 技术在世界上处于领先地位，与 PKI 相关的绝大部分标准都由美国制定。2000 年 6 月 30 日，美国总统克林顿正式签署美国《全球及全国商业电子签名法》，给予电子签名、数字证书以法律上的保护，这一决定使电子认证问题迅速成为各国政府关注的热点。美国联邦政府的 PKI 体系建设形成了以下信任层次和信任域：（1）策略批准机构（PAA）：这是联邦 PKI 的根节点，负责批准二级节点的安全策略；（2）策略产生机构（PCA）：也叫做策略认证机构，是联邦 PKI 的二级节点，定义下级产生公钥证书节点的安全策略；（3）认证机构（CA）：是联邦 PKI 的三级节点，依据 PCA 定义的安全策略，为下级用户（可能是下级 CA）签发和维护数字证书、CRL 结构等；（4）用户：数字证书及相应私有密钥的持有者，用户利用数字证书和私有密钥进行数据保护、身份鉴别等安全行为。除上述层次外，联邦 PKI 体系还包含一个目录系统，用于存放有效证书和已经作废的证书。美国联邦政府在研究各联邦政府已建成的 PKI 体系的基础之上，为解决各种不同认证系统之间的交叉认证问题，于 1998 年提出了桥接 CA 的概念，旨在解决不同信任域之间的信息传递问题，避免形成信任孤岛。

加拿大在 1993 就已经开始了政府 PKI 体系雏形的研究工作，到 2000 年已在 PKI 体系方面获得重要的进展，已建成的政府 PKI 体系为联邦政府与公众机构、商业机构等进行电子数据交换时提供信息安全的保障，推动了政府内部管理电子化的进程。加拿大与美国代表了发达国家 PKI 发展的主流。

欧洲在 PKI 基础建设方面也成绩显著。已颁布了 93 / 1999EC 法规，强调技术中立、隐私权保护、国内与国外相互认证以及无歧视等原则。为了解决各国 PKI 之间的协同工作问题，它采取了一系列措施：积极资助相关研究所、大学和企业研究 PKI 相关技术；资助 PKI 互操作性相关技术研究，并建立 CA 网络及其顶级 CA。并于 2000 年 10 月成立了欧洲桥 CA 指导委员会，于 2001 年 3 月 23 日成立了欧洲桥 CA。

此外，许多国外的企业开展了 PKI 的研究。较有影响力的企业有 Baltimore 和 Entrust，其产品如 Entrust / PKI 5.0，已经能较好地满足商业企业的实际需求。VeriSign 公司也已经开始提供 PKI 服务，Internet 上很多软件的签名认证都来自 VeriSign 公司。

1.1.2 ⇒ PKI 在亚洲的发展

在亚洲，韩国是最早开发 PKI 体系的国家。韩国的认证架构主要分三个等级：最上一层是信息通讯部，中间是由信息通讯部设立的国家 CA 中心，最下一级是由信息通讯部指定的下级授权认证机构（LCA）。日本的 PKI 应用体系按公众和私人两大类领域来划分，而且在公众领域的市场还要进一步细分，主要分为商业、政府以及公众管理内务、电信、邮政三大块。

PKI 技术在整个亚洲虽然有了一定的发展，但处于一个相对落后的水平，还存在着许多亟须解决的问题。

1.1.3 ⇒ PKI 在我国的发展

我国的 PKI 技术从 1998 年开始起步，由于政府和各有关部门近年来对 PKI 产业的发展给予了高度重视，2001 年 PKI 技术被列为“十五”863 计划信息安全主题重大项目，并于同年 10 月成立了国家 863 计划信息安全基础设施研究中心。国家计委也在制定新的计划来支持 PKI 产业的发展，在国家电子政务工程中明确提出了要构建 PKI 体系。目前，我国已全面推动 PKI 技术研究与应用。2004 年 8 月 28 日，十届全国人大常委会第十一次会议表决通过了电子签名法，规定电子签名与手写签名或者盖章具有同等的法律效力。这部法律的诞生将极大地推动我国的 PKI 建设。

自从 1998 年国内第一家以实体形式运营的上海 CA 中心（SHECA）成立以来，PKI 技术在我国的商业银行、政府采购以及网上购物中得到广泛应用。目前，国内的 CA 机构分为区域型、行业型、商业型和企业型四类；截至 2002 年底，前三种 CA 机构已有 60 余家，58% 的省市建立了区域 CA，部分部委建立了行业 CA。其中全国性的行业 CA 中心有中国金融认证中心 CFCA、中国电信认证中心 CTCA 等。区域型 CA 有上海 CA 中心、广东电子商务认证中心等。但是，我国的 PKI 建设还是处于起步阶段，存在不少亟须解决的问题，主要是以下几个方面：一是缺乏国家统一指导，管理问题突出，至今尚未建立权威的管理部门。分散的 CA 规模小，利用率低，低估了建设 CA 的社会责任和经济责任。二是各种来源不同、参差不齐的技术供应厂商大量涌现，亟待研究具有我国自主知识产权的基础技术和标准体系。在尚未确立国家标准的情况下，各家在建立 CA 的过程中对技术标准和管理规范的理解有较大差距，并且各家 CA 基本处于互相分割状态，成为互不关联的信任孤岛，尚未形成完整的国家 PKI 体系。缺乏有力的法律支持。可喜的是电子签名法的确立让人们看到了希望。

我国正在拟订全面发展国内 PKI 建设的规则，其中包括国家电子政务 PKI 体系和国家公共 PKI 体系的建设。从 2003 年 1 月 7 日在京召开的中国 PKI 战略发展与应用研讨会可知，我国将组建一个国家 PKI 协调管理委员会来统管国内的 PKI 建设，由它来负责制订国家 PKI

管理政策、国家 PKI 体系发展规划，监督、指导国家电子政务 PKI 体系和国家公共 PKI 体系的建设、运行和应用。据有关机构预测，电子政务的外网 PKI 体系建设即将展开，在电子政务之后，将迎来电子商务这个 PKI 建设的更大商机，中国的 PKI 建设即将迎来大发展。

PKI 的应用非常广泛，PKI 支持 SSL、IP over VPN、S / MIME 等协议，这使得它可以支持加密 Web、VPN、安全邮件等应用。而且，PKI 支持不同 CA 间的交叉认证，并能实现证书、密钥对的自动更换，这扩展了它的应用范畴。一个完整的 PKI 产品除主要功能外，还包括交叉认证、支持 LDAP 协议、支持用于认证的智能卡等。此外，PKI 的特性融入各种应用（如防火墙、浏览器、电子邮件、群件、网络操作系统）也正在成为趋势。基于 PKI 技术的 IPSec 协议，现在已经成为架构 VPN 的基础，它可以为路由器之间、防火墙之间，或者路由器和防火墙之间提供经过加密和认证的通信。目前，发展很快的安全电子邮件协议是 S/MIME，S/MIME 是一个用于发送安全报文的 IETF 标准。它采用了 PKI 数字签名技术并支持消息和附件的加密，无须收发双方共享相同密钥。目前该标准包括密码报文语法、报文规范、证书处理以及证书申请语法等方面的内容。基于 PKI 技术的 SSL / TLS 是互联网中访问 WEB 服务器最重要的安全协议。当然，它们也可以应用于基于客户机 / 服务器模型的非 WEB 类型的应用系统。SSL/TLS 都利用 PKI 的数字证书来认证客户和服务器的身份。

随着 Internet 应用的不断普及和深入，政府部门需要 PKI 支持管理；商业企业内部、企业与企业之间、区域性服务网络、电子商务网站都需要 PKI 的技术和解决方案；大企业需要建立自己的 PKI 平台；小企业需要社会提供商业 PKI 服务。此外，作为 PKI 的一种应用，基于 PKI 和虚拟专用网市场也随着 B2B 电子商务的发展而迅速膨胀。总的来说，PKI 的市场需求非常巨大，基于 PKI 的应用包括了许多内容，如 WWW 安全、电子邮件安全、电子数据交换、信用卡交易安全、VPN。从行业应用来看，电子商务、电子政务、远程教育等方面都离不开 PKI 技术。随着 PKI 技术的应用与发展，无论是在有线网络，还在无线世界，PKI 必将发挥巨大作用。

由于 PKI 是重大国家利益和网络经济的发展的制高点，也是推动互联网发展、保障事务处理安全、推动电子政务、电子商务的支撑点。因此，建立健全的国家 PKI 体系，将有力地促进我国电子政务以及整个国家信息化的发展。这样，政府和企业都十分重视 PKI 建设，PKI 应用有着巨大的发展前景。

1.2 PKI 理论基础

1.2.1 什么是基础设施

基础设施就是一个普适性基础，它在一个大环境起着基本框架的作用，例如，电子通信网络和电力供应基础设施。在电子通信网络中，局域网和广域网可以让企业内部的计算机在 Intranet 上互相交流数据，让个人用户登录 Internet 冲浪；对于电力供应基础设施，各种电气设备只要插在电源插座上，就可以获取运行所需要的电压和电流。这些设施基本原理共通，操作简便，只要遵循基本的原则，不同的实体就可以方便地使用基础设施提供的服务。

作为基础设施，需要实现“应用支撑”的功能，可以让“应用”正常工作。比如电力系统可以支撑电灯的工作，而且电力基础设施也要具有通用性和实用性，使它能够支持各种新的应用。比如微波炉的应用在电力基础设施设计的时候并没有出现，基础设施的使用应该就像把电气设备的插头插到墙上的插座一样简单，它应具有以下特性：

（1）具有易于使用、众所周知的界面。

（2）基础设施提供的服务可以预测并且有效。

（3）应用设备无须了解基础设施的工作原理。

还以电灯为例，电灯使用者并不关心电能是怎样在发电站里产生，如何经过变电设备转换，最后以什么方式送到房间里来的，房间里遍布的各种各样的插座都没有任何区别。只要把电灯的电源插头插到任何一个插座里，它就能通过众所周知的接口（电源插座）得到指定的电压和电流，从中获得能量，于是正常地工作。

1.2.2 安全基础设施的概念

安全基础设施必须依照同样的原理，同样提供基础服务，也就是说要具有普适性。它为整个组织提供的是保证安全的基本框架，并且可以被组织内任何需要安全的应用和对象使用。安全基础设施的“接入点”必须是统一的、便于使用的（就像墙上的插座一样）。只有这样，那些需要使用这种基础设施的对象在使用安全服务时，才不会遇到太多的麻烦。具有普适性的安全基础设施首先应该是适用于多种环境的框架，这个框架避免了零碎的、点对点的，特别是没有互操作性的解决方案，引入了可管理的机制以及跨越多个应用和计算平台的一致的安全性。不难想象，假如每一对通信方都使用他们自己的通信线路进行通信，或者每个人都用自己的发电机来产生电压和电流，这个世界将是多么的混乱!

安全基础设施能够保证应用程序增强数据和资源的安全，保证增强与其他数据和资源进行交换中的安全。安全基础设施还必须具有同样友好的接入点，应用程序无须了解基础设施提供安全服务的原理，它只要能得到服务就行了。对于安全基础设施来说，能够提供一致有效的安全服务是最重要的。

安全基础设施提供的服务主要包含以下几个方面：

（1）安全登录

在访问网络资源,或者使用某些应用程序的时候，用户往往会被要求首先“登录”或者“注册”。在这一步骤中，典型的操作过程包括用户输入用户身份的信息（如用户标识或姓名、昵称）以及认证信息（如口令或其他机密信息）。如果除了合法用户没有人能够获取用户的认证信息，采用这种方法能够安全地允许合法用户进入系统或者指定的应用程序。

绝大多数使用过计算机的人都对这种操作比较熟悉。登录是广泛使用的一种保护措施，但是它所带来的问题也是显而易见的。比如，当一个网页要求用户进行登录，这个用户是远程的（也就是从不同的设备，比如另外一台计算机登录），所以口令信息会在未受保护的网络上传递，这就非常容易被截取或监听，所谓的重放攻击就是通过中途截取来实施的。即使口令已经被加密也无法防范重放攻击（有的安全基础设施会增加时间信息来做防止重放攻击，这在后面会详细说明）。