Springer

计算机安全基础

Fundamentals of Computer Security

[德] Josef Pieprzyk, Thomas Hardjono, Jennifer Seberry 著
田玉敏　薛赛男　等译

中国水利水电出版社
www.waterpub.com.cn

计算机安全基础

Josef Pieprzyk

[德] Thomas Hardjono 著

Jennifer Seberry

田玉敏 薛赛男 等译

中国水利水电出版社

内 容 提 要

本书重点介绍了密码学、计算机与网络安全的基本概念，为读者提供了完整而全面的理论和技术支持。本书的主要内容包括：密码学基础、私钥密码系统、公钥密码系统、伪随机数、散列法、数字签名、认证、秘密共享、零知识证明系统、群体密码学、密钥建立协议、身份识别、入侵检测、电子投票和数字货币、数据库保护与安全、访问控制以及网络安全等。

全书内容广博权威，讲解由浅入深，且重要的章节都附有习题，可以帮助读者进一步掌握本章的内容。本书适用于计算机专业或相关专业本科生专业课、研究生课程教材，也可作为专业人员的参考书。

图书在版编目（CIP）数据

计算机安全基础 /（德）帕布鲁兹（Pieprzyk,J.）等著；田玉敏等译. —北京：中国水利水电出版社，2006

书名原文：Fundamentals of Computer Security

ISBN 7-5084-4075-7

Ⅰ. 计… Ⅱ. ①帕… ②田… Ⅲ. 电子计算机－安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2006）第 110980 号

书　　名	计算机安全基础
作　　者	[德] Josef Pieprzyk Thomas Hardjono Jennifer Seberry 著
译　　者	田玉敏 薛赛男 等译
出版发行	中国水利水电出版社（北京市三里河路 6 号 100044） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）63202266（总机）、68331835（营销中心）、82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京市天竺颖华印刷厂
规　　格	787mm×1092mm 16 开本 29.25 印张 729 千字
版　　次	2006 年 10 月第 1 版 2006 年 10 月第 1 次印刷
印　　数	0001—4000 册
定　　价	48.00 元

前　言

本书的主要目的是论述计算机与网络安全的基本概念。本书的初稿源自作者在澳大利亚武龙岗（Wollonggong）大学教授本科课程《计算机安全》时使用的讲稿。后来，给本书添加了许多课题，这些课题主要作为高级密码学课程的内容讲授给研究生。本书包含的某些章节，特别是本书后面的那些章节是为了帮助学生们准备他们的学术报告会而准备的。最近，本书被麦克夸利河（Macquarie）（澳大利亚）大学计算系用作三年级本科生的一门新课程《密码学与信息安全》的教科书。

本书共有 18 章。第 1 章简单地概述了密码学的历史。作为一本书，其包含的知识应该是完备的，因此在有关原理这一章（第 2 章）介绍了必要的背景知识。这一章由数论基础开始，涵盖了代数结构、计算复杂度以及信息论基础。

关于私钥密码系统的那一章（第 3 章）包括传统密码、DES 系列密码以及精选的在征集 AES 时提交的现代密码系统的一个子集。这一章还介绍了差分密码分析和线性密码分析。第 4 章讨论公钥密码学的背景，论述公钥的概念并讨论其实现。至少有两个原因使 RSA 密码系统值得注意。第一个原因是：其安全性与因式分解的难度密切相关。另外一个原因是：为了通信安全，人们广泛采用 RSA。最后，这一章讨论了概率密码和现代公钥密码系统。

第 5 章研究伪随机数并介绍多项式不可分这一概念。然后讨论比特伪随机发生器、函数及其置换。第 6 章论述散列法、生日悖论，研究其在破译散列函数方面的应用。这一章的主要内容致力于讨论散列函数的 MD 系列（MD5、SHA-1、RIPEMD-160 以及 HAVAL）。以键入—散列法结束本章。

第 7 章从一次性签名方案开始讨论签名方案。这一章论述的基本签名方案是 RSA 和 ElGamal 签名。此外，第 7 章还讨论盲签名、不可否认签名和防失败签名。第 8 章论述认证，认证虽然与数字签名有关，但已经发展了自己的理论以及专业词汇。

秘密共享是使小组能够实施密码操作的主要密码工具之一。第 9 章论述了秘密共享的基本理论。第 10 章介绍秘密共享在密码学中的应用。

第 11 章讨论的密钥建立协议分为两大类：密钥协商协议和密钥分配协议。这两类协议通常涉及通信双方需要生成新密钥的情况。密钥建立协议的多方形式的重要性日益增加，因而也在本章中进行了论述。本章最后简单介绍 BAN 逻辑。

零知识证明系统是双方——证明者和验证者——进行交互的一个交互系统。证明者声明某一命题为真，并且想说服验证者这一命题的确为真。双方交互，交互到最后，验证者或者被说服相信命题为真，或者是另一种情况，验证者发现命题不为真。第 12 章论述这一课题。

第 13 章讨论身份识别（identification）。首先概述了用于用户身份识别的生物识别技术。之后，讨论口令以及质询—响应识别。但这一章的主要内容致力于论述基于零知识证明的识别。

有关入侵检测的那一章（第 14 章）首先讨论两种一般的方法：异常和误用检测。前一种方法使用用户行为的简档（profile）对可疑的入侵做出判定。后一种方法利用一个描述误用计算资源特征的单一简档。同时还论述了主机和网络入侵检测系统的选择实现。

第 15 章介绍电子商务技术，同时还包括电子选举和电子货币方面的知识。第 16 章着眼于数据库安全，重点是安全过滤器、密码方法和数据库视图。最后概述了 Oracle8 中应用的安全特性。

第 17 章研究访问控制。考虑了三种模型：强制性访问控制、任意访问控制和基于角色的访问控制。这一章还讨论了一些选择实现。第 18 章介绍 IPSec 协议和计算机病毒。

本书的内容大致可以分为两部分：

1. 密码学（第 3 到 13 章）
2. 计算机与网络安全（第 14 到 18 章）

可以参照下面的层次结构来安排各章的内容：

绪论	基础理论

密码学			
私钥密码系统	公钥密码系统	秘密共享	认证
伪随机数	散列法	零知识证明系统	
数字签名			
群体密码学	密钥建立协议	身份识别	

计算机与网络安全				
入侵检测	电子选举和数字化货币	数据库保护与安全	访问控制	网络安全

密码学部分包括 4 章基础内容：私钥密码系统、公钥密码系统、秘密共享和认证。可以独立地学习，因为各章的内容几乎没有交叉（参见上表第 3 行）。关于伪随机数、散列法和零知识证明系统（上表中的第 4 行）建立在前 4 章所述知识的基础之上。例如，零知识证明系统要求很好地掌握公钥密码系统。“散列法”一章对基础章节的依赖不是很强，但散列法的确利用了私钥和公钥密码。数字签名的概念与私钥、公钥密码以及散列法密切相关。密码学部分中包括关于复杂课题的几章，我们希望读者一定要首先理解这一部分每章中前两行的概念。特别是要理解有关章节中的内容：

- 群体密码学：建议学完有关公钥密码体制、秘密共享、散列法以及数字签名这几章。
- 密钥建立协议：要求读者掌握公钥密码系统的内容，包括数字签名的背景知识。
- 身份识别：最好熟悉数字签名以及零知识证明系统。

本书可以作为本科生和研究生课程的教材。下面列出了本书能够支持的一些课程示例：

- 密码学导论：基础理论、私钥密码系统、公钥密码系统、散列法和数字签名。
- 电子商务：基础理论、公钥密码系统、散列法、数字签名、电子选举以及数字化货币。
- 高级密码学：认证、秘密共享、群体密码学、密钥建立协议、零知识证明系统以及身份识别。
- 计算机与网络安全：入侵检测、数据库保护及安全、访问控制以及网络安全。

各位合作者对本书的贡献如下表所示：

合著者的名字	章节
Josef Pieprzyk	所有章节
Thomas Hardjono	第 14 章和第 16 章
Jennifer Seberry	第 3 章和第 18 章

致谢 作者感谢提出宝贵意见和建设性批评意见的人。我们特别感谢 Marc Fischlin、Ron Rivest 和 Abhi Shelat 对本书提出了中肯的评论、建议以及修改意见。感谢花费时间和精力给我们提出反馈意见的许多同事，他们是：

Colin Boyd　　Nicolas Courtois
Ivo Desmedt　　Dieter Gollmann
Hossein Ghodosi　　Jeffrey Horton
Andrew Klapper　　Keith Martin
Anish Mathuria　　Krystian Matusiewicz
Igor Shparlinski　　Michal Sramka
Janusz Stoklosa　　Huaxiong Wang
Xianmo Zhang

我们向那些无意中遗漏没有列出名字的同事致歉。

没有 Springer-Verlag 的 Alfred Hofmann 和他的团队以及 Ingeborg Mayer、Frank Holzwarth、Ronan Nugent 等的大力支持和鼓励，就不会有本书。谢谢你们。我们还感谢 Kate Krastev 和 Deanne van der Myle 在本书最后定稿时所给予的帮助。

发现遗漏或者错误的读者可以直接与作者联系。

本书由田玉敏、薛赛男翻译，在翻译过程中，谢君英、张波、易磊、唐美艳、赵岗善、代菊容、郭蓓、孟宪瑞、郭军喜、杜芳、盛海燕、武堂、李明做了不少工作，在此表示感谢。

目　　录

第 1 章　绪论

1.1　引言

1988 年，《新大英百科全书》将密码学（Cryptology）定义为：

研究以安全、通常也是保密的方式进行通信的科学。它包括密码编码学和密码分析学两部分。前者涉及信息呈现技术和基本原理的研究与应用，这种技术使得除预期的接收者之外，其他所有人都无法理解所呈现的信息；而后者则是关于破解密码系统以恢复信息的艺术和科学。

目前，现代密码学主要集中于各种信息保护方法和技术的设计和评价，因此密码学的这一定义需要扩展。信息保护不仅涉及保密（传统的防窃听保护），还涉及认证、完整性、可验证性、不可否认性及其他更多的特定安全目标。讨论算法设计、协议以及用于保护信息免受特定威胁的系统的那部分密码学称为密码编码学（Cryptography）。

要将信息保护与系统、协议或服务整合在一起，设计人员需要掌握：

- 系统（协议或服务）将要工作的环境的详细规范，包括一组安全目标。
- 威胁和有关系统中可能篡改信息流的地方描述列表。
- 必需的保护级别或来自攻击者（或对手）的预期强度（依据可访问的计算资源）。
- 系统的预计生命周期。

密码编码学为设计人员提供了实施要求的信息保护（也就是实现预期的安全目标）的工具。基本工具集包括加密算法、认证码、单向函数、散列函数、秘密共享方案、签名方案、伪随机位生成器、零知识证明系统等。利用这些基本工具，可以创建更复杂的工具和服务，例如，门限加密算法、认证协议、密钥建立协议和多种面向应用的协议，包括电子支付系统、电子投票以及电子商务协议等。每种工具的特点都是其安全规范通常都指定了推荐的配置和抗特殊威胁的强度，如窃听和对信息的非法修改等。设计人员可以使用密码编码学提供的所有工具来将它们合并为单一的解决方案。最后，设计人员还必须对解决方案的质量进行验证，包括对获得的整体安全性进行仔细分析。

密码学的另一部分是密码分析学（Cryptanalysis）。密码分析学使用数学方法证明设计（信息保护的实现）没有达到安全目标或经受不住设计安全规范中给出的各种威胁的攻击。如果声明的安全参数是粗略高估出来的，或更为经常的是，如果不了解不同威胁之间的相互联系，则很可能发生这种情况。

留心的读者可能会认为：密码编码学包括密码分析学，因为设计人员总是对所获得的信息保护应用某种分析。为了澄清这一点，应注意密码编码学的目的是设计新的安全算法、协议、系统、方案和服务，而密码分析学则集中于发现新的攻击。攻击（密码分析学的一部分）会被转换为所谓的设计准则或设计属性（密码编码学的一部分）。由攻击获得的设计准则使我们能够设计免受攻击的系统。

密码编码学试图使用有关各种可能的攻击的所有可用知识来证明所获得的设计是安全的。

而密码分析学仔细研究可能的和实际的威胁以发现新的攻击，并证明设计是不安全的（是脆弱的）。总之，证明信息保护设计坚不可摧是不可能的，而反过来证明信息保护设计不安全则是可能的——只要给出一种攻击就足够。

1.2 术语

密码编码学的词汇非常多。本书将逐一介绍比较复杂的术语。下面介绍一组基本术语。

基本的安全要求。这包括：保密性（或机密性）、真实性、完整性和不可否认性。保密性可确保发送者和接收者之间的信息流对局外人来说是无法理解的，并保护信息免受基于窃听技术的威胁。真实性使消息的接收者可以确定发送者的真实身份，从而防止假冒消息、替代消息或电子欺骗。完整性使接收者能够确认通过不安全通道传送消息时，外来者有没有进行篡改，从而保证对消息流的任何修改都能够被检测出来。传送的消息的顺序发生变化，消息的某些部分被删除，或旧消息重放所导致的任何修改都可以检测出来。不可否认性防止消息的发送者否认他们曾经发送过该消息。

加密是为确保通过不安全通信信道传送的消息的保密性或机密性而使用的第一步密码操作。加密操作取一段信息（通常称为消息、消息块或明文），然后利用密钥将其翻译为密文（加密文本或编码字）。解密是加密的逆操作。持有正确密钥的接收者可以从密文（加密文本）恢复消息（明文）。

对加密（或解密）过程的逐步描述称为加密算法（或解密算法）。如果不需要区分加密和解密，我们将把它们通称为密码（Cipher）、密码算法或密码系统。

私钥，即对称密码系统，其加密和解密过程使用相同的密钥。更准确地说，加密密钥和解密密钥不需要完全相同——知道了其中任何一个就可以找到另一个（对两种密钥必须保密）。

公钥，即非对称密码系统，其加密和解密过程使用不同的密钥。即使知道其中一个也不会暴露另一个。

散列是生成任意长度的消息的相对较短的摘要的密码操作。散列算法必须具有抗碰撞性，即找到两条具有相同摘要的不同消息非常困难。

单向函数是这样的函数：根据其自变量值很容易求出其函数值，而反过来，在已知函数值的情况下，求其自变量值则比较困难。

电子签名是一个公开的、较短的字符串（或位串），用于确认电子文档（任意长度的消息）的原作者。

秘密共享是在参与者中间分发秘密的一种方法，以便每一个足够大的参与者子集都能通过汇集其共享份额再现他们的秘密。这样的子集的类统称为存取结构。秘密共享由所谓的分发者建立，对于给定的秘密，分发者生成所有的共享份额并将它们发送给所有的参与者。秘密的重新计算由所谓的组合者完成，合作的所有参与者都将他们的共享信息委托给组合者。存取结构之外的任何一个或任何一组参与者都无法了解该秘密。

密码分析学也有其自己的术语。一般来讲，密码设计安全性可以是无条件的，也可以是有条件的。无条件安全设计可以免受任何攻击者的攻击，并具有无限的计算能力。而对于有条件安全设计，其安全性取决于逆转基本密码问题的难度。这种设计充其量也只能达到基本密码问题的强度。