普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

# 认证理论及应用

李晓航 王宏霞 张文芳 编著
沈昌祥 审

Information Security

http://www.tup.com.cn

根据教育部高等学校信息安全类专业教学指导委员会制订的《信息安全专业指导性专业规范》组织编写

清华大学出版社

普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇



# 认证理论及应用

李晓航 王宏霞 张文芳 编著
沈昌祥 审

http://www.tup.com.cn



根据教育部高等学校信息安全类专业教学指导委员会制订的
《信息安全专业指导性专业规范》组织编写

清华大学出版社
北京

## 内容简介

本书是一本集中介绍信息安全领域中认证技术的教材。全书共分为8章，主要内容包括认证理论的基础、Hash函数和报文鉴别、数字签名、实体认证和密钥交换协议、身份认证协议、智能卡技术及其在认证系统中的应用、基于数字水印技术的多媒体认证、典型的实用网络认证协议等。

本书在编排时主要围绕密码学中为对抗主动攻击而引入的认证理论及相关内容，突出了应用性，并结合作者在相关领域的科研成果引入了新的认证技术，如基于数字水印的多媒体认证技术。

本书可作为信息安全、计算机应用等专业的研究生和高年级本科生以及相关领域技术人员的教材，为他们在认证理论及应用方面的学习和工作提供必要的参考。



**图书在版编目（CIP）数据**

认证理论及应用 / 李晓航，王宏霞，张文芳编著．—北京：清华大学出版社，2009.11
（高等院校信息安全专业系列教材）
ISBN 978-7-302-20827-3

Ⅰ．认…　Ⅱ．①李…　②王…　③张…　Ⅲ．电子计算机－安全技术－高等学校－教材
Ⅳ．TP309

中国版本图书馆CIP数据核字(2009)第156672号

**责任编辑**：张　民　李玮琪
**责任校对**：梁　毅
**责任印制**：王秀菊

**出版发行**：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编**：100084
**社　总　机**：010-62770175　　**邮　　购**：010-62786544
**投稿与读者服务**：010-62776969，c-service@tup.tsinghua.edu.cn
**质　量　反　馈**：010-62772015，zhiliang@tup.tsinghua.edu.cn
**印 刷 者**：北京国马印刷厂
**装 订 者**：北京市密云县京文制本装订厂
**经　　销**：全国新华书店
**开　　本**：185×260　　**印　　张**：15　　**字　　数**：350千字
**版　　次**：2009年11月第1版　　**印　　次**：2009年11月第1次印刷
**印　　数**：1～3000
**定　　价**：25.00元

高等院校信息安全专业系列教材

# 编审委员会

# 出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数既是在本专业领域有深厚的学术造诣，又是在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教

材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展将起到重要的指导和推动作用。“高等院校信息安全专业系列教材”将在教育部高等学校信息安全类专业教学指导委员会的组织和指导下，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并根据教育部高等学校信息安全类专业教学指导委员会制订的《信息安全专业指导性专业规范》以及信息安全学科的发展不断修订和完善。

我们的E-mail地址是：zhangm@tup.tsinghua.edu.cn；联系人：张民。

清华大学出版社

# 本书序

认证技术是信息安全领域一个非常重要的研究方向，也是在网络安全实际应用中普遍涉及的必要技术。本书所涉及的认证理论基础、数字签名、报文鉴别、认证协议、身份证明、智能卡认证技术、多媒体认证技术和网络认证等内容涵盖了认证领域的广阔内容，可作为信息安全及相关专业高校研究生、本科生普遍适用的教材，以及信息安全领域技术人员必备的技术参考书籍。

在西南交通大学双聘院士交流会上，我了解到西南交通大学早在2001年已设立了信息安全专业，并已开设研究生专业基础课“认证理论与技术”和本科生专业基础课“认证理论及应用”多年，但一直没有合适的教材。由于信息安全专业是一个新兴专业，所以目前市面上关于认证理论方面的教材和专著非常少，而学生在上课时非常需要有一本教材。《认证理论及应用》这本书有助于建立信息安全专业良好的课程体系结构，并满足高校教材及市场的需求。编写这本书的3位老师均多年从事信息安全方向的教学和科研，有着丰富的授课经验和科研实践经历。该书结合应用实例阐述理论，便于抽象理论的理解，同时引入了新的先进的认证技术，并注重知识与技术的更新。

该书是在李晓航老师编写的讲义“认证理论及应用”的基础上经认真修改、扩充而成的。讲义已使用5年，学生反映良好。该书的编写工作得到了西南交通大学研究生特色教材项目的大力支持。因此，我很高兴推荐该书在清华大学出版社出版，相信该书的出版会得到信息安全及相关研究领域广大读者的肯定和喜爱。

沈昌祥

2009年9月

沈昌祥，中国工程院院士，教育部高等学校信息安全类专业教学指导委员会主任委员。

# 前言

21世纪是信息的时代。随着国家信息化的不断推进和电子商务、电子政务的大力建设，信息已经成为最能代表综合国力的战略资源，信息化正在对国家和社会的各方面产生巨大影响。然而，伴随信息化而来的信息安全问题也随之突显，能否有效地保护信息资源，保护信息化进程健康、有序、可持续发展，已经成为关乎国家和社会发展的头等大事。

保障信息安全主要依靠密码学理论及其相关应用。密码学的最初目的是“保密”，即保证机密信息只能被系统中授权的各方所获得。然而随着攻击手段的不断发展，主动攻击逐渐成为信息系统安全的主要威胁，如何防止敌手对信息系统进行主动攻击变得越来越重要。“认证”(Authentication)是现代密码学中对抗主动攻击的重要手段，它对于开放网络环境中各种信息系统的安全有着重要作用，其主要目的是提供信息的真实性、完整性和不可抵赖性，以对抗伪造、篡改和重放等攻击。可以说，在某些情况下“认证”比“保密”更为重要。

为了更好地突出认证理论在现代密码学中的重要作用，建立信息安全专业良好的课程体系结构，作者所在高校开设了“认证理论及应用”这门课，作为信息安全专业的主要专业课。但在授课中发现，经典的密码学教材大都以“保密”为主，以“认证”为辅。为此，作者在参考国内外经典教材的基础上，编写了《认证理论及应用》讲义，用于课堂教学，并在此基础上，结合教学实践和科研工作编著了本书。

本书的主要特色是：

① 围绕密码学中为对抗主动攻击而引入的认证理论及相关内容来进行编排，是一本集中介绍信息安全领域中认证技术的书籍；

② 在编写时突出了应用性，结合应用实例来阐述理论，便于读者深入浅出地理解抽象的问题；

③ 引入了新的认证技术和研究成果，如基于数字水印的多媒体认证技术，注重了知识与技术的更新。

全书共分为8章，第1章是认证理论的基础，阐述了认证系统的一些基本概念、欺骗概率和完善认证等。第2章介绍了Hash函数和报文鉴别，包括经典Hash函数算法介绍和分析，以及利用加密和MAC等实现报文鉴别的方法。第3章介绍了数字签名，包括常规的签名算法和有特殊用途的签名体制。第4章介绍了认证协议，主要用于实体认证及密钥交换。第5章介绍

了身份认证，包括传统的基于密码协议的认证和基于指纹识别的认证。第6章介绍了智能卡技术及其在认证系统中的应用。第7章是基于数字水印技术的多媒体认证，包括图像和音频内容的真实性和完整性认证。第8章介绍了典型的实用网络认证协议，包括IPSec、Keberos、SSL和PKI等标准协议中的认证原理和实现。此外，为帮助读者复习和巩固相关知识，在每章结尾均附有习题或思考题。

本书可作为信息安全、计算机应用等专业的研究生和高年级本科生以及相关领域技术人员的教材，为他们在认证理论及应用方面的学习和工作提供必要的参考。

本书的第1章和第2章部分内容、第5章和第6章由李晓航编写，第1章、第4章和第7章由王宏霞教授编写，第2章、第3章和第8章由张文芳编写。此外，陈帅参与了本书的部分编写和校对工作，在此表示衷心感谢。

本书的撰写工作得到了教育部博士点基金（编号：20070613024）及西南交通大学研究生特色教材项目的支持，在此表示感谢。

由于作者水平有限，书中不妥与疏漏之处在所难免，殷切希望读者指正。

作　者

2009年8月于成都

# 目录

# 第1章 认证理论基础

随着信息的多元化及数字化的迅猛发展，信息安全技术显得越来越重要，而且信息安全技术应用水平的高低直接影响了信息高速公路建设的进一步发展。近20年来，由于计算机硬件处理能力的极大提高和密码学的迅速发展，信息安全理论与技术也在逐步完善和丰富。认证技术是信息安全理论与技术的一个重要方面，主要包括用户认证和信息认证两个方面。前者用于鉴别用户身份，后者用于保证通信双方的不可抵赖性和信息的完整性。

根据认证信息的性质可以将用户认证分为秘密知识证明，物理介质证明和实体特征证明。秘密知识证明主要通过通信双方共享的口令、个人识别码和密钥等进行身份认证。在物理介质证明中，证明方必须提供令牌卡、信用卡和密钥卡等物理介质验证自己的身份。实体特征证明包括实体的物理特征和生物特征，物理特征主要包括计算机通信设备的网卡（如地址、硬盘序列号等），生物特征包括指纹、笔迹、脸形、虹膜、视网膜、脉搏、耳廓和声音等。

在某些情况下，信息认证显得比信息保密更为重要。例如，在金融网络中发生的业务或交易，可能交易的具体内容并不需要保密，但是交易双方应当能够确认是对方发送（接收）了这些信息，同时接收方还能确认接收的信息是完整的，即在通信过程中没有被修改或替换。另一个例子是网络中的信息广播（通知），此时接收方主要关心的是信息的真实性和信息来源的可靠性。因此，在这些情况下，信息认证将处于首要的地位。

从用户角度来看，非法用户常采用以下手段对网络系统进行攻击。

① 窃取口令：非法用户获得合法用户身份的口令，这样一来，虽然他（她）未获得授权，但他（她）可以访问这些系统资源；

② 流量分析：非法用户对通信双方交换的信息进行分析，试图判断或还原原信息；

③ 重传：非法用户截获信息，然后再传送给接收者；

④ 修改或伪造：非法用户截获信息，替换或修改信息后再传送给接收者，或者非法用户冒充合法用户发送信息；

⑤ 阻断服务：阻止系统资源的合法管理和使用。

为了保证信息应用的安全性，认证服务应当提供实体的身份认证、信息的完整性检测、防止重传攻击、秘密认证信息的生成和管理等功能，在某些应用中还要求实现抗抵赖和零知识证明等功能。概括起来，网络安全服务应当提供如下认证功能。

① 可信性：信息的来源是可信的，即信息接收者能够确认所获得的信息不是由冒充者所发出的；

② 完整性：要求信息在传输过程中保证其完整性，即信息接收者能够确认所获得的

信息在传输过程中没有被修改、延迟和替换；

③ 不可抵赖性：要求信息的发送方不能否认他(她)所发出的信息，同样，信息的接收方不能否认已收到了信息；

④ 访问控制：非法用户不能够访问系统资源，合法用户只能访问系统授权和指定的资源。

由此可见，一个安全的信息系统应该提供机密性、鉴别性、完整性、不可抵赖性和可用性等服务，以对抗各种被动攻击(截获)和主动攻击(伪造、篡改、重放及中断等)。传统上，密码学的主要目的是提供机密性，以保证机密信息只能被系统中授权的各方所获得。随着技术的不断发展，如何防止对手对信息系统进行主动攻击变得越来越重要。认证(authentication)是现代密码学中防止主动攻击的重要技术，它对于开放环境中各种信息系统的安全有着重要作用。认证的主要目的是提供信息的真实性、完整性和不可抵赖性，以对抗伪造、篡改和重放等主动攻击。为便于理解，下面给出与认证相关术语的定义。

① 保密(confidentiality)：即保证信息为授权者享用而不泄露给未经授权者；

② 数据完整性(data integrity)：信息数据未被非授权者篡改或者损坏；

③ 实体鉴别：验证一个实体的身份；

④ 数据源发鉴别：验证消息来自可靠的源点，且没有被篡改；

⑤ 签名：一种绑定实体和信息的办法，能够实现用户对电子形式存放消息的认证；

⑥ 授权：把官方做某件事情或承认某件事情的批准传递给另一实体；

⑦ 访问控制：限制资源只能被授权的实体访问；

⑧ 抗否认：防止对以前行为否认的措施；

⑨ 可用性：信息可被授权者访问并使用。

本章介绍的认证理论主要是由 G. J. Simmons 发展起来的，他证明了该领域的许多基本结果。这一理论也是将 Shannon 的信息论用于研究认证系统的理论安全性和实际安全性问题，指出认证系统的性能极限(欺骗概率的下限)，以及设计认证码必须遵循的原则。因此，它是研究认证问题的基础。

## 1.1　认证系统基本概念

### 1.1.1　认证系统模型

保密和认证是信息系统安全的两个重要方面，但它们是两个不同属性的概念。认证不能自动地提供机密性，而保密也不能自然地提供认证功能。图 1-1 是一个基于对称密码体制的对称加密与认证系统模型，为了可靠传送一个(认证后的)消息，通信双方遵循如下基本协议：

① 首先，双方一起选择一个随机密钥 $k \in K$；

② 之后，如果发送方打算在一个不安全的信道上将源状态 $s$ 传给接收方，发送方计

算 $a=e_k(s)$，并把消息$(s,a)$发给接收方；

③ 接收方收到$(s,a)$后，计算 $a'=e_k(s)$，如果 $a'=a$，那么接收的这个消息是可靠的，否则拒绝该消息。

图 1-1 所示方案的认证性在于攻击者不知道密钥，不能按照自己的意图篡改密文内的信息位。因此 $B$ 可确信消息 $M$ 是由 $A$ 发出的。

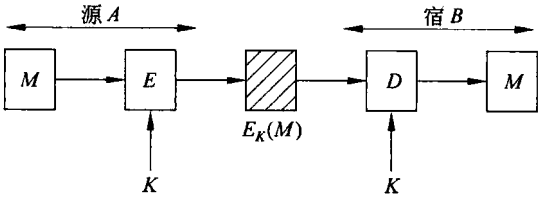


图 1-1 对称加密与认证系统模型

下面再来讨论一下基于非对称密码体制的加密和认证系统模型。分别用 $KU_a$ 和 $KU_b$ 表示 $A$ 方和 $B$ 方的公钥，其对应的私钥分别为 $KR_a$ 和 $KR_b$。图 1-2 是一个公钥加密系统。只有掌握私钥 $KR_b$ 的合法用户才能解密，因此该系统具有保密性。然而，由于加密消息所用的是公钥 $KU_b$，该密钥公开，因此，攻击者能够按照自己的意图篡改密文内的信息位。所以图 1-2 所示的系统仅有保密功能，而无认证功能。

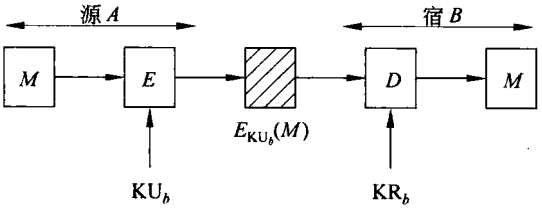


图 1-2 公钥加密系统(有保密性，而无认证性)

如果用私钥 $KR_a$ 加密，用公钥 $KU_a$ 解密，如图 1-3 所示。由于攻击者不知道私钥 $KR_a$，所以他不能按照自己的意图篡改密文内的信息位，因此该系统具有认证性。但解密用的是公钥 $KU_a$，任何人可以通过公开列表获得该公钥，显然该系统无保密性。

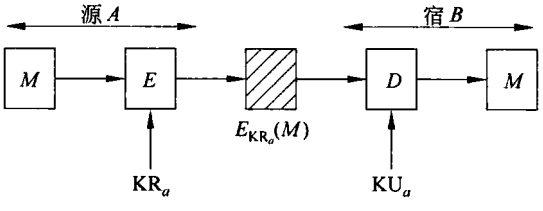


图 1-3 公钥加密系统(有认证性，而无保密性)

纯认证系统的模型如图 1-4 所示。在这个模型中发送者通过一个公开的无扰信道将消息发送给接收者，接收者不仅想收到消息本身，而且还要验证消息是否来自合法的发送者以及消息是否被篡改过。系统的攻击者不再像保密系统中的窃听者那样始终处于消极被动地位，而是主要采用主动攻击，因此称其为系统的窜扰者(tamper)更加贴切。实际的