网络空间安全系列教材

应用密码学

◎ 汤永利　闫玺玺　叶 青　编著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络空间安全系列教材

应用密码学

汤永利　闫玺玺　叶　青　编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

应用密码学作为实现网络信息安全的核心技术，是信息安全应用领域所有人员必须了解的基础知识。从教学适用性出发，本书全面介绍了应用密码学的基本概念、基本理论和典型实用技术。本书对密码学概述、序列密码、分组密码、公钥密码、单向散列函数和消息认证、数字签名、身份认证与访问控制、密钥管理、PKI 技术、电子现金与电子支付系统、安全电子选举系统、安全多方计算等知识进行了深入、系统的描述，并通过多个应用系统全面剖析了相关的密码应用。

本书属于“网络空间安全系列教材”，重视读者对应用密码学知识的系统理解，以及有针对性地讲述重要的知识点。全书图文并茂、文字流畅、表述严谨，包含了应用密码学的基本理论、关键技术及当前热门的实用案例。本书可作为高等院校密码学、信息安全等专业本科生和研究生的教材，也可供从事网络安全领域应用和设计开发的科研人员、工程技术人员参考。

图书在版编目（CIP）数据

应用密码学/汤永利，闫玺玺，叶青编著. —北京：电子工业出版社，2017.1
ISBN 978-7-121-30136-0

Ⅰ. ①应… Ⅱ. ①汤… ②闫… ③叶… Ⅲ. ①密码学 Ⅳ. ①TN918.1

中国版本图书馆 CIP 数据核字（2016）第 248400 号

策划编辑：袁 玺
责任编辑：底 波
印 刷：北京京海印刷厂
装 订：北京京海印刷厂
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
开 本：787×1 092 1/16 印张：23 字数：588.8 千字
版 次：2017 年 1 月第 1 版
印 次：2017 年 1 月第 1 次印刷
定 价：50.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：192910558（QQ 群）。

网络空间安全系列教材

编委会名单

序

随着经济全球化和信息化的发展，以互联网为平台的信息基础设施，对整个社会的正常运行和发展正起着关键的作用。甚至，像电力、能源、交通等传统基础设施，也逐渐依赖互联网和相关的信息系统才能正常运行。网络信息对社会发展有重要的支撑作用。

网络空间是利用全球互联网和计算系统进行通信、控制和信息共享的动态虚拟空间，包括4个要素，分别是网络平台、用户虚拟角色、资产数据和管理活动，网络空间是社会有机运行的神经系统，已经成为继陆、海、空、天之后的第5空间。

网络空间面临的威胁也与日俱增。从国际上看，国家或地区在政治、经济、军事等各领域的冲突都会反映到网络空间中，而由于网络空间边界不明确、资源分配不均衡，导致网络空间的争夺异常复杂。另外，网络犯罪和网络攻击也对个人和企业构成严重威胁。在网络中，个人隐私信息泄露并大范围传播的事件已经屡见不鲜，以非法牟利为目的、利用计算机网络进行的犯罪已经形成了黑色的地下经济产业链。如何充分利用互联网对经济发展的推动作用、保护公民和企业的合法权益，同时又要控制其对经济社会发展带来的负面威胁，需要研究和探索更加科学合理的网络空间安全治理模式。正如习近平总书记所言：“没有网络安全，就没有国家安全。”

加强网络空间安全已经成为国家安全战略的重要组成部分。2014年2月，中央网络安全和信息化领导小组成立。2015年6月，国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科，并明确指出需加强“网络空间安全”的学科建设，做好人才培养工作。2016年3月，国务院学位委员会下发通知，明确全国共有29所高校获得我国首批网络空间安全一级学科博士学位授权点。6月，中央网络安全和信息化领导小组办公室、国家发展和改革委员会、教育部、科学技术部、工业和信息化部、人力资源和社会保障部联合发文，《关于加强网络安全学科建设和人才培养的意见》（中网办发文［2016］4号）指出，网络空间的竞争，归根结底是人才竞争。我国网络空间安全人才还存在数量缺口较大、能力素质不高、结构不尽合理等问题，与维护国家网络安全、建设网络强国的要求不相适应。该文提出要加快网络安全学科专业和院系建设、创新网络安全人才培养机制、加强网络安全教材建设、强化网络安全师资队伍建设、完善网络安全人才培养配套措施等意见。

网络空间安全主要研究网络空间中的安全威胁和防护问题，即在有敌手的对抗环境下，研究信息在产生、传输、存储、处理、销毁等各个环节中所面临的威胁和防御措施，以及网络和系统本身面临的安全漏洞和防护机制，不仅包括传统信息安全所研究的信息的保密性、完整性和可用性，同时还包括构成网络空间基础设施的安全和可信度。从宏观层面来看，网络空间安全的研究对象主要包括全球各类各级信息基础设施的安全威胁；从微观层面来看，主要对象包括通信网络、计算机网络及其设备和应用系统中的安全威胁。

数学、信息论、计算复杂性理论等是网络空间安全所依靠的重要理论基础。

网络空间安全的理论体系由3部分组成。一是基础理论体系，主要包括网络空间理论、

密码学、离散结构理论和计算复杂性理论等。其中，信息的机密性、完整性、可控性、可靠性等是核心，对称加密、公钥加密、密码分析、侧信道分析等是重点，在复杂环境中的可证安全、可信可控及定量分析理论是关键。二是技术理论体系，主要包括网络空间安全保障理论体系。从系统和网络角度来看，研究和设计网络空间的各种安全保护方法和技术，重点包括芯片安全、操作系统安全、数据库安全、中间件安全、恶意代码等，以及从预警、保护、检测到恢复响应的安全保障技术理论；从网络安全角度来看，以通信基础设施、互联网基础设施等为研究对象，聚焦研究通信安全、网络安全、网络对抗等。三是应用理论体系，从应用角度来看，针对各种应用系统，研究在实际环境中面临的各种安全问题，如 Web 安全、内容安全、垃圾信息等，涵盖电子商务、电子政务、物联网、云计算、大数据等诸多应用领域。

网络空间安全有如下 5 个研究方向。一是网络空间安全基础，包括网络空间安全数学理论、网络空间安全体系结构、网络空间安全数据分析、网络空间博弈理论、网络空间安全治理与策略、网络空间安全标准与评测等。二是密码学及应用，包括对称密码设计与分析、公钥密码设计与分析、安全协议设计与分析、侧信道分析与防护、量子密码与新型密码等。三是系统安全，包括芯片安全、系统软件安全、虚拟化计算平台安全、恶意代码分析与防护等。四是网络安全，包括通信基础设施及物理环境安全、互联网基础设施安全、网络安全管理、网络安全防护与主动防御（攻防与对抗）、端到端的安全通信等。五是应用安全，包括关键应用系统安全、社会网络安全（包括内容安全）、隐私保护、工控系统与物联网安全、先进计算安全等。

中国密码学会教育与科普工作委员会与电子工业出版社合作，共同筹划了这套“网络空间安全系列教材”，主要包括《密码学》、《密码学实验教程》、《公钥密码学》、《应用密码学》、《密码学数学基础》、《密码基础算法》、《典型密码算法 FPGA 实现》、《典型密码算法 JAVA 实现》、《公钥密码算法 C 语言实现》、《密码分析学》、《网络空间安全导论》、《信息安全管理》、《信息系统安全》、《网络空间安全技术》、《网络空间安全实验教程》、《网络攻防技术》、《同态密码学》、《对称密码学》等。希望为信息安全、网络空间安全、网络安全与执法、信息对抗技术等本科专业提供教材，也为密码学、网络空间安全、信息安全等专业的研究生和博士生，以及从事该领域的科研人员提供教材和参考书。为我国网络空间安全教材建设、普及密码知识和网络空间安全人才培养，贡献绵薄之力。

2016 年 12 月

前　言

随着通信和计算机技术的快速发展，各种新兴的网络应用层出不穷，安全问题越来越成为全社会关注的焦点，并成为制约网络应用发展的主要瓶颈之一。应用密码学作为实现网络信息安全的核心技术，在保障网络信息安全的应用中具有重要的意义。为了适应社会的需求，满足网络信息安全教育的发展需要，作者根据团队老师多年的教学和科研工作实践，在学习、总结众多国内外有关网络信息安全和应用密码学文献的基础上，针对社会研究人员和高校师生的需求完成了本书的撰写工作。

本书特点如下。

（1）理论与实践相结合。本书不但对密码学的基本理论和关键技术有系统而深入的介绍，而且还介绍了许多实用的热门案例，更适合于当前的国内现状。

（2）内容新颖成熟。本书不但对成熟的密码应用有深入的介绍，而且对许多国际前沿的应用进行了详细剖析。

（3）易教易用，合理适当。本书的编排从教学适用性出发，特别重视读者对应用密码学知识的系统理解；有针对性地重点讲述，在内容体系结构、语言表达、内容选取、实例及应用等方面都做了特别的考虑，易教易用。

（4）可读性强。本书在内容安排上力求层次清晰、结构合理、主次分明、重点突出，十分有助于读者在把握全局的同时，深入了解局部知识。本书在语言表达上力求通俗易懂、言简意赅、图文并茂，使读者可以很容易对相关内容产生深刻的理解。

（5）读者对象广泛。作为国内应用密码学方面不多的教材之一，本书的主要读者是通信、计算机、信息安全、密码学等相关专业的学生。但是，本书也可以广泛适用于从事信息处理、通信保密、计算机等领域的科研人员和工程技术人员等。

本书共12章，比较全面地介绍了应用密码学的基本概念、基本理论和典型实用技术。第1章密码学概述，介绍了密码学的基本概念、密码体制分类及密码学的发展史。第2章序列密码，介绍了伪随机序列的定义、序列密码基础概念、序列密码的设计与分析等，并对常用的序列密码算法进行了详细的分析。第3章分组密码，介绍了分组密码定义、经典的分组密码体制（DES、AES、SM4等算法）。第4章公钥密码，介绍了公钥密码的原理及相关基础知识、RSA算法、椭圆曲线密码ECC算法、基于身份的加密体制和基于属性的加密体制。第5章单向散列函数和消息认证，介绍了单向散列函数的定义，MD5、SHA－1、SM3算法，消息认证的定义与基础知识。第6章数字签名，介绍了数字签名的基本概念、RSA数字签名、离散对数签名体制、椭圆曲线签名体制及数字签名标准DSS，并以实例对数字签名应用进行了讲述。第7章身份认证与访问控制，介绍了常见的身份认证技术、访问控制原理以及访问控制策略和应用。第8章密钥管理，介绍了密钥的种类、生成、分配、协商、托管以及密钥分割，并以Internet密钥交换协议分析了密钥管理应用。第9章PKI技术，介绍了PKI

的概念、关键技术、相关标准，并介绍了 PMI、AAA 的概念与基础知识。第 10 章电子现金与电子支付系统，介绍了相关概念、安全支付协议和相关的应用案例。第 11 章安全电子选举系统，介绍了各种电子选举投票协议。第 12 章安全多方计算，介绍了安全多方计算定义与基础知识，一般安全多方计算协议，以及特殊安全多方计算及应用。

本书由河南理工大学汤永利、闫玺玺、叶青组织编写，并负责全书的统稿、修改及定编工作。具体编写分工如下：闫玺玺编写第 1 ~ 3 章，汤永利编写第 4 ~ 8 章，叶青编写第 9 ~ 12 章。另外，许多研究生也参与了部分资料的收集、整理和书稿的校对工作，在此对他们付出的辛勤劳动表示深深的感谢。

由于作者水平有限，书中难免出现各种错误和不当之处，望广大读者提出意见和建议。

编著者

目　录

第1章　密码学概述

1.1　密码学基础

密码学的主要任务是解决信息的保密性和可认证性问题，即保证信息在生成、传递、处理、保存等过程中，不能被未授权者非法地提取、篡改、删除、重放和伪造等。密码学本身也是一门正在迅速发展的综合性新学科。密码学所需要的知识横跨数学、物理、计算机、信息论、编码学、通信技术等多种学科。密码学是信息安全的核心，为解决信息安全问题提供了许多有效的核心技术，在保护信息的机密性、认证性等方面发挥着关键性的作用。

简单地说，密码学（Cryptology）是研究信息系统安全的一门科学。它主要包括两个分支，即密码编码学（Cryptography）和密码分析学（Cryptanalysis）。密码编码学是对信息进行编码实现隐蔽信息的一门学问，其主要目的是寻求保护信息保密性（Privacy）和认证性（Authentication）的方法。密码分析学是研究分析破译密码的学问，其主要目的是研究加密消息的破译或消息的伪造。密码编码学和密码分析学相互对立，而又互相促进地向前发展。

密码编码学的研究重点是算法，包括数据加密算法、数字签名算法、消息摘要算法及相应的密钥管理协议等。这些算法提供两方面的服务：一方面，直接对信息进行运算，保护信息的安全特性，即通过加密变换保护信息的机密性，通过消息摘要变换检测信息的完整性，通过数字签名保护信息的抗否认性；另一方面，提供对身份认证和安全协议等理论的支持。应用密码学的主要研究内容包括以下方面。

1. 数据加密（Data Encryption）

数据加密算法是一种数学变换，在选定参数（密钥）的参与下，将信息从易于理解的明文加密为不易理解的密文，同时也可以将密文解密为明文。加密、解密时用的密钥可以相同，也可以不同。加密、解密密钥相同的算法称为对称算法，典型的算法有 DES、AES 等；加密、解密密钥不同的算法称为非对称算法，通常一个密钥公开，另一个密钥私藏，因此也称为公钥算法，典型的算法有 RSA、ECC 等。

2. 消息摘要（Message Digest）

消息摘要算法也是一种数学变换，通常是单向（不可逆）的变换，它将不定长度的信息变换为固定长度（如 16 字节）的摘要，信息的任何改变（即使是 1bit）也能造成摘要面目全非，因此可以通过消息摘要检测消息是否被篡改。典型的算法有 MD5、SHA－1 等。

3. 数字签名（Data Signature）

数字签名主要是消息摘要和非对称加密算法的组合应用。从原理上讲，通过私有密钥用非对称算法对信息本身进行加密，即可实现数字签名功能。用私钥加密只能用公钥解密使得接收者可以解密信息，但无法生成用公钥解密的密文，从而证明此密文肯定是拥有加密私钥的用户生成的，因此是不可否认的。实际实现时，由于非对称算法加/解密速度很慢，通常

先计算消息摘要，再用非对称加密算法对消息摘要进行加密而获得数字签名。

4. 密钥管理（Key Management）

密码算法是可以公开的，但密钥必须严格保护。如果非授权用户获得加密算法和密钥，则很容易破解或伪造密文，加密也就失去了意义。密钥管理研究就是研究密钥的产生、发放、存储、更换和销毁的算法和协议等。

5. 身份认证（Authentication）

身份认证是指验证用户身份与其所声称的身份是否一致的过程。最常见的身份认证是口令认证。口令认证是在用户注册时记录下其用户名和口令，在用户请求服务时出示用户名和口令，通过比较其出示的用户名和口令与注册时记录下的是否一致来鉴别身份的真伪。复杂的身份认证则需要基于可信的第三方权威认证机构的保证和复杂的密码协议来支持，如基于证书认证中心（CA）和公钥算法的认证等。

身份认证研究的主要内容包括认证的特征（知识、推理、生物特征等）和认证的可信协议及模型。

6. 授权和访问控制（Authorization and Access Control）

授权和访问控制是两个关系密切的概念，常常替换使用。它们的细微区别在于，授权侧重于强调用户拥有什么样的访问权限，这种权限是系统预先设定的，并不关心用户是否发起访问请求；而访问控制是对用户访问行为进行控制，它将用户的访问行为控制在授权允许的范围之内，因此，也可以说，访问控制是在用户发起访问请求时才起作用的。打个形象的比喻，授权是签发通行证，访问控制则是卫兵，前者规定用户是否有权出入某个区域，而后者检查用户在出入时是否超越了禁区。

授权和访问控制研究的主要内容是授权策略、访问控制模型、大规模系统的快速访问控制算法等。

7. 审计追踪（Auditing and Tracing）

审计和追踪也是两个关系密切的概念，审计是指对用户的行为进行记录、分析和审查，以确认操作的历史行为。追踪则有追查的意思，通过审计结果追查用户的全程行踪。审计通常只在某个系统内进行，追踪则需要对多个系统的审计结果综合分析。

审计追踪研究的主要内容是审计素材的记录入式、审计模型及追踪算法等。

8. 安全协议（Security Protocol）

安全协议又称密码协议，是以密码学为基础的消息交换协议，其目的是在网络环境中提供各种安全服务。在安全协议中，经常使用对称密码、公开密钥密码、单向函数、伪随机数生成器等密码算法，换句话说，安全协议就是在消息处理环节采用了若干密码算法的协议。安全协议中使用密码算法的目的是防止、发现窃听和欺骗。安全协议运行在计算机网络或分布式系统中，为各方提供一系列步骤，借助于密码算法来实现密钥分配、身份认证及安全地完成电子交易。

1.2 密码体制

1.2.1 密码体制定义

密码学的基本思想是将一种形式的消息变换成另外一种形式的消息。因此，从某种意义