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

现代密码学概论

潘森杉 仲红 潘恒 王良民 编著

http://www.tup.com.cn

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

高等院校信息安全专业系列教材

现代密码学概论

潘森杉 仲红 潘恒 王良民 编著

Information Security

http://www.tup.com.cn

清华大学出版社
北京

内 容 简 介

本书旨在向从事网络空间安全的入门者介绍什么是现代密码学，它从哪里来；现代密码学包含哪些基本内容，在网络空间里有哪些应用。作为入门书籍，面向的主要读者对象是准备从事网络空间安全的研究者和计算类专业中对信息安全有兴趣的本科学生，为他们建立较为全面的密码知识体系视野、增加对密码学应用领域的了解。

本书从古代军事上的密码传递信息应用开始，分析密码的行程和密码技术的变迁；结合密码的发展与应用历史，穿插以历史故事，较为系统地介绍了 DES、AES、RSA 等经典密码算法，讨论了数字签名、密钥管理、秘密分享等经典密码协议，还介绍了椭圆曲线、量子密码等新兴密码技术，以及密码技术在电子货币与物联网应用等热点技术话题。

图书在版编目(CIP)数据

现代密码学概论/潘森杉等编著. —北京：清华大学出版社，2017
(高等院校信息安全专业系列教材)
ISBN 978-7-302-46147-0

Ⅰ. ①现… Ⅱ. ①潘… Ⅲ. ①密码学—高等学校—教材 Ⅳ. ①TN918.1

中国版本图书馆 CIP 数据核字(2017)第 013695 号

责任编辑：袁勤勇　李　晔
封面设计：常雪影
责任校对：白　蕾
责任印制：刘海龙

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**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
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：保定市中画美凯印刷有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：14.25　　**字　　数**：325 千字
版　　次：2017 年 5 月第 1 版　　**印　　次**：2017 年 5 月第1 次印刷
印　　数：1～2000
定　　价：35.00 元

产品编号：061265-01

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，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，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又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起到重要的指导和推动作用。2006年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时5年，制定出我国第一个信息安全专业指导性专业规范，于2012年年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013年，新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定，2014年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》（由清华大学出版社正式出版）。“高等院校信息安全专业系列教材”在教育部高等学校信息安全专业教学指导委员会的指导下，根据《高等学校信息安全专业指导性专业规范》组织编写和修订，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，并随着我国信息安全学科的发展不断完善。

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

“高等院校信息安全专业系列教材”编审委员会

前言

通常来说，大多数人都知道信息技术，甚至知晓一点信息安全和网络安全的新闻，但是并不知道密码学。信息技术的迅猛发展变革着人们的生活和工作方式，例如，相隔两地的亲人朋友更喜欢用手机视频聊天而不是打电话，快节奏的上班族更喜欢用手机软件订外卖而不是去餐馆，年轻人出门买东西更喜欢用手机支付而不是带钱或银行卡。信息技术的这些变化在使人们的生活更加便捷的同时，也面临着信息安全和网络安全问题，著名的新闻就有“棱镜门”事件，FBI 与苹果公司的诉讼事件等。然而，我们并不知道，这些事情和我们有什么关系，也不知道这些信息安全秘密的保护是通过一种密码技术实现的，更不知道那个密码是什么，是不是上网账号的那个“密码”？难道设置一个密码还需要通过一门课、一本书来“学”吗？

虽然我们都停留在“不知道”的阶段，但是密码技术和以密码技术为基础的信息与网络安全问题已经延伸到社会大众的广泛需求上来。更为重要的是，这些和我们生活融为一体的信息与网络，组成了一个完全新型的“网络空间”，这是一个和海、陆、空并列的第四空间，我们生活在这个新型的空间里，无可避免地依赖这个空间，并被它制约。我们从一系列事件来看看网络空间的重要性：2005 年 4 月，美国政府公布了总统 IT 咨询委员会向总统提交的《网络空间安全：迫在眉睫的危机》紧急报告；2009 年 5 月 29 日，奥巴马公布了名为《网络空间政策评估——保障可信和强健的信息和通信基础设施》的报告，并在其讲话中强调网络空间安全威胁是“美国面临的最严重的国家经济和国家安全挑战之一”；2009 年 6 月 23 日，美国宣布成立了网络空间司令部，并于 2010 年 5 月 21 日正式启动工作，同时公布了《网络空间国际战略》；2014 年 2 月，美国国家标准与技术研究所（NIST）提出了《美国增强关键基础设施网络安全框架》，指出目前世界上有 100 多个国家具有一定的网络作战能力，有 56 家公开发布了网络空间的安全战略。这说明，网络空间作为人类的行动空间，已经成为国家安全考虑的作战空间——一方面，可以通过网络行为，摧毁一个国家的政权；另一方面，网络空间的安全和领土、领空安全一样，成为国家安全的重要组成部分。所以，国家主席习近平同志亲自担任信息化与网络安全领导小组组长，确立了网络空间安全学科，这体现了我国对第四空间安全与自由的重视。

这些信息的枚举，让我们知道了网络空间安全原来这么重要。可是，我们依然不知道这一切和本书有什么关系，我们为什么要学习密码学。是因为

网络空间的信息安全往往需要用到密码技术来保护，而密码却不是记在我们大脑中的一串口令。什么是密码，密码背后的设计者是什么样的人，密码技术从哪里来，用到哪里去，它们是否和我们的日常生活有紧密关联，它们有什么样的技术瓶颈，它们会在多大程度上影响我们的生活？我们将在本书讲授密码技术的同时，穿插一些历史上的趣闻轶事，在提高可读性的同时介绍密码学的历史，引发读者对密码技术的思考，从而提高学习的兴趣。其实，关于密码学的教科书已经有很多了，这些“教材”往往以其专业的密码技术和严密的数学基础让人望而却步，甚至于信息安全专业的本科生看了都嫌枯燥，如果一本教材只提供给那些对数学和密码技术本身有浓厚兴趣和天分的人，那么这个教材还是不是教材呢？编者认为，一本入门级别的好的密码学教材，尤其是《现代密码学概论》这样的书，不仅要系统地介绍密码学的框架和应用，给读者以概貌；还要引导读者去认识生活中的密码问题和密码技术，譬如：

- 密码是什么，和我关系很大吗？是不是我们网上购物时，用到的用户名和登录口令，我们常常称呼这个口令为密码，而且当这个口令被他人截获时，我们就认为“我的密码丢了”。在本书中，我们将告诉大家口令(password)并非密码，也不是密钥，但是我们登录网络账户的时候，密码技术的确在幕后默默地保护着我们的隐私。除此之外，本书在介绍密码技术无处不在的同时，也将教会你如何让网易邮箱查看不了你所收发的邮件，以及如何验证你在网上下载的 Windows 10 系统安装文件是否完整有效，把高深的密码学和日常的生活关联起来。让读者认识到，密码技术提供的安全无处不在，在介绍复杂枯燥的数学方法时，给出一些日常生活的应用场景，这是本书的一个特点。
- 一些我们未曾关注到的安全问题，例如网上流传的照片上，脸书(Facebook)的 CEO Mark Zuckerberg 用胶带封住了摄像头和麦克风，他为什么要这么做？如果我们说这是基于信息安全的考虑，您会不会觉得奇怪？现代的信息技术已经能够让我们“刷脸”签名、声音签名了，简单的例子是，你一定在纸质合同或协议上署过名吧，签名能不能被复制和模仿呢？在电子世界里也是如此，本书将教你如何防范自己的签名被他人利用，以致造成权益损失。本书以这些签名技术所使用的密码技术为背景，诠释了 QQ 登录口令、支付宝口令等，如何设置才安全，以及这样设置的理由。甚至，我们还讨论了如何安全地从银行或 ATM 上大额取款。我们不能说读完本书，读者将披上一身安全的铠甲，让骗子无法得逞；但是我们能让读者在读完本书之后，对安全问题有初步的理性认识。
- 新型计算技术、网络安全事件，譬如量子计算机和量子密码离我们还有多远，据说加拿大 D-Wave 公司研发出了量子计算机，在这样超强的计算能力面前，传统的密码技术还能保护我们的安全吗？又如，美国 560 万指纹被盗、微软操作系统的“心脏出血”、孟加拉国银行打印机被黑客控制导致 1 亿美元被窃……这些事件是怎么回事？为什么神奇的密码学没有防住？如何才能将无孔不入的黑客拒之门外？

当我们在前言部分如此叙述的时候，可能会误导读者对本书定位的思考，然而，编者需要声明的是：本书并不是一本安全技术的实用手册，我们仅仅是在介绍密码技术的时

候，顺便提到它有这些应用；本书也不是密码学历史和应用的科普论文，我们介绍了详细的算法、具体的推演甚至还有一部分严格的证明；这是一本适用于计算类专业（包含计算机科学与技术、软件工程、网络工程、物联网工程和一些以工程应用人才为培养目标的信息安全专业）学生了解信息安全知识的密码学入门教材。密码学与信息安全密不可分，其方向涉及数学、计算机、通信、物理和生物等领域。交叉学科和专业课——这个双重性决定了想要精通这门课程是较困难的。所以，我们面向的读者群体是那些对信息安全有兴趣却不痴迷于数论和算法，他们希望获得一本通俗易懂的教材让他知道密码学是什么，可以用在哪里，并且如果这些基本的知识能够激发他的学习兴趣，还可以在这本书里进行一些初步推导和演算。在以后的工程应用或者理论中，如果需要更深的密码技术和更专门的理论体系，本书则无法提供，只能引导读者去寻找更为专业的著作。作为一本入门级别的教材，本书有以下三个特点：

（1）知识全面，体系合理。书中涵盖了密码学的基本概念、算法和协议，并加入了必要的数学知识，也就是当您读到某一部分需要数学基础的时候，不用去图书馆借阅，也不用翻阅某个特定的“数学基础”书，您马上就能看到相关的基础知识。

（2）技术深入，介绍浅显。作者用浅显的图形、例子和故事，甚至并不严密的对比分析等来描述部分知识，尽可能给读者建立形象的技术概貌。对于有兴趣的读者愿意深入钻研的基础问题，例如 DES、AES 算法，作者列出了详细的加解密过程。

（3）话题模式、内容趣味性强。在知识点的学习过程中穿插了相关人物故事的介绍，并给出了实用的例子，在讲解枯燥的专业知识的同时，提供一些趣味的话题，可以用来向自己的家人、甚至文科的朋友讲解，去展示自己专业的神奇，并从中获得学习的乐趣。

全书是按照密码的演化史来展开的，共分 10 章，涉及密码算法、安全协议、安全应用等内容。在本书的撰写过程中，潘森杉博士负责了全书的统稿与编辑，使得写法风格一致，并完成了第 7～10 章的编写；潘恒博士参与了第 1、2、5、6 章的编写；王良民教授和笔者共同讨论，确定了文章的框架，审阅了全书，并组织安徽大学的研究生杨树雪、张庆阳、吴海云、刘亚伟、谢晴晴、徐文龙、李从东等搜集了材料、提供了教材编写的基本素材，完成了第 1～6 章的编写工作。本书各章节的内容安排如下：

第 1 章介绍了密码学的基本模型和概念，用实际的例子来说明密码是日常生活不可或缺的组成部分。

第 2 章讲述了古代人是如何凭借着其聪明才智进行保密通信和密码破译的，其间往往还伴有惊心动魄的故事。这部分内容涵盖单表替换、多表替换、分组密码、一次一密以及伪随机数的生成。

第 3 章详细描述了 DES 这个经典密码方案，虽然其安全强度已不能满足要求，但它的设计思想是值得学习的。

第 4 章介绍了 DES 的继任者——AES，这是密码学研究者的必学方案。

第 5 章解释了最著名的公钥密码方案——RSA 公钥密码方案，同时解释了公钥方案是如何解决古典密码与对称密码所遇到的密钥分配难题的。

第 6 章介绍了公钥密码的另一个作用是实现数字签名，并且除了基于大整数分解的 RSA 方案，还介绍了基于离散对数问题的公钥密码方案——ElGamal。

第7章从密码学的角度讲述如何生成密钥并进行密钥维护，内容可能和现实生活中我们可能要记住多个口令（例如各种银行卡、网络账户、手机账户等）这个头疼的问题关联。

第8章告诉我们如何把“鸡蛋”（秘密）放在不同的“篮子”里，如何能够让强盗相信你有保险柜的密码并能保住你性命等问题，从而引出密码协议中的一些重要话题。

第9章把读者领入这些密码学“新”技术的大门，介绍了椭圆曲线、双线性对、群签名、量子密码等名词概念，读者或许是第一次看到它们，但它们其实已经发展了相当一段时间并且其中一些已经是成熟的技术，

第10章讲述密码具有丰富的应用：电子商务、比特币和物联网等。

需要特别感谢的是“安徽省高等教育振兴计划-信息安全新专业建设”项目（编号2013zytz008）、“江苏省推荐国家级综合改革试点项目”和江苏大学教学改革重点项目（编号2011JGZD012）的资助，是这些教学建设和研究类项目，让我们有动力和耐力完成了全书长达四年的编撰工作。此外，作为编写的教材，本书除整体安排和语言组织之外，所包含技术内容，都非编者原创，均来自书本材料和网络搜集。我们尽力标注出所引用的出处，但是一方面由于文献的交叉引用，我们很难找到原始发布者；另一方面为了教材的可读性，我们不能做到类似科技论文和专业著作那样对每一句的来源都严格论证引用。如果未能对所借鉴的资料标注出处，敬请原作者和读者谅解并不吝指教。编者将在后续版本中更正并给出相应的说明。

仲　红

2016年12月

目录

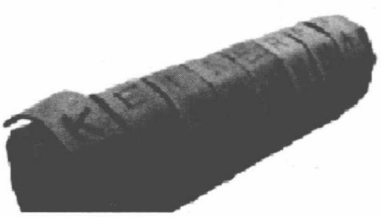
第1章 密码学基础模型与概念

1.1 密码学基本概念

1.1.1 Scytale 密码棒

美国情报专家戴维·卡恩(David Kahn)的著作《破译者》中有一句广为流传的话:“人类使用密码的历史几乎和使用文字的时间一样长。”当人类开始研究通信技术的时候就开始研究如何能确保通信信息的保密。本书第一个引例讲述的是公元前的古希腊人,他们使用一种名为 Scytale 的密码棒对信息进行加密,把加密了的信息,写在羊皮带子上,通过危险的区,传达军事情报。

如下图所示,Scytale 密码棒将用来书写信息的羊皮条螺旋状裹在密码棒上,然后将想传送的**消息**(**message**)写好之后取下羊皮条卷,通过其他公开的非保密的渠道将信送给收信人。对任何一个拿到羊皮卷的人,若不知道密码棒的直径,就很难将羊皮条上的内容解读出来。在远古时代,这种使用密码棒的方法和密码棒的直径都称为加密方法有效性的原则。



缠绕在棒子上书写的有意义的消息称为**明文**(**plaintext**)或原文,明文是信息传送过程中需要保密的信息;而从棒子上揭下来一条羊皮带子上所写的没有明确意义的乱码的称为**密文**(**ciphertext**)。这种通过密码棒将明文变成密文的过程,称为**加密**(**encryption**);而收信人通过密码棒将密文乱码变成有意义的明文,这个过程称为**解密**(**decryption**)。在这个过程中,密码棒或者说密码棒的直径是问题的关键所在,称为**密钥**(**key**)。

> **揭暄**
>
> 明末清初著名军事理论家,他在《兵经百言》中用一百个字条系统阐述了古代军事理论,其中“传”字诀是古代军队通信方法的总结。
>
> 原文:军行无通法,则分者不能合,远者不能应。彼此莫相喻,败道也。然通而不密,反为敌算。故自金、旌、炮、马、令箭、起火、烽烟,报警急外;两军相遇,当诘暗号;千里而遥,宜用素书,为不成字、无形文、非纸简。传者不知,获者无迹,神乎神乎!

1.1.2 保密通信模型

以上述例子为背景，我们继续假想，在远古的希腊时代，一个部族 A 要穿越几个敌方管理的区域，把自己发动攻击的时间和对象送达给他的盟友 B。于是，他通过民间的商道传送信息，这个商道是通信的**公开信道**，公开信道大家都可以使用，而且敌方甚至可以控制这个信道。现在问题的关键是，A 不仅要将密文送达给 B，还要把密码棒送给 B，否则 B 仅仅拿到了一堆乱码。我们不管 A 和 B 是如何事先约定使用密码棒的方法和密码棒的直径，而是统一地将其称为**秘密信道**。这样，在这个公元前的例子中，就已经有了图 1-1 所示的保密通信模型。

在图 1-1 所示的保密通信模型中，出现了密码学中常见的三个人物：Alice，协议的发起者；Bob，协议的应答者；Eve，窃听者和可能的攻击者。密文 c 在公开的信道上传送，而密钥 k 在一个秘密的安全信道传送。Eve 是公开信道上的一个不可信的第三方，根据 Eve 的恶意程度，在密码学书籍中，往往用不同的称呼来代表，例如，Oscar，被动的观察者，仅仅根据从公开信道获得的资料进行破译；Malice 或者 Mallory，主动的攻击者，可能会拦截数据、篡改信息、冒充合法的通信者。

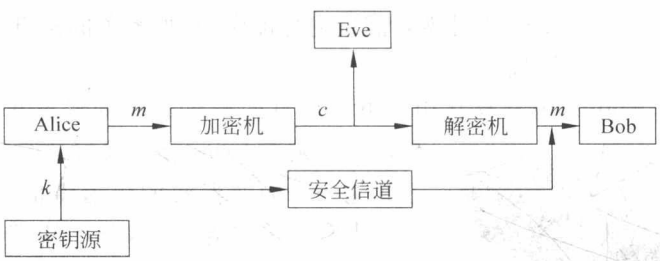


图 1-1 保密通信模型

通过图 1-1 的保密通信模型，可以很清楚地表明密码学的作用：就是保证 Alice 和 Bob 能在公开的信道上通信，而窃听者、攻击者 Eve 不能理解他们通信的内容。

1.1.3 攻击者的能力

在图 1-1 所示的保密通信模型中，存在一个攻击者 Eve，Eve 通常可以采取如下几种攻击手段：

A. 搭线窃听，读取 Alice 发送 Bob 的消息；

B. 被动破译，试图寻找密钥并读取用该密钥加密的消息；

C. 中断通信，从公开信道阻拦从 Alice 发送给 Bob 的消息；

D. 篡改消息，拦截 Alice 发送给 Bob 的消息 m，并用一个伪造的消息 m′替代 m；

E. 伪造通信，伪装成 Alice 发送消息 m 给 Bob，让 Bob 误以为是在和 Alice 通信。

图 1-2 给出了上述五种攻击的图示描述，其中 A、B 两种攻击属于被动攻击，通常用 Oscar 表示，而 C、D 和 E 属于主动攻击，通常用 Malice 表示。一般来说，被动攻击难以被