信息安全系列丛书

Cryptographic Protocols

密码协议基础

邱卫东　黄　征　李祥学　郭　捷　编著

陈克非　审

高等教育出版社

信息安全系列丛书

Cryptographic Protocols

密码协议基础

邱卫东　黄　征　李祥学　郭　捷　编著
陈克非　审

高等教育出版社

内容简介

本书较为全面、深入地介绍了信息安全体系中的基础密码协议、高级密码协议及应用密码协议，按照由浅入深的原则，将全书分为13章，内容包括三大部分：基础密码协议、高级密码协议及应用密码协议。基础密码协议由引论、密钥协商、实体认证、比特承诺协议组成；高级密码协议部分包括高级签名协议、零知识、不经意传输、秘密分享和门限密码、安全多方计算协议；应用密码协议部分包括Kerberos协议、IKE密钥管理协议、电子现金及无线安全通信。

本书对各类密码协议及其相关应用进行了详细的论述和分析，可作为高校计算机、信息安全、电子信息与通信、信息与计算科学等专业高年级本科生和研究生的教学参考书，也可作为相关工程技术人员学习信息安全知识的入门读物。通过阅读本书，读者不仅能够全面熟悉和了解各类密码协议的设计理念和安全机制，还可以提高密码及相关安全协议的独立设计和分析能力。

图书在版编目(CIP)数据

密码协议基础／邱卫东等编著．—北京：高等教育出版社，2008.11
（信息安全系列丛书）
ISBN 978-7-04-025154-8

Ⅰ.密… Ⅱ.邱… Ⅲ.密码—理论 Ⅳ.TN918.1

中国版本图书馆CIP数据核字（2008）第162364号

策划编辑 陈红英 **责任编辑** 陈红英 **封面设计** 刘晓翔 **版式设计** 陆瑞红
责任校对 刘 莉 **责任印制** 韩 刚

出版发行	高等教育出版社	**购书热线**	010－58581118
社 址	北京市西城区德外大街4号	**免费咨询**	800－810－0598
邮政编码	100120	**网 址**	http://www.hep.edu.cn
总 机	010－58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	北京民族印务有限责任公司	**畅想教育**	http://www.widedu.com
开 本	787×1092 1/16	**版 次**	2009年1月第1版
印 张	17	**印 次**	2009年1月第1次印刷
字 数	320 000	**定 价**	28.00元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

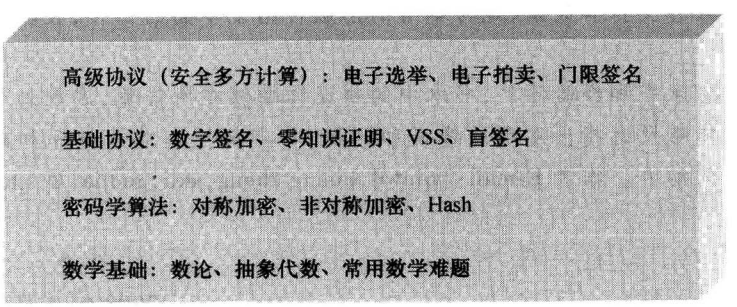
物料号 25154-00

前言

随着我国信息化进展的日益加速，信息安全得到了各个领域和行业的广泛重视。虽然我国的信息安全起步较晚，但近十五年在各个方面都取得了长足的进步，对信息安全的理解也再不局限于加、解密这样狭隘的层面上。各高等院校为国家培养了大量的信息安全专业人才，并涌现了一大批具有自主开发能力的信息安全方面的企业。

笔者在信息安全领域有着近10年的研究和教学的经历，对信息安全的内涵有着较深的理解。目前，企业界对于信息安全的认识存在一定的缺陷，易将信息安全与网络安全划等号，对于各类算法、协议的认知也不够深入，只是简单地将国家商业密码管理委员会制定的标准实现作为目标。而往往由于缺乏对密码算法、协议的深入了解，无法对算法、协议进行优化实现，安全系统在速度和效率方面存在瓶颈的现象屡见不鲜，对于设计实现新的算法、协议方面更是无能为力。这将严重阻碍我国信息安全产业自主化的进程。

在人才培养方面，国内各高等院校都加强了信息安全专业本科和研究生的培养力度，开设了相关的信息安全专业，进行了详细的课程设计。一般来讲，协议、密码算法和底层的数学基础有如下关系：



目前高等院校的大部分教材均以信息安全数学基础或现代密码学作为主要讲述内容，往往忽视了密码协议尤其是高级密码协议的设计和分析，对于密码协议这方面的内容也只作非常简单的介绍，这对于人才的培养来讲是非常不利的。

笔者自2004年加入上海交通大学信息安全工程学院以来，将“密码协议基础”作为研究生的专业课程引入到研究生的培养计划中，并将此课程作为高年级本科

生的选修课程。从授课的效果来看,学生反映良好。在该课程教学材料的基础上,作者综合了已有的研究成果,通过对密码协议设计和分析的介绍,对各类基础密码、高级密码和应用密码协议进行了论述,尤其是通过安全分析、设计范例等手段,使得读者不仅可以了解各类密码协议的详细步骤,更为重要的是通过这些分析和范例,使得读者能够理解各类密码协议的设计理念和设计思路,从而能够进一步分析和自行设计新型的高级密码和应用安全协议,增强自主创新能力。作者也希望该书能够为工程技术人员提供更全面的参考,使得安全业界的工程技术人员能够更深入地了解各类算法、协议的设计思路和机理,并提升他们在算法、协议的优化实现方面的能力。

全书共分13章,内容包括引论、密钥交换协议、实体认证协议、比特承诺、高级签名协议、零知识证明、不经意传输协议、秘密分享与门限密码学、安全多方计算、Kerberos协议、IKE协议、电子现金、无线网络通信安全协议。

为了顺利地学习本书,学习前读者应有信息安全数学基础、近世代数、基础数论、现代密码学、计算机网络和操作系统方面的知识。本书是按照基础密码协议、高级密码协议和应用密码协议的顺序撰写的,虽然各章内容有一定的独立性,但仍然建议按照章节顺序阅读。

本书可作为计算机、信息安全、电子信息与通信和信息管理等专业高年级本科生和研究生教材,也可作为相关工程技术人员学习信息安全知识的入门读物。

本书由邱卫东主持编写,各章内容主要基于邱卫东的“密码算法与协议”课程的教学讲义,其中第6、11、12章由邱卫东执笔,第1、4、9、13章由黄征执笔,第2、3、5、8章的初稿由李祥学执笔,第7、10章的初稿由郭捷执笔。邱卫东对全书进行了统稿,陈克非教授对全书进行了详细的审阅,龚征博士通读了全书,并提出了许多修改意见,在此表示感谢!在本书选题策划和撰写过程中得到了高等教育出版社的陈红英的大力支持和鼓励,她为本书的出版付出了辛勤的工作,在此表示最真诚的感谢!

限于作者水平和经验不足,书本中的错误和缺憾在所难免,诚恳地希望读者在使用本书时能够及时指出发现的错误和问题,作者将把有益的批评和建议作为今后本书修订的动力。作者E-mail:{qiuwd,huang-zheng,xxli,guojie}@sjtu.edu.cn。

作者

2008年9月

于上海交通大学信息安全工程学院

目录

第1章　引论

密码协议在信息安全实践中有着非常重要的应用。本章将首先介绍密码协议的基本概念，简单评述现有密码协议分析的基本方法，然后给出一个常用密码协议的例子，以使读者对密码协议的基本概念和密码协议的安全性分析有更直观的理解。

1.1　密码协议基础

从最基本的密钥共享、密钥分发到电子商务与电子政务领域中的各种应用（如电子现金、电子公文传输、电子选举等）都离不开密码协议。密码协议的设计是否科学，密封协议的分析是否完备，是信息安全领域的研究和技术人员始终要考虑的问题。这些问题直接关系到密码协议的应用安全及合理效率。

1.1.1　密码协议的基本概念

协议（protocol）是日常生活中经常使用的一个概念。人们经常碰到的协议，如劳动协议、就业协议等，是指协议的参与者为了达到某种目的而对每个参与者作出的行为约束。计算机通信领域里广泛使用协议的概念，这里的协议往往是指协议中两个或者两个以上的参与者为了达到特定的目的而采取的一系列步骤[1]。例如TCP/IP通信协议中的握手协议等。协议的概念包含了以下几层含义：

（1）协议规定了一系列有序执行的步骤，必须依次执行。

（2）协议中有两个或者两个以上的参与者。一个参与者是不能构成协议的。

（3）协议都有明确的目的，即需要完成什么目标、防范什么风险等。

例如一个简单的两人分苹果协议：有两个协议的参与者A和B，只有一个苹果，需要A和B执行一个协议，将苹果在两个参与者中公平地分成两份，A和B各取一份。一个著名的公平分苹果方法是“一个人切，另一个人先取”。按照这样的思想设计的协议如下：

（1）A将苹果切为两份。

（2）B选择其中的一份作为自己应得。

（3）A取剩下的一份作为自己应得。

这个简单的协议中有两个参与者,他们通过执行上述一系列的步骤达到一个目的:将一个苹果在两个参与者中公平分配。

密码协议(cryptographic protocol)也是一种协议。密码协议因为需要使用一些基本的密码算法(如对称加密、公钥加密和安全散列算法)作为构造协议的基本模块(building block),并满足一定的安全需求,密码协议由此而得名。不过没有一个严格的界限来区分密码协议和一般的协议,有一些密码协议并没有使用密码算法,如线性秘密分享、安全多方计算协议等,但是研究者还是习惯将这些协议都归入密码协议的范畴。密码协议与基本密码算法的关系由图1.1所示。

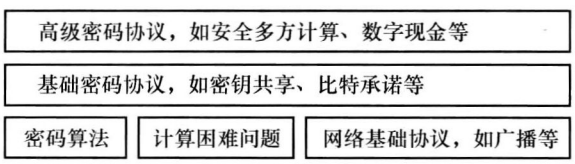


图1.1 密码协议与基本密码算法的关系

1.1.2 密码协议的特点

人们经常为了保护重要、敏感的数据而执行密码协议,这使得对密码协议的攻击成为一个非常有利可图的活动。在网络环境中执行的协议会面临各种窃听、篡改的攻击,甚至协议的参与者也会有某些恶意的企图希望能从协议执行中获得额外的好处。一般协议的设计只需要分析协议执行的正确性以及协议执行的效率。密码协议的设计和一般协议相比除了有正确性和执行效率的要求外,还有以下一些特殊要求:

(1) 安全需求 基本的安全需求包括加密、认证和不可抵赖性。加密保证密码协议执行过程中所涉及的敏感数据不能为非授权者所知;认证可以保证协议参与者的合法身份;不可抵赖性可以保证协议执行过程是可以稽查的,这对于有仲裁者(可信第三方)参与的密码协议是很关键的。

(2) 鲁棒性 并不是所有密码协议的参与者都是按照协议的要求来执行协议的,其中可能有恶意参与者。恶意参与者可以通过不按照协议要求执行或者向协议输入非法数据等方法来破坏协议的执行过程,从而达到阻止协议执行或者获取额外信息的目的。鲁棒性要求密码协议在有恶意参与者的情况下能部分地正确执行,同时严格保护其他诚实参与者所持有的秘密信息。

恶意参与者的存在是密码协议和一般通信协议之间的重要区别,这也使得密码协议的设计和分析变得比较困难。

1.1.3 密码协议的分类

通常根据协议对可信第三方的依赖程度可以将密码协议分为如下几类[2]:

(1) 仲裁协议 仲裁者就是可信第三方,协议需要可信第三方的帮助才能正确执行。可信第三方的存在可以使密码协议高效执行。仲裁协议的问题是现实的计算机网络中很难找到一个协议参与者都信任的仲裁者,并且如果网络中参与者都信任仲裁者的话,仲裁者容易成为易受攻击之处。

(2) 裁决协议 裁决者也是可信第三方,但是裁决者并不直接参与协议的执行。裁决者只是在有争议的时候才参与协议的执行。这样协议对可信第三方的依赖程度降低了。

(3) 自动执行协议(Self-enforcing Protocol) 最理想的协议,协议本身体现了公平性,不需要可信第三方的参与,当某个参与者实施欺骗行为时能够被其他参与者发觉,从而终止协议或者将欺骗者排除。

1.2 密码协议模型

密码协议的设计和分析都必须在一定的条件和假设下进行,例如协议参与者的个数、协议参与者的诚实程度、协议参与者之间的网络连接情况等。所有的这些条件和假设构成了密码协议的模型(Model),换句话说,密码协议的模型描述了密码协议的运行环境。所以在设计和分析密码协议之前,首先需要清楚地描述密码协议模型。通常人们从三个方面来描述密码协议模型,这三个方面分别是协议参与者的类型、参与者之间的网络连接情况和协议攻击者的能力(见图 1.2)。

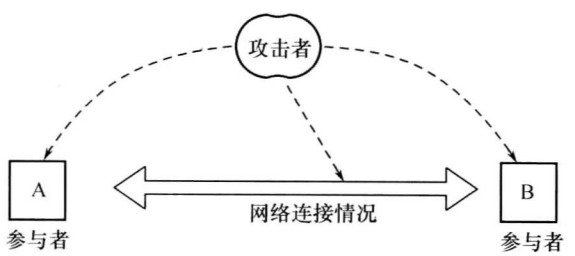


图 1.2 安全模型的要素

1.2.1 协议参与者角色类型

密码协议的执行过程中有多种多样的角色存在,依据角色的不同,可以将参与密码协议的主体分为协议参与者、协议攻击者、可信第三方(Trusted Third Party)、仲裁者(Arbiter)。

(1) 协议参与者 参与者按照协议的要求参与协议的执行,向协议提供输入,从协议中获得输出。

(2) 协议攻击者 密码协议的执行一般是在网络环境中,所以除了协议本身需要的参与者之外,还会有一些“参与者”通过窃听或者篡改报文等方法“主动”参