HZ BOOKS

IP网络技术丛书

IPSec 新一代因特网安全标准

IPSec: the new security standard for the Internet, intranets, and virtual private networks

（美）Naganand Doraswamy, Dan Harkins 著

京京工作室 译

机械工业出版社
China Machine Press

Prentice Hall PTR

IP网络技术丛书

IPSec——新一代因特网安全标准

(美) Naganand Doraswamy 著
Dan Harkins
京京工作室译

机械工业出版社
China Machine Press

本书系统地介绍了计算机与网络安全的基本原理，讨论了在IP堆栈的每一层实施安全保障的策略。介绍了IPSec的结构和组件；身份验证和保密性机制；验证头和封装安全载荷的用法；VPN通道传输以及Internet密钥交换(IKE)。最后，本书展望了IPSec的未来，包括最新的压缩、多点传送、机动运算和PKIX技术。

本书是一本既权威又全面的IPSec指南，无论你是网络或Web专家、软件开发者、还是安全专家，都必须掌握IPSec——而通过本书，你可以做到！

本书版权登记号：图字：01-1999-2861

图书在版编目(CIP)数据

IPSec: 新一代因特网安全标准/（美）多勒斯瓦米（Doraswamy, N.），（美）哈尔肯斯（Harkins, D.）著；京京工作室译. - 北京：机械工业出版社，2000. 1

（IP网络技术丛书）

书名原文：IPSec: The New Security Standard for the Internet, Intranet, and Virtual Private Networks

ISBN 7-111-07710-5

Ⅰ.I... Ⅱ.①多...②哈...③京...Ⅲ. 因特网 - 传输控制协议 Ⅳ.TP393.4

中国版本图书馆CIP数据核字 (1999) 第54142号

机械工业出版社 (北京市西城区百万庄大街 22号 邮政编码 100037)

责任编辑：陈贤舜

北京市密云县印刷厂印刷 · 新华书店北京发行所发行

2000 年 1 月第 1 版 · 2000 年 3 月第 2 次印刷

787mm × 1092mm 1/16 · 8.5印张

印数：6 001- 9 000 册

定价：20.00元

译 者 序

随着Internet网在全世界的普及，数以千百万计的人可以实时通信，并能访问几乎没有限制的信息。在Internet中，任何东西都可通过IP传输。如何保障IP传输的安全性就是一个很大的问题。IPSec是一种协议套件，可以“无缝”地为IP引入安全特性，并为数据源提供身份验证、数据完整性检查以及机密性保证机制，可以防范数据受到来历不明的攻击。

凭借IPSec，Internet的安全体系将迈入一个新时代。各大公司可开始构建自己的VPN和其他以Internet为中心的、面向任务的应用，同时保证自己的数据具有高度的安全性。在此，我们向大家推荐这本既权威又全面的IPSec指南——由IPSec标准化和IP安全研究的两位专家亲笔撰写。

本书讨论了IPSec的结构、设计、实施以及用法。对套件内的每一种协议都进行了详细讨论，同时讨论的还有IPSec的常规配置以及未来怎样对有问题的地方加以调节。

本书面向那些对网络安全有兴趣，而且打算通过IPSec实施安全方案的读者。在本书中，还介绍了数据加密和连网的基本知识，以便为初学者打好基础。

因译者水平和时间所限，书中难免有错误之处，敬请广大读者指正。

京京工作室

1999.10

作者简介

Naganand Doraswamy——Nortel Networks公司的资深首席工程师，IETF、VPN和IP安全密钥工作小组一名异常活跃的成员。他同时是Bay Networks（目前是 Nortel Networks）的一名网络安全总工，目前正致力于下一代路由器体系和协议的开发。他也是FTP Software的IP Security领导人。

Dan Harkins——Network Alchemy的一名资深研究员，致力于高性能和容错路由器的安全协议的开发。他以前曾是Cisco Systems公司的“网络协议安全部”的一名软件工程师。IPSec的标准“Internet密钥交换（IKE）”协议便是由他编写的。目前是几个IETF工作组的活跃成员，并服务于美国商业部的“技术咨询委员会”，负责联邦政府的“密钥管理架构”的开发。

前　言

Internet连接着全世界数以千百万计的人。人们可以实时通信，并能访问几乎没有限制的信息。数据、影像，你想象得到的几乎任何一种通信，每分每秒都在Internet上进行着。其中有些通信是“私用”性质的。

Internet采用的“语言”是IP，亦即“互联网协议（Internet Protocol）”。任何东西都可通过IP传输。然而，也有一样东西是IP不曾提供的，那就是安全（Security）。在路由过程中，IP包可被伪造、篡改或者窥视。IPSec是一种协议套件，可以“无缝”地为IP引入安全特性，并为数据源提供身份验证、数据完整性检查以及机密性保证机制，可以防范数据受到来历不明的攻击。

以IPSec的强大能力为基础，Internet可发挥出它所有的潜力：

- 通信是商务的根源。如果不能保证客户的订单真实可信，那么很难为自己的服务收费。如果不能确保机密信息的机密，就不可能将自己的生意做大，伙伴关系也很难建立。
- 除非能担保记录和信息保持机密，否则不能利用Internet拓展自己的服务，同时降低成本。
- 对一些个人服务来说，比如家庭记帐、证券交易以及保险业等，如果能保障这些交易安全进行，便能得到极大的简化和扩展。

Internet要继续发展，安全是一项重要的前提。而目前适用于所有Internet通信的唯一一种安全技术就是IPSec。IPSec除适用于IP目前的版本（IPv4）以外，也适用于下一代的IP——IPv6。除此以外，IPSec可为运行于IP顶部的任何一种协议提供保护，比如TCP、UDP和ICMP等等。IPSec是目前最易于扩展、最完整的一种网络安全方案。

IPSec使“端到端”的数据保密成为可能，换言之，进入或发出一台计算机的任何信息都可确保其安全。亦可在网络内部实施IPSec，构成一个“虚拟专用网络（Virtual Private Network，VPN）”。在这种网络中，两个全然不同的网络被整合成一个，连接它们的是一条由IPSec提供安全保卫的“通道（Tunnel）”。

本书讨论了IPSec的结构、设计、实施以及用法。套件内的每一种协议通常都统称为“IPSec”（验证头、封装安全载荷以及Internet密钥交换），我们会对其进行详细讨论。同时讨论的还有IPSec的常规配置，以及未来怎样对有问题的地方加以调节。

本书面向那些对网络安全有兴趣，而且打算通过IPSec实施安全方案的读者。这些安全方案包括构建VPN、电子商务以及端到端保密通信等等。在本书的开头，将介绍数据加密和连网的基本知识，为那些既非加密专家，亦非网络专家的人打好基础。

本书的结构

本书分为3部分：概论、详细分析以及实施和配置问题。

第1部分由3章构成。第1章讨论的是IPSec的加密技术基础，解释了用于加密和身份验证的对称及公共密钥加密。第2章介绍了TCP/IP的基本知识，以及在TCP/IP协议堆栈的各层实施

安全措施的优缺点。第3章是对IPSec的一个综述，讨论了IPSec的基本架构，以及其中包含的每种协议——AH、ESP和IKE，并提醒大家注意各协议间的联系。

第2部分包括第4～第7章。其中，第4章对IPSec的结构进行了详尽说明。IPSec的基本概念、不同的模式、选择符、安全联盟以及安全策略均在讨论之列。第5和第6章详细讨论了用来保护IP的两种协议：封装安全载荷（ESP）和验证头（AH）。针对协议头的构建和布置，我们介绍了包的进入及外出处理规则。第7章对Internet密钥交换进行了深入讨论。同时讲述的还有各个不同的协商阶段，各种交换措施，各种验证方法，以及可供协商的选项等等。

第3部分由第8～第11章构成。第8章对策略以及它对IPSec的意义进行了讨论。这里展示了一个支持IPSec策略的体系，以及一个策略模块。第9章总结了在一个TCP/IP堆栈上实施IPSec时（采取“与平台无关”的方式），可能会遇到的一些问题。第10章讨论了各种不同的IPSec配置方式：端到端安全、虚拟专用网络以及“公路战士”情况。第11章展望了IPSec将来的发展，其中包括网络层压缩同IPSec的集成、将IPSec扩展到“多点传送”（多播）通信、与密钥恢复有关的问题、IPSec与第2层通道传输协议（L2TP）间的沟通以及公共密钥体系等等。

网络图例

在本书描绘的网络示意图中，虚线代表逻辑连接（比如两个设备并不物理性地连接）；实线代表物理性连接（比如两个设备间的物理性链路，而且它们是直连的）；而一条较粗的管道则意味着两个设备间建立了安全连接通道。

目　录

第三部分 配置问题

第一部分 概 论

第1章 加密历史与技术

恐怕从一开始，人就具备了保守秘密的本能。想想看，自你有记忆开始，是不是就已开始做这样的事情？这是一种很自然的人类行为。人们总是有、而且一直都有一些秘密。这些秘密要么只能由自己掌握，要么由自己和自己允许的人掌握。要想保密，最简单的做法就是不把它告诉别人。知道“秘密”的人越多，泄秘的可能性越大，最后秘密将不成其为秘密。

1.1 加密历史

在古代，保守一项秘密似乎要容易一些，因为只有少数人才有读书、写字的特权。如果一项秘密是书写下来的，那么只有数量极少的人才知道它是什么意思。通过限制人们学习书写文字，便可做到保密。然而，这种保密机制显然具有很大的局限性。

随着越来越多的人掌握了读写文字的能力，越来越有必要在这些人中间保守秘密。这种需要在战争期间愈发迫切。尽管真正打仗的人可能大多数都是文盲，但那些发动战争的小丑却并非如此。而且战争双方无疑都会雇佣一些能够读写敌方语言的士兵。想来，古代战场上的军队通信或许就是加密术的起源吧！

早期的加密方法非常简单。据说凯撒大帝曾用一种初级的密码来弄乱他传达的消息。对那些他认为能够分享秘密的人，便告诉他们如何重新组合回原来的消息。这种密码便是著名的“凯撒密码（The Caesar Cipher）”。它其实是一种简单的替换加密法：字母表中的每个字母依次都被靠后的第三个字母取代。换言之，字母A变成D，B变成E，X变成A，Y变成B，Z变成C，依此类推。尽管这种加密术极易解码，但是“li brx grq’ w nqrz krz lw’ v qrw reylrxv!”——转换成明文便是“if you don’ t know how it’ s not obvious!”（如果不知道原理，可也没那么简单！）。这种加密术的一个变种是ROT-13密码，每个字母均循环移动13个位置。

简单的替换加密存在重大的缺陷，因为重复出现的某个字母总是会用相同的字母替代。通过对某种语言的分析，便可知道字母被移位的大致距离——请注意上述密文中字母“r”的出现位置。熟悉英语的人就知道，它可能是一个元音——这种信息随即便可用来判断移位距离。

在古代，人和人之间的信任并不是唯一要关心的问题，身份验证也很重要。如果只有少数人能读会写，那么签名或许足以证明一个人的身份。但随着掌握读写知识的人越来越多，印章逐渐成为“签署人”一种独特的记号。利用这种记号，便可证明信件、文档和法令签署人的身份确实无误。但随着技术的发展，人们可轻松仿制出各式各样的印章，所以它也失却了原先的“独特”性。事实上，伪造印章是件再容易不过的事情。

发展到近代，密码和与之对应的译码术在历史上占据了一个重要的地位。在美国被硬扯进入二战之前，军队已有能力破解日本政府的密码。所以，美国政府事实上能够事先知道日

本攻击珍珠港的消息。然而，这一能力并未得到很好的利用。由于这次“奇袭”，美国遭受了惨重的损失。在同一次战争中，德国政府使用一种名为Enigma的加密设备，对自己的通信进行加密。这种设备使用了一系列转轮（Enigma机器共准备了5个，但每次通信的时候，均只使用其中的3个）。这些转轮包含了字母表中的所有字母，每个都可以单独进行设置。对正常输入的文字来说，其中每个字母都被转换成看似随机的输出字符。之所以说它“看似”随机，是由于换位顺序的组合是一个天文数字。对Enigma机器的破解首先由波兰发起，最后由英国完成。对Enigma的解密产生了许多“可歌可泣”的故事，内容之丰富，完全可以写成另一本书，事实上，已有关于这个主题的多本书籍问世。

自凯撒大帝的年代开始，一直到当代，通信技术在稳步地发展着。从纸张到电报、电传、电话、传真以及E-mail，人和人之间的通信变得如此方便和普遍。与此同时，保障这些通信的安全也逐渐成为一项重要课题。最开始的时候，只有少数人关心此事，而且通常都是政府和军队。

每种通信方法的安全取决于建立通信的那种媒体（或媒介）。媒体越开放，消息落入外人之手就越有可能。现代通信方法一般都是开放和公用的。打一次电话，或者发一次传真，信号会穿越一个共享的、公共的“电路交换”电话网络。而在发一次E-mail的时候，它也会穿越一个共享的、公共的、包交换的网络。在网络中，位于通信双方两个端点之间的任何一个实体均可将消息（信号）轻易拦截下来。如果要通过现代的通信技术来进行数据的保密传输，便必须采用某种形式的加密技术，防范那些“偷窥者”窃取秘密。

现代的基本加密技术要依赖于消息之目标接收者已知的一项秘密。通常，解密方法（亦即“算法”）是任何人都知道的——就象所有人都知道怎样打开门一样。然而，真正用来解开这一秘密的“密钥（Key）”却并非尽人皆知——就象钥匙一样，一扇门的钥匙并不是任何人都拿得到的。当然，还有某些加密系统建立在一种保密的算法基础上——通常把它叫作“隐匿保密”。但大多数人都讨厌使用这种加密方法，因为它未向公众开放。人们无从得知它的加密能力到底有多强，是否存在缺陷等等（目前针对“加密芯片”展开的辩论便是这样的一个例子）。

那么，剩下的问题就是如何保障密钥的安全了——密钥只应该由那些应该拥有的人持有。现代的密码术为此提供了强有力的保证！

1.2. Internet的崛起

随着Internet的日益流行，人们对它的起源产生了各种各样的说法。从浏览器公司到工作站厂商，一直到某些路由器的制造商，许多人都声称自己是Internet的始祖，或者说自己是它的骨干。但大多数人都认为，当代的Internet起源于60年代末期，当时称为阿帕网（ARPANET）。阿帕网当时是作为一个研究工具使用的，用户主要是那些为美国政府工作的人员，并全体接受“高级研究项目部（Advanced Research Projects Agency，ARPA）”的领导。它的第一名承包商是位于麻萨诸塞州剑桥市的BBN公司。

建设阿帕网主要是为了方便大学、军队和国家实验室之间的通信。通过阿帕网，散布于各地的研究人员相互间可以交换文件和电子消息。随着网络规模的扩大，它逐渐分割成两个部分：MILNET（军队网）和ARPANET（阿帕网，名字未变）。前者用于军事通信，后者继续作为一种科研工具使用。到80年代初，人们为阿帕网规定了一种通信协议标准——实际是

一套协议（协议套件）。这就是著名的TCP/IP协议套件，它最终变成了只是“TCP/IP”这一种协议。TCP/IP是当今几乎所有网络通信的基础。

1987年，美国国家科学基金会（NSF）建立了一个网络，将散布在全国各地的六个超级计算机中心互联到了一起。这个网络便是著名的NSFnet，范围之大，贯穿了美国全国。从西海岸加利福尼亚的圣地亚哥，一直到东海岸新泽西州的普林斯顿。NSFnet最开始采用56K的租用线路，在那些日子里当然绰绰有余，但按今天的标准来看也不免太慢了，所以NSF也公开征求铺设一个新的高速网络的提议。最后，由MCI、IBM和MERIT（以密歇根大学的一个网络为基础的一家组织）联合草拟的一个提议胜出。自此，我们现在称为Internet的一个网络干线被建立起来。

在90年代的10年间，这个网络的骨干不断得到扩张。许多电信公司提供高速租线供客户连接Internet，而当地的Internet服务供应商（ISP）提供廉价的本地入网服务，吸引越来越多的用户上网。今天，通过互惠服务条例，互联网络可承载对方的通信。这样便建立了一个世界性的网络，用户只需缴纳本地入网费用，便可访问全世界的资源。

1.3 Internet的安全

Internet是一种不易让人捉摸的东西。从不同的角度看，它可能有多个不同的样子。在此，让我们从“分享秘密”的角度来看待整个Internet！可将Internet想象成一个巨大的厅堂，充斥着形形色色的人，嘈杂无比。在这样的环境中，要想沟通一项秘密显然是异常困难的。随着两个人之间距离的增大，别人偷听到他们之间的对话的概率也会迅速增大。由于Internet是一种真正意义的全球网，所以假如没有加密技术的帮助，所有的通信都会毫无“秘密”可言。

随着Internet的快速扩张（这几年几乎以“爆炸”性的速度增长），人们对它的依赖程度也越来越高。信息可以便宜和可靠地传递，而通信正是商家赖以生存的根本。对一家打算从事电子商务的公司而言——亦即通过Internet销售产品和提供服务，通信的安全是一个最基本的前提。对于象信用卡号码这样的敏感信息来说，它们必须得以有效的保护，而且商家必须能对每一笔业务进行验证和授权。除此以外，商家可通过Internet连接分散于各地的办事机构或子公司。电子邮件（甚至电话）可通过Internet在办事机构之间路由传送。由于敏感的公司内部资料也可能通过这种链路传输，所以对于安全保密的要求是显而易见的。

但Internet的安全问题并不仅仅牵涉到做生意的商家。每个人都需要、而且有权利保护自己的个人隐私。某人上网之后，对隐私的这种要求并未消失。随着消费类电器越来越向Internet靠拢，对安全的要求也日益迫切。通过Internet使用自己的电话和VCR时，我们不希望有一些喜欢恶作剧的人或者一些黑客来侵占我们的电话线路，或者不定时开关我们的VCR。

然而，隐私也不仅仅是信任谁和不信任谁的问题，它也包括匿名的权利。人们在赛伯空间里畅游的时候，一个经常被忽略的问题是个人保持匿名的权利。按照传统，我们看过什么、去过哪里、与谁交谈过、选举的是谁以及购买了什么东西，所有这些信息都是不应公开的，也是不应为别人所知的。假如在赛伯空间里，要求人们必须提供在现实生活中通常隐匿的信息，便会极大地打击这些人上网的积极性。

幸运的是，加密技术可有效地解决这些问题。

1.4 加密工具

加密工具并非只有单独的一种！有多种技术都可用来加密信息、安全地交换密钥、维持信息完整以及确保一条消息的真实性。将所有这些技术组合在一起，才能在日益开放的世界中，提供保守一项秘密所需的各项服务。

其实，世上本不存在“绝对安全”的东西。对任何一项秘密来说，都存在泄密的可能。分析专家必须根据实际情况判断出泄密的后果有多严重，以及泄密的可能性有多大。通常，一种加密方法的“健壮度”是由其复杂程度来决定的。例如，假设某种特定的加密系统复杂程度是2的32次方，我们便认为为了破解它，需进行2的32次方次独立的运算。这个数量表面上似乎非常大，但对一部高速计算机来说，它每秒钟也许就能执行数百乃至上千次这样的解密运算。所以对这种加密系统来说，其能力尚不足以保证秘密的安全。正是考虑到这样的情况，所以我们用“计算安全”来量度一个现代加密系统的安全程度。

1.4.1 加密基础

就公共密钥加密系统而言，它有一部分建立在“单向函数和活门”的基础上。所谓“单向函数”，是指一个函数很容易朝一个方向计算，但很难（甚至不可能）逆向回溯。所谓“活门”，是指一种可供回溯的“小道”。换言之，利用它预留的安全通道，可欺骗系统，逆行回到初始状态——亦即暴露出秘密。

为使这样的单向函数能有效地应用于加密系统，它必须有能力对任何输入都进行这样的单向计算。比如在一个有限的范围内，很容易计算出数字的乘积，但却很难分解出生成那个乘积的各个乘数。另一个例子是离散对数问题：一个大质数p，以及一个底数g。已知一个特定的值y，求指数x，如下所示：

$$g^x = y \bmod p$$

其中，mod是“求余”的意思。模指数很容易便可计算出来，但假若想通过一次离散对数运算恢复原来的指数，却是异常艰难的。对于每一类数字——奇数、回文数字、可用47除尽的数字，离散对数如何解决仍然非常困难。

单向函数没有正式的数学表达公式，但某些函数似乎拥有单向函数的一些属性，所以通常将它们称作“单向函数”。当然可能存在一些途径，可象求积那样快速地找出乘法因子，但迄今为止尚无人发现。正是考虑到这方面的原因，我们才可以很好利用这种乘因计算困难的特性。

所谓“活门函数（Trapdoor Funcitons）”，解释起来稍微有些困难。现代加密算法广泛地运用了这种技术，但却很难一下子指着某个函数，肯定地说：“那便是活门函数！”有一个例子可以很好地解释活门函数。试想一棵树，上面有许多分枝。从一片树叶到树干是一条直路，不要求作任何选择。但要想从树干返回一片特定的树叶，却要求选择一个分枝，然后选择一个子分枝，接着是更深一层的分枝，依此类推，最后，选择具体的树叶。“活门”负责的便是对这种分枝选择方法进行描述。

至于发现一片特定树叶的困难程度，显然取决于树的深度。图1-1展示的那棵树总共有5层的深度，所以有2的5次方片树叶（32片）。从树干到图中选定的目标树叶所经过的“活门”就是“左－右－右－左－右”这个“密钥”。应该注意的是，活门函数完全不适合用作任何种

类的加密用途。但为了演示一个活门的概念，它还是能够胜任的。

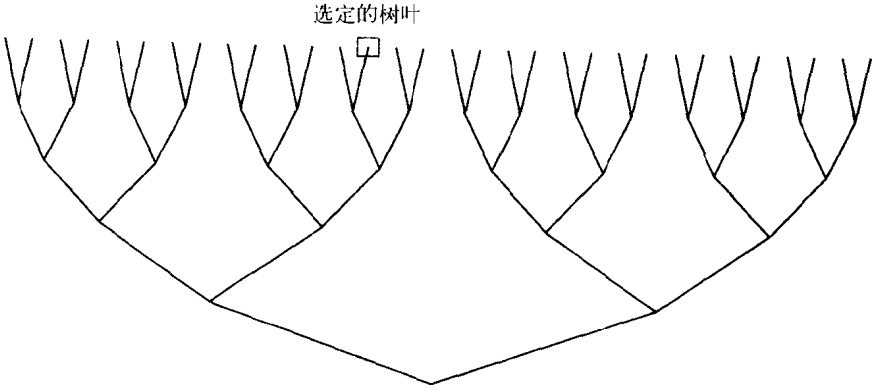

图1-1 一棵活门函数树

在现代加密技术中，我们将单向散列函数应用于身份验证及完整性校验。“单向散列函数”并不同于刚才讲述的“单向函数”的概念。散列函数采用一条长度可变的消息作为自己的输入，对其进行压缩，再产生一个长度固定的摘要。一致的输入会产生一致的输出。由于对任何长度的输入来说，输出都是固定的，所以显而易见地，对一种散列算法H来说，可能存在两个不同的输入：X和Y——比如H(X)和H(Y)。这样便产生了冲突。单向散列函数的设计宗旨便是将这种冲突的发现（亦即找到两个会产生一致散列摘要的随机输入）变得非常困难。

当今流行的散列函数是MD5（Message Digest 5，消息摘要5）和SHA（Secure Hash Algorithm，安全散列算法）和RIPEMD。尽管它们生成的摘要具有不同的长度，而且拥有不同的速度及抗冲突特性，但都是目前所广泛采用的。

和单向散列函数相比，单向函数（建立在一个“活门”的基础上）使用时要涉及到更多的计算。和用散列函数保障消息的完整性比较起来，假如用单向函数加活门的方式（比如数字签名方案）来保障消息的完整性，那么后者需要的时间要多得多。但在某些情况下，也许根本就不能使用一个单向散列函数。在以后的章节内，我们将向大家展示IPSec和IKE如何同时运用这两种技术。

另外一种经常用到的技术是简单的“异或（XOR）”函数。它既不是单向函数，也不是活门函数，但同样是构建加密系统一种有用的工具。有基本数学知识的人都知道，两个0进行XOR运算的结果是0，两个1进行XOR运算还是得0，而一个0和一个1（或者一个1和一个0）的XOR运算结果是1。XOR运算一个非常重要的特点就是它的交替性。取得任何数据后，用长度固定（一个位、一个字节或多个位、字节）的一个键值对其执行XOR运算。得到结果后，再用同样的键值对那个结果执行XOR运算，便能恢复原来的数据。这其实就是一种非常简化的“加密”算法。但要注意的是，只要知道了输入或输出数据，都有可能推断出另一边的输入。这个特征通常并不是一种真正实用的加密算法所具有的，它暴露出用XOR算法进行加密的弱点。

1.4.2 机密性

数据的机密性是由加密算法提供的。算法将一条正常的消息（明文）转换成乱码（密文），再将乱码转换回正常的消息，实现加密（编码）和解密（译码）的过程。有些加密算法是对

称的——用来加密的能力可同样用来解密，而另一些算法是不对称的——不用“活门”，便不可能对加密的东西进行解密。不对称算法并不当作两个独立的函数对待（一个用于加密，另一个用于解密），而是当作单独的一种算法。因此，无论一种特定算法的“对称性”如何，加密算法都是可以交替（双向）使用的。

明文＝解密（加密（明文））

这一点是显而易见的，因为对于将自己的输入永久性打乱（不可恢复）的任何一种算法来说，尽管非常安全，但却没什么实用价值。

1.4.3 对称加密算法

对称加密算法要么以“块”的方式，要么以“流”的方式，对输入进行处理。“块加密算法”的例子包括DES、CAST和Blowfish等等，它每次对一个数据块进行处理。至于块的大小，则取决于算法本身（上例三种算法均采用64位的块长度）。对一个块的处理叫作加密算法的“处理单位”。而在另一方面，“流加密算法”每次处理的是数据的一个位（或者一个字节）。用一个键值适当地进行种子化处理，便能生成一个位流（“位”指二进制的“位”），可用它对输入数据进行XOR运算。

注意无论块加密还是流加密，它们都特别适用于批量加密。由于IPSec仅采用了块加密算法，所以大家需要阅读其他的书籍或资料，了解流加密算法的详细情况——本书不打算对其作深入探讨。

块加密算法可采用不同的模式工作。不同的模式将上一次操作的结果“喂”给当前操作，从而将数据块链接到一起。综合运用这些模式，便可使一种加密算法变得更为“健壮”，对特定的攻击产生更强的免疫力。举个例子来说，块加密算法的基本应用就是“电子密码本（Electronic Code Book，ECB）”模式。每个明文块都加密成一个密文块。由于使用相同的密钥，相同的明文块会加密成相同的密文块，所以对一段已知的明文来说，完全能构建出一个密码本，其中包含所有的密文组合。如果我们知道一个IP数据包已进行了加密处理，那么由于密文的头20个字节代表的是IP头，所以可利用一个密码本，推断出真实的密钥是什么。

由于不能保证输入数据的长度正好为一个密码块长度的整数倍，所以根据具体的模式，需要对输入进行适当的填充。假如块的长度是64位，而最后一个输入块的大小仅48位，那么就有必要增添16位的填充数据，然后才能执行加密（或解密）运算。以具体的模式为基础，加密后的填充数据要么成为密文的一部分，要么立即删去。

加密块链接（CBC）模式可取得前一个密文块，并在对下一个明文块进行加密之前，先对两者执行一次XOR运算（如图1-2所示）。假如是第一个块，那么与它进行XOR运算的是一个初始化矢量（Initialization Vector，IV）。IV必须具有健壮的伪随机特性，以确保完全一致的明文不会产生完全一致的密文。解密过程与加密相反：每个块都会进行解密，并在对前一个块进行解密之前，对两者进行一次XOR运算。解密到第一个块，它同样会与IV进行XOR运算。在IPSec中，目前定义使用的所有加密算法都属于“块加密算法”，采用CBC模式运行。

其他流行的模式包括“加密回馈模式（Cipher Feedback Mode，CFB）”，前一个密文块会被加密，并与当前的明文块进行XOR运算（第一个明文块只与IV进行XOR运算）；以及“输出回馈模式（Output Feedback Mode，OFB）”，它会维持一种加密状态，不断地加密，并与明

文块进行XOR运算，以生成密文（IV代表初始的加密状态）。

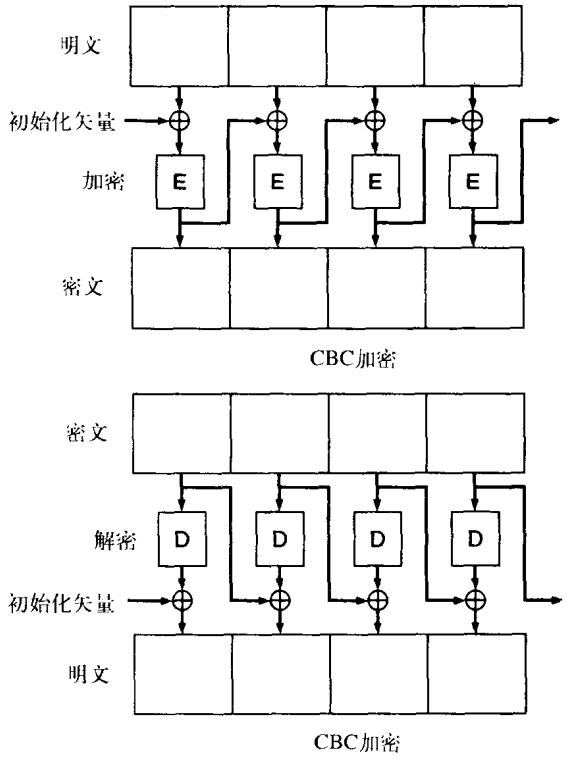

图1-2 加密块链接方式

1.4.4 不对称加密算法

不对称加密算法另一个通俗的名称叫作“公共密钥算法”。其中要用到两个密钥，一个是公共的，一个是私人的。一个密钥负责加密（编码），另一个负责解密（译码）。在仅知公共密钥的前提下，完全不可能据此推断出私人密钥是什么（就像前面的定义，我们可认为公共密钥算法是“计算安全”的。好的公共密钥算法是建立在单向函数基础上的。

一般认为公共密钥加密术是由Whitfield Diffie和Martin Hellman发明的。详情可见他们的论文“加密新思路（New Directions in Cryptography）”，由IEEE的“信息理论学报”于1976年出版。最近，英国政府的“通信电子安全协会”（即CESG，地位相当于美国的“国家安全局”）公开了一些文件，显示出他们的密码专家实际提出这一概念还要早6年！1970年，James Ellis草拟了一份CESG内部报告，冠以冗长的“保证不安全的数字加密的安全的可能”标题，其中讨论了一种可行的理论。后来，Clifford Cocks和Malcolm Williamson分别撰写论文，对实际的方案进行了描述，其内容已基本接近后来的RSA以及Diffie-Hellman方案。但无论如何，Diffie-Hellman论文的出版是一个异常重要的事件。比起推迟了20多年才公开的英国政府文件，它的重要性要大得多。假如“加密新思路”未在IEEE得以出版，英国政府的机密文件至今可能也不会解密公开。至于背后到底隐藏着什么秘密，恐怕只有天晓得了。

1. RSA 目前最流行的公共密钥算法就是RSA，名字来源于它的发明者：Ron Rivest，Adi Shamir以及Leonard Adleman。RSA之所以能够保密，关键在于假如已知两个非常大的质数的乘积，那么很难解析出到底是哪两个质数相乘的结果（因数分解）。RSA的重要特点是其

中一个密钥可用来加密数据，另一个密钥可用来解密。这意味着任何人都能用你的公共密钥对一条消息进行加密，而只有你才能对它进行解密。另外，你也可用自己的私人密钥对任何东西进行加密，而拿到你的公共密钥的任何人都能对其解密。这时，大家可能会想了：这样做有什么实际意义呢？注意这个概念在“非拒认”及数字签名中是非常重要的（不久就会详细讲到）。

RSA的一个缺点是速度非常慢，而且能处理的数据最多只能有它的密钥的模数大小。例如，一个1024位的RSA公共密钥只能对少于或等于那个长度的数据进行加密（实际最多只能有1013位，因为用RSA定义如何加密时，还要进行编码，这又要用去11位的长度）。尽管这一限制与“对称块加密算法”类似，但RSA的速度使其并不适合进行大批量的数据加密。然而，RSA也并非一无是处。相反，对于象密钥交换和数字签名这样的重要技术来说，它已成为一种事实上的标准！

2. El-Gamal　另一种公共密钥加密系统是El-Gamal，名字也是从其发明者来的：Taher El-Gamal。El-Gamal加密系统建立在“离散对数问题”的基础上。El-Gamal的主要缺点就是密文长度达到了明文的两倍。对于已经非常饱和的网络来说，这个问题无疑是一个大的缺点。但另一方面，El-Gamal本身是没有专利的（由El-Gamal拥有的唯一一项专利已在1998年到期），而RSA是有专利的。而且要想从专利持有人——RSA Data Security（RSA数据安全）公司——那里申请使用许可证，所需费用贵得惊人！但值得“庆幸”的是，RSA的专利也会在2000年的9月20日到期，还剩下不到一年的时间。El-Gamal加密系统与Diffie-Hellman密钥交换非常相似，我们不久便会详细解释这一点。

1.4.5　身份验证和完整性

为保守一个秘密，它的机密性是首先必须保证的。但假如不进行身份验证，也没有办法知道要同你分享秘密的人是不是他／她所声称的那个人！同时假如不能验证接收到的一条消息的完整性，也无法知道它是否确为实际发出的那条消息。单向散列函数在这方面可以大展身手！

1.4.6　身份验证

公共密钥加密可用来进行身份验证，只需构建一个所谓的“数字签名”即可。传统的手写签名具有一些非常重要的属性。由于难以伪造，所以很难否认。但由于手写签名只是文件上另外书写的一样东西，所以对一个不小心的人来说，有可能在一份已经签署的文件上增加额外的文字（尽管很难再造就一份书写工整的文件），造成签署人同意或承认多余文字的假象。由于Internet其实就是一个很大的匿名场所，数字信息可能存在很长的一段时间，所以我们还需要另外一些属性，来完善数字签名。

数字签名必须很难伪造，使签署人很难否认这是自己的签名，这和传统的手写体签名是一样的。除此以外，它还必须保证消息的完整性，而且必须是独一无二的。在一份经数字签名的文件中，我们希望禁止再增加额外的文字，也希望禁止从一份真实可靠的、已经签署的文档中移出签名，将其转嫁到其他文档。采用公共密钥加密技术，这些属性均可以实现。

最简单的做法是将数字签名想象为“加密”，而将对数字签名的验证想象为“解密”。事实上，这正是RSA签名的工作原理。但另一种公共密钥算法却不是这样工作的。这种算法现