第16章　基于网络的语音安全

主要内容：

- 窃听
- 电话跟踪
- 电话劫持
- 加密和安全
- 服务拒绝
- 其他安全问题
- 避免语音网络脆弱性

人们日常打电话的时候很少考虑到安全问题，实际上，每天在语音线路上传输的潜在机密信息量是相当惊人的。本章概要介绍安全问题的基本知识及基于网络的语音（ VON）协议的实现，必要时附加一些详细的说明，同时也占用适当的篇幅讨论了系统安全的维护方法。

众所周知，美国电话电报公司（AT&T）曾经占领了整个电话系统，从技术角度上讲该公司已具备了绝对的监控能力。但是由于利润比较低，人们对个人信息并不十分感兴趣，个人电话系统也很少被监视，甚至窃听和干扰私人电话曾经为法律所认可。

1996年远程通信法案成立，AT&T公司也在深入扩大的市场分化中逐渐解体，人们的安全意识不断提高。现在，我们所发送的呼叫是通过许多不同的实体到达通信终端的，尽管如此语音通信安全仍被深切关注，一切载波信号正在连续不断地控制对系统的访问，以避免非法入侵者窃听或干扰电话线路。

VON协议在许多方面进行了改进。搜索或控制数据的能力更接近于原始资料，而且可能与监视的人相关联，由于非法得到的信息能够获利，以致试图危及通道的安全的行为频频发生，不仅是电话公司能够维护和访问线路，其他公司和个人也能做到。研究表明， VON系统可实现安全性，但必须进行很好地规划。 VON系统也存在一些脆弱性、典型的有窃听、电话跟踪、电话劫持和服务拒绝。

16.1　窃听

窃听从电话系统发明之日起就已存在。最早的古典窃听案件出现于电话网络还是接线总机操作员进行手工转换的时候，当时的接线总机操作员对城镇每一个人的闲谈都了如指掌。

搭线窃听是最普通的会话窃听方式，只需将导线一端连接在电话铜线上，另一端系在扬声器或记录装置上。搭线窃听十分简单，但它需要对电话线进行物理访问并且在仅能在一根电话线上窃听。一旦语音呼叫在T1或ISDN线上转化为数字信号，呼叫就会转换成 0和1，并且以高达24路的呼叫进行多路传输。这时，为了窃听一根特定的电话线，对方必须区分呼叫被分配在哪一个时间段。当然我们也需要一些特殊的设备，并且不能中断服务也不能对中继线进行物理访

问，实现对线路的监控和解码。如果漫无目的从数千根线上窃听某个电话，那么不仅需要专业化的设备还需要足够的耐心，这些困难使电话系统窃听相对不普遍，只有政府和法律部门才有能力使用。

下面我们以语音网络解决方案在反窃听领域的应用为例，简单介绍应用过程中所产生的一系列问题。语音网络系统的窃听首先涉及到的是专业的语音数据包搜索设备、语音帧中继、ATM语音和IP语音等媒体设备都有可能窃听。

16.1.1 语音帧中继

语音帧中继与T1或ISDN干线在功能上相似，使用数字干线连接帧中继，能增加正常干线上的窃听难度，因为窃听者需要用专业化的设备，才能译解语音帧并为其解码。同时，帧中继使用多路复用，将数据与语音同时发送，这也增加了窃听的难度。绝大部分 VOFR装置是直接导入PBX和帧中继的，这给访问和连接带来了许多问题。首先，窃听者必须找到想要窃听的线路，通常这些线路是帧中继干线。其次，在找到正确的线路以后，必须确定一种连接方法。通常，一旦对方将主干线连接到线路上，帧的解码方案也就随之确立。通常由一个修改的帧中继路由器接受这些线路和通过其接口的帧，然后用所有的数据帧来组合语音帧，再从选出的语音帧中找到我们需要的呼叫。若想窃听到真实的呼叫就必须重新组合这些语音帧，使用正确的编码解码器进行语音通信解码。显然，这种窃听方式比窃听常规的电话系统更复杂，仅被为数不多的尖端攻击者所采用，即便可能的话，它的攻击危险也非常小而且容易暴露目标。窃听异步传输模式连接与之相似，这里不作详细讨论。

16.1.2 语音ATM

语音ATM与语音帧中继具有异曲同工之处。在大型专用网络上， VOATM将PBX主干线接口连接到数据路由器上，由一个控制存取单元执行（与 VOFR相同），利用ATM接口指向远程通信中央电话局。与帧中继相比， VOATM的窃听难度更高。帧中继在铜线上实现从客户到远程通信地的传递，而ATM则是在光纤线上进行高速多路传输。光纤上窃听必须保证最少的中断，窃听设备必须设置在能够收到语音帧的窃听器上，而且高速传输线的数据窃听设备造价昂贵。这一系列的因素使得ATM语音窃听极难实现，昂贵的费用迫使大部分窃听者另寻它途。

16.1.3 语音IP

现行的各种VoIP解决办法为窃听者提供了一条更加简捷的路径，其中网络嗅探器是必不可少的装置，它能够识别在线传输的数据包。我们将在第 20章介绍，这是实现IP网络窃听的通用方法之一。

目前，大多数公司的内部网络都用以太网作为基础结构。由于以太网是一种共享的媒体装置，所有网卡都能解释穿过物理网段的所有数据帧。网卡首先采集传入的数据包进行辨别，如果判断数据包是发往该主机的，就将该数据传输到计算机，否则，就丢掉数据包。而在网络接口设置为混杂模式的情况下，网卡会将所有的数据包传输到计算机内部。混杂模式经常在运行解码和显示接收数据包程序时采用，实现这种功能的程序即所谓的“嗅觉程序”，它对大部分软

件平台是相当实用的。详见第20章。

许多年来，嗅觉程序普遍地应用于发现和排除网络故障。修改嗅觉程序使我们能够观察记录全部UDP数据包，进而搜索并记录RTP数据流，与此同时，我们也获得了所有发生在特殊段的VoIP呼叫数据包。

早期的以太网一般是由单独段构成。随着越来越多的公司采用交换机硬件来分割各自的LAN网，这能够限制被监视的呼叫数量。但是使用在 20章所介绍的地址解析协议和端口监视技术，能使交换机像正常的集线器一样，将所有的网段暴露给攻击者。

嗅探所有的网络通信能访问正在进行的所有呼叫。当事件的序列很难确定时，攻击者能够用一个终端窃听VoIP上的所有线路，而不需要对线路进行物理访问。如果网络中有网关，一个终端就能窃听和记录整个T1线路或者多路T1线路上的呼叫。但是如果缺乏特殊的设备，在 VoIP系统上进行窃听也很危险。这里我们只讨论通过 UDP数据包来得到RTP数据流。

嗅探器可以记录所有的控制通信。在记录过程中嗅觉程序将进一步被修改，目的是为了模拟一个听端用户参加会议的情景，这样嗅觉程序就能容易的掌握终端之间用于协商的编码解码方式和传送的RTP数据流的UDP端口，而且这种会议终端仿真程序还能够实现语音的实时重放。当然，嗅觉程序的这种仿真功能也为窃听者所密切关注。

嗅探器也是系统解密高手的一件利器。一旦取得了某一系统的访问权，那么该系统所有带有密码和敏感信息的数据包也就唾手可得，因为在语音信息已经编码成数字数据的基础上，入侵者能够轻而易举的记录和窃听任何近期收到的呼叫，并且，他们也可以简单的建立一个连接VoIP终端的双重数据流。网络分割是对付嗅探器保护的一种最为普遍而有效的形式。嗅探器仅仅工作在共享的物理网络线路上，在确保语音通信量的前提下，只要没有个人计算机在类似 IP电话的物理网络上工作，如果我们对线路传输的通信量适当限制，就能够大大削弱嗅探器的功能。另外，一些专用的网络扫描器也能够分辨带有混杂模式网络接口的机器，比如安全软件技术中的反嗅探器。

16.2 电话跟踪

电话跟踪实质上是记录呼叫的源和目的电话号码，它的脆弱性与窃听密切相关。如果嗅探器的设计目的是为了记录呼叫控制数据包和 RTP数据流本身，那么电话跟踪就属于窃听 VoIP电话的一部分。

16.2.1 非VoIP网电话跟踪

非VoIP网电话跟踪与在语音帧中继和语音 ATM上的电话窃听具有相同的约束条件，在这两种情况下，数据流的能见度比较差。在模拟网络上很容易实现自动跟踪，但对于有权获取数据的代理处，相关的计费公司将会向其提供某一线路的正确记录。

16.2.2 VoIP网电话跟踪

在VoIP系统中，指定终端上的电话跟踪同样可以达到窃听的目的。只要劫获数据包，机器就能搜索并记录全部呼叫，在此基础上，入侵者通过控制交换机硬件，就可以跟踪整个商业区

内的所有电话，包括多路T1线路或ISDN PRI。

商业电话跟踪既有其积极的一面，又有其消极的一面。信息透明度的提高能够有效刺激雇员工作的积极性，避免欺骗电话；但是它又令人心存疑忌，因为许多公司想得到那些已分给了用户、提供者或竞争者的数据。

嗅探器如果经过修改具备电话跟踪功能，就能够记录文件的全部数据。跟踪呼叫源和目的并不是信号通道里传送的惟一有价值的数据，通道中也包括 DTMF信息。按下标准电话的任一数字键就能产生双音多频音调，为了与 DTMF音调协调作用，各种基于电话技术的系统相继出现。其中，语音邮件和电话卡系统是两个典型的范例。不仅带有语音邮件密码的 DTMF音调可能被俘获，而且带有语音邮件系统号码和邮箱号码的电话，甚至当用电话卡打电话或用 DTMF传送消息时这些音调也都可能被俘获。

所有的VoIP协议都支持电话跟踪，俘获报头信息能够提供呼叫源和呼叫目的。报头对于呼叫本身的路由选择是至关重要的，因此它包含了呼叫的源和目的。

H.225初始化一个呼叫的同时就已经提供了 H.323呼叫源和目的。通过记录呼叫双方的号码，就能实现对每一个呼叫的源和目的的跟踪。由于 H.323呼叫都带有一个特殊的标识符，所以就有可能提供有关该呼叫的更多信息。例如，通过嗅觉程序查看呼叫 ID的释放完成报文，就可以得到呼叫时间。SIP也可以被跟踪，从而记录含有呼叫源和目的的邀请报文。

16.3 电话劫持

尽管它并不是VoIP系统中常见的攻击，但它仍然可能在中途劫持该呼叫流，并将该介质流重定向到另一个终端。

16.3.1 H.323

H.323可以通过3种方法实现电话劫持。首先，一个终端能够发送信息给一个正在通话的端点，信息的内容为将呼叫转移到另一端点。这就促使端点释放当前呼叫并连接另一特殊端点，这种盗用电话的方式将呼叫从初始终端连接到一个新的终端，从而劫持呼叫。

其次，入侵终端借助H.450.2的呼叫转移功能，发送一个伪造的 H.450.2报文给呼叫端点中的一个，使其呼叫报文中指定的终端，这种呼叫转移在地理位置分散的企业中尤为典型。不同的是，并没有采用 PBX进行呼叫转移，呼叫转移只是发生在远程终端之间。相比之下，这使电话劫持更易实现。

最后，这也是H.323电话劫持中最复杂的一种形式，它需要控制网闸，在这种电话劫持中，是网闸把进入该领域的钥匙递给了闯入 H.323网络入侵者。这样，入侵者就能够随意跟踪电话，控制电话带宽，并且阻止任何对端点的 H.323服务。当控制全部别名和注册信息的网闸被外部操控时，入侵者就能轻而易举控制呼叫的改向，比如他可以重定向所有到公司经理的呼叫。为了实现电话劫持，当网闸为端点建立一个呼叫的时候，该呼叫被劫持并传送一个空消息给呼叫中的两个端点，之后切断呼叫并发送所有的 H.245消息给新的端点，产生新的协商、确定新的主 /从关系并建立端点之间的新的呼叫。

16.3.2 会话创始协议（SIP）

从某种意义上说，SIP比H.323更成功的避免了电话劫持。SIP很少控制正在进行的呼叫，借助SIP重定向服务器的特殊功能，入侵者可以俘获邀请报文并能发送一条 300消息暗示被呼叫方已经离开，出示自己的转发地址，以此使呼叫者与终端相连来欺骗呼叫者。

H.323和SIP都支持使用加密来保护RTP数据流的安全。H.323称其安全附件为H.235协议。该协议非常健壮，不仅仅可以用来加密流，还可以用来加密 H.245信令报文。

16.4 加密和安全

加密是一种公认的保障通信安全的流行方法，数据经过高技术加密处理就能够拒绝非法访问。尽管线路上数据传输的基本形式是简单的 0和1，但是与一般的文件相比，加密语音面临更多的挑战。

16.4.1 H.245加密

H.245加密通过必要的鉴定形式以确保能够使用数字证书或挑战响应。为此，在挑战响应或者访问根结点以验证数字证书的情况下，端点必须有一份共享秘诀，以产生密钥。如果有一个共享的或者用密钥签署的数字签名， H.245就能够利用它们加密，然后通过端点将密钥发送到安全的H.245通道中再对媒体数据流进行解码。秘密是执行对称加密所必备的，我们用它来产生密钥部分。无法共享秘密两个终端不能加密和解密同一个信息，但是任何知道密钥的人都能够解密，正因为如此常常导致发送紊乱。同时，对称加密不能在两个无法共享秘密的端点间实现，如果一定要实现对称加密，我们就得通过公共密码系统 Diffie-Hellman密钥交换生成关键码秘密。但是，初始序列必须明码传送，允许俘获或攻击。媒体数据流在开放逻辑通道报文中交换密钥，启动加密。管理者使用包括密钥的同步加密字段，而接收者则使用相同的密钥解密数据流。如果H.245通道不安全，那么密钥将很容易被网络嗅探者劫获，在这种情况下，就要利用 H.245加密更新或加密更新请求命令来修改密钥以防泄密事件发生。总之， H.245通道必须具备足够的安全性能来阻止电话跟踪或对其他相关信息的攻击，比如呼叫重定向或盗用电话卡等等。

16.4.2 会话创始协议和加密

SIP加密依赖于RTP规范，RTP为使用了加密算法的特定区域提供了一种提取关键字的方法，这也使得RTP信息也能被加密。加密规范概要为 RFC1890。

在会话描述协议中，SIP同时传送加密算法和密钥，规定用“ k ”参量传送端点之间的信息，反映密钥信息传送过程。但这只能处理数据流本身的加密，因为 SDP是在SIP报文中发送的，它以明码形式传送，很容易被捕获，从而得到密钥并对媒体流解码。

另外，SIP利用公共密钥机制轻松地实现了报头信息加密，加密报头字段允许终端指定使用的加密方法。邀请报文的接收者可用专用密钥对加密部分进行解码。 SIP规定用空白线来区分报头的加密部分和未加密部分信息，同时也能通过数字签名的使用提供认可，这有效阻止了攻击者利用中间人干扰加密电话。

16.4.3 媒体网关控制协议和加密

媒体网关控制协议属于高层控制协议，它在许多方面的设计独具特色。在它的核心协议中不包含为安全呼叫提供的内在加密。MGCP的设计满足了高水平的专业化应用，如载波等级服务首次展示、中继线多通路等。这些应用软件一般用于低等待时间，高带宽的专用网络。这些网络对因特网的IP结构没有任何访问点，因此个人呼叫的安全性并不是首要问题。MGCP加密支持是一个低层协议，也正因为如此它通常用来实现IPSec或不可靠网络的专用VPN通道。

16.4.4 加密和服务质量

目前，加密技术虽然能够增强语音网络系统的安全性，但实际应用的还相当少，语音通信仍旧严重依赖于端到端的服务质量。实际上，大量数据包的损失、过多的延迟等都将影响到语音通信质量。

加密技术之所以没有广泛普及，其中一个重要的影响因素是硬件设计与延迟之间的矛盾。因为对于没有专用的电路的分组交换拓扑结构，数据包通过的路径将会产生延迟。当网络阻塞或者出现一个微小通信阻塞时，就会发生延迟混乱。同时，编码译码的问题也不可忽视，因为编码译码器将模拟信号转换成数字信号，编码数据的解码等都会增加额外的延迟，而系统通常无法承担大量的延迟。所以如何排除产生延迟的隐患是设备售方人员所密切关注的问题。尽管现有加密处理会引起很大的延迟，影响到系统的正常工作，但只要有足够的市场需要，生产商也可能大量制造专用处理器，所以低延迟加密仍具有很大的发展潜力。

16.5 服务拒绝

服务拒绝对任何一个基于网络服务的用户的影响是微乎其微的，但它对语音通信却起着举足轻重的作用。如今金融体系对语音系统如此依赖以致一个中断可能导致整个地区的经济陷入瘫痪状态，可见语音通信的重要程度。目前，服务拒绝已成为IP界攻击的一种普遍方式，攻击者可以随心所欲的切断任何电话。由于VoIP使用的带宽和我们正常的网络带宽相同，这就使得VoIP很难抵御大规模的DoS攻击。

如果VoIP实现包括因特网传输，那么给出一个网络IP地址，大型DoS或DDoS就能消除指定的电话。VoIP终端其实也相当于一个结点，它很难抵御同类型的DoS攻击。同步信号溢出也将引发一系列问题，并且网络会有遭到攻击的危险。以特殊的呼叫为目标，他们使用的协议有可能用来断开呼叫连接，拒绝服务。

语音服务拒绝方法

利用伪造的H.245关闭逻辑通道报文可以产生服务拒绝。如果存在一个与H.323系统相关的网闸，那么伪造的网闸“脱离请求”报文可能终止呼叫，实际上也就起到了服务拒绝的作用。

在SIP协议中，没有加密的伪造的“BYE”请求可能过早地终止正在进行的呼叫，由于使用伪造的删除连接报文，在MGCP中也同样可以产生服务拒绝。

16.6 其他安全问题

语音IP可能引发网络安全新问题。媒体数据流全部使用 RTP协议，这就涉及到了UDP端口的动态分配，进一步影响到防火墙管理。许多防火墙管理员会禁止未被申请的内部通信，但是VoIP则要求所有的UDP数据包都能被传输。在 H.323中，H.245也用来动态分配TCP端口，这会导致一些问题。另一个安全问题是必须连接 IP网络，这使得音频系统很容易被访问。另外，提供VoIP服务的设备和操作系统也存在一定的脆弱性。

16.7 避免语音网络脆弱性

现在语音网络已经暴露出一些明显的弱点，也许潜在的弱点还更多。我们应该通过多层次的技术应用来保护语音网络免受影响。某些保护 VON基础结构的方法有助于克服现有的弊端并且尽量避免新的弱点出现。实际上， VON系统和网络具有许多类似的安全问题，某些手段是通用的。

确保数据通信安全、防止外来入侵的方法是多种多样的。我们可以在网络边界周围设置障碍、注意与公共网连接的防火墙的使用、后门 Modem采用电话防火墙控制以及协调好公司之间的权限分配等等，同时内部网络的分割也将有助于提高网络速度和限制内部嗅探器的数量。我们还可以通过交换机、网桥、路由器和分割防火墙迫使攻击者无法获取网段的信息，除非他们使用更尖端的技术。还可以将 VoIP系统放在一个与本地LAN完全独立的网络上，需要指出一点，这些安装了VoIP的独立网络应该使用与 LAN不同的地址。尽管个人计算机连接语音系统的使用会受到阻碍，但是这种拓扑结构提供了一个完整的缺口阻止边界路由器以外的网络通信量，极大地提高了系统的性能。如果必须采用当前 LAN的物理结构，那么通过使用一个独立的寻址机制，不提供网络间的路由选择，也能够阻止熟练的攻击者，然而却无法阻止嗅探器获取数据包。最后一种方法是利用相关的加密协议，但如上所述，现阶段由于系统延迟问题，许多设备并不支持加密协议，所以通常不采用这种技术维护语音网络。

16.8 结论

总之，VON技术通过平衡现有的基础结构成功地优化了语音传输系统，具有相当广阔的市场前景，但是VON仍存在许多技术难题。窃听、电话跟踪、电话劫持和拒绝服务对系统构成了威胁，因此网络设计必须使这些危险最小化，同时防火墙和加密技术有效保证了数据通信安全。

第17章　多媒体协议和安全

主要内容：

- 多媒体概要信息
- 视频会议
- 有线电视
- 有线调制解调器
- 卫星

这一章处理不同网络拓扑上的多媒体传输的安全，这不仅包括标准线路上的视频会议，而且包括在因特网上、有线Modem系统上、有线电视上、卫星电视上和其他卫星传输的视频会议。

17.1　多媒体概要信息

多媒体是一个挺复杂的术语，在其本质上，它是有至少 2种媒体性能的东西，就我们的目的而言，我们就采用这个定义并且用它来指能显示音频和视频数据流的终端。这些数据可能是远程电话会议、电影、电视频道、或者电视频道库，这些多媒体数据能在所有的网络拓扑上传输，但有些拓扑有内在的安全风险，这在这一章的后面讨论。

17.2　视频会议

今天的世界连接越来越紧密，远程旅行变得更加容易，而且变得越来越不必要。现在不仅有多方共享会议语音数据的能力，而且真实的视频数据流能够被传输到会议的双方。在视频会议早期，专用设备用来实现视频连接，每个系统有一个照相机和电视，这些设备能把资料数字化，然后对音频和视频数据进行多路传输，这些数字然后统一被送到高带宽的数字化链路，例如T-1或ISDN线路。

在当时，这些设备是非常昂贵的，并且这些数字线也是如此，这很大地限制了视频会议对地理位置分散的大公司的市场，这表示视频会议数据只能在两个位置不同的专用网络间进行传送，对于访问载波线路的人而言，这限制了数据拦截的危险，视频会议的这种方法极大的推动了个人计算机的发展。

17.2.1　网络视频会议

过去常常需要复杂的设备来实现视频会议，但是，大部分今天生产的计算机有显示视频和音频的功能，他们也能够处理音频数字和视频数字以及数据流的传输和接收。除了一个花费甚少的基于计算机的照相机外，一台计算机能完全作为视频会议终端。网络上的免费软件也可实现视频会议，通过使用 VoIP、H.323和SIP协议上的扩展协议，这些应用软件能实现视频会议。这些协议，当用来实现视频会议时，像他们用来实现 VoIP一样，有相同的内在的风险，因此，

他们对嗅探和数据通信的记录是脆弱的，记录不仅包括会议音频的部分，而且也包括视频数据流。因为视频会议仅仅是 VoIP的另一种数据流，所以这些协议对视频会议的跟踪、劫持和重定向都是非常脆弱的。因为有支持它的协议： H.323和SIP，所以视频使用 UDP端口的另一套装置传送。这些数据与RTP流的音频部分并行传送，且控制数据流的协议完全一样。

17.2.2 视频会议安全

视频会议无论用传统的方法或网络传输，都能当作一个复杂的电话来查看，这使攻击者的工作越来越难，因为他必须处理多类数据。在 PSTN中，视频会议在一个宽带 ISDN通道里处理。这些设备使用一个与 15章所讨论的类似的编码解码器，但是对视频部分和音频部分也分别有独立的编码解码器。

在PSTN、ISDN类型线路上窃听和记录视频会议是非常复杂的。首先，攻击必须毫无疑问的获得网络元件访问权，复制所有运行的数据，然后找到正确的编码解码器来译码。一旦数据被编码，它变成了数字形式，所以能进行加密，但是考虑在数据加密之前的数据访问的障碍，就很容易理解为什么只有如此少的加密工具。由于网络访问权，网络视频会议是一种不同的方式。因为VoIP系统的建立是为了进行网络视频会议，所以将视频加入 VoIP呼叫中也是可行的，这些系统把视频作为一个使用自己的编码解码器编码的附加数据流。因为任何归于 VoIP的脆弱性对视频会议系统都是相同的，这使包含在数据流中的数据更加脆弱。视频会议的拦截和记录能通过嗅探器把所有的数据包记录下来。当发送标题报文来建立视频通道时，协议将指定使用什么样的编码器进行视频传送，这为攻击者解码这些数据流提供了必要的信息。像嗅探和记录所有在H.323或SIP数据流的标题数据包的电话跟踪一样，跟踪会议内容和参加会议的人所采用的方法是相同的。这标题信息在视频会议和 VoIP中是一样的，它们只是视频信息的附加数据流，所以劫持和拒绝服务以相同的方式工作。

加密作为一种解决方案成效甚微，因为视频传输数据比音频部分的带宽更紧张，这导致了更多原始的数据需要被加密且线路上会有更多等待时间。不幸的是，电路上的低等待时间的需求仍未改变，所以加密可能不是一个明智的选择。这鼓励人们在足够安全的专用网络上运行基于IP的视频会议，或保证视频会议对敏感的信息不是一场讨论会。

17.3 有线电视

有线电视在美国大部分家庭里被广泛使用，这是因为有线电视是单向服务，所以与它相关的安全风险是服务偷盗，通道的设置是从单点到多点传送。单点被作称电缆头并且用户是接收端点，这种拓扑结构允许拥有这些线的有线电视公司使用电磁频谱的任何一部分来传送所有的模拟通道电视信号，每一个通道都有自己的频率，用户方的网络访问经常被电话端的物理访问控制。从终端获得物理访问之后，有线电视公司通过使用在线过滤器过滤用户通道信号，这些过滤器仅仅阻塞了电磁频谱所需的那部分。

17.3.1 数字电缆

数字传输的使用实现以后，有线电视的世界开始改变，有线电视公司发现他们不仅通过使

用数字传输增加了许多额外的通道，而且他们也能够得到更多有利的计费市场信息。使用一个编码解码器可把模拟信号编码成数字信号，视频编码器与音频编码器是相类似的，但它们需要采样更多的数据，数字有线电视仍然是一个单向服务，所以与它相关的危险也是服务偷盗。网络连接由两部分构成，电话端的物理连接和对数字信号译码的机顶盒，这些被加密的数字信号进一步被保护，机顶盒有一张智能卡用来提取解密数据流的必需的密钥，带有智能的机顶盒控制所有不同级别的用户访问和计费账单，与电力改变电缆线路相比，这使服务偷盗更难，并且智能卡的程序必须能够修改以允许访问。

17.3.2 有线电视安全

从有线电视公司的观点来看，有线电视安全的主题在本书讨论范围之外，现有机制的缺点在别处也有更详细的讨论，所以本书只讨论私人信息的传输。模拟有线电视对私人信息传送是不友好的网络，基本的前提是任何一个连接网络的人都能够窃听和偷看你的传输。这也许是可接受的，但是如果在一个非专用网络上，最好不要传送私人信息。从某种方式来说，由于网络的3个访问点，数字有线电视更安全。以智能卡为基础的加密对当前技术而言是难以渗透的，但是，这种网络仍然将信号发送到与它连接的所有终端，这有内在的危险并且这种网络不应当用于安全传送。有线电视的数字传输并不是电缆公司使用的惟一的革新方法，但是，因特网服务的需要已经产身生了全新方法：有线调制解调器。

17.4 有线调制解调器

对想要更多更好的Web页面的用户来说，因特网的繁荣带动了对带宽的巨大的需要，电话调制解调器被推向了极至，但是对用户来说这结果仍然是太慢了。市场促使有线电视公司考虑利用其基本结构来传输IP数据。有线电视公司以高达3Mbps的传输速度使市场前景被看好，并且有一个通向美国成千上万家的线路结构。有线调制解调器技术是为零售用户提供宽带访问而开发的。有线调制解调器实际上是用词不当，因为它不调制或解调，而是一个网桥，对用户前端网络的以太网帧进行翻译，然后以电缆网络的拓扑形式打包，这使有线调制解调器比调制解调器更相似于CSU/DSUS。网络的拓扑与有线电视是一样的，从一单点进入，对多个端点进行服务，主要的不同是数据通信是双向传输的，通过更新配置拓扑来接受双向通信，运行一个对系统每一个电缆头的访问连接之后，有线电视有了非常好的传送宽带的方法。

但是这类系统是有局限性的，因为它起初设计是为了单向通信，且数据对每一个端点都是相同的，它被作为“总线”型网络设计。对同类单向通信这是很好的，但当数据截然不同而且双向传输之后，问题就产生了。首先的问题是带宽本身的灵活性。因为你是网络的服务用户，所以下班时间可以提供很好的访问速度，但是当每一个人都在线时，带宽被所有的终端共享，这导致了与有线调制解调器相关的第二个问题：因为它是共享网络，所有的数据都传送到所有的端点，因此你的数据可能被网络另一方俘获或破坏。

有线调制解调器的安全问题

有线调制解调器存在于共享网络，这表明所有的数据包都将被送向所有的端点，如同第25章中所讨论的。任何广播网络接口的终端将会丢弃目的地址不是该终端的数据包，这可能通过

指定端口混合模式来克服，以致终端转发所有的数据到计算机的应用层，这种活动对攻击者是相当有利的，攻击者有机会欺骗整个网络的通信。

首先出现的有线调制解调器是简单的网桥。网桥将所有数据从电缆接口转发到本地以太网（用户与网络的连接触点）。有线调制解调器依赖于因特网的计算机的 TCP/IP栈来丢弃地址错误的数据包。近来，有线调制解调器变得更加先进，能根据其正确的 MAC地址接收数据包。电缆公司更积极地保护他们的网络，并且为了防止滥用系统，阻塞了源 MAC地址。所有这些障碍目前都能被克服。如果使用有线调制解调器的系统不能转发所有的数据包，系统可以使用以前的有线调制解调器或者购买有线网络接口设备。这些设备通常很昂贵，但是它们提供了很多改进功能。它们虽然不能配置成将所有的数据包转发到本地以太网中，但它们可以手工设置 MAC地址。这对于任何基于MAC的攻击或通信阻塞来说都十分重要。有些电缆公司只允许授权的 MAC地址进行网络通信，但很容易使用 ARP查找有线网络上的所有 MAC地址，当你需要发送数据，而电缆公司进行过滤处理时， ARP还能生成一个差异报告。直到有线网络使用 VPN通道或IPsec加密之前，数据包都有可能从总线上被捕获。因此，最好不要认为有线系统是一个安全的网络，也不要在上面传送任何敏感数据。

有线调制解调器网络的其他危险是它们总是为那些有科技背景的人提供访问，因为电缆公司很少提供防火墙来保护他们的客户，这些人很容易受到威胁。任何访问都应当有一个通信过滤装置来保护后面的端点。

17.5 卫星

每天，在世界电信基础结构上都会增加上千英尺的光纤电缆。因为光纤能以很高的速度携带大量的数据，所以可以说它是一个非常好的媒体。但是它也有缺点 —— 它是相当脆弱的，并且安装起来也很昂贵。光纤工作在地下隧道里，如果没有光纤覆盖物，安装光纤非常昂贵，这就导致了卫星通信的使用，卫星通信适用于不能用光纤服务的地方，以及遥远的地方或没有好的通信基础设施地方，使用卫星通信的巨大利益是如果你有一个接收天线，你就能使用它。卫星通信多年来用于进行全球电视频道转播和一些长途电话的传送。最近，卫星被用来提供有线电视的传送以及支持全球任何地方的便携式电话通话。因为卫星对无线传输而言仅仅是一个天线接收器，因此它不是没有危险的，卫星的高度和位置允许任何人接收转播信号。

17.5.1 模拟卫星传输

模拟卫星是用来传输电视的初始波段，也称 C波段卫星。模拟卫星不仅被用来传输信号给电视终端用户，而且也用来在站与站之间对电视节目进行中继传输。电视网络已经发射了很多颗人造卫星，所以窃听他们的信号也是很容易实现的，仅仅一根碟形的卫星天线就可以收到信号，将它放到正确的方位角和仰角，并且将它调适当的频率就可以看到清楚的信号，许多通过模拟卫星传输信号的人试图通过在信号加入噪声来搅乱信号，这些噪声的结构是一定的，因此它能够通过鉴频器滤出来，这些被扰乱的信号被用来保护高级的通道或其他的内容，但是有时候市场会有鉴频器出售。无线传输的增长和电磁频谱的有限性已经把越来越多的卫星数据变为了数字形式。

17.5.2 数字卫星传输

数字卫星传输变得越来越普遍，用在数字卫星上的设备和用在模拟卫星上的基本类似，本质上是来自地面站的微波通信，上行传输到卫星，卫星复制信号并将发送给接收终端。差别是数字卫星的数据是纯数字，避免信号受噪声的干扰，允许多路传输，并且允许压缩和加密，数字卫星当前最普遍的商业用途是为数字电视传送信号，这个系统与数字有线电视有类似的工作方式。卫星传送一条窄带数据流，终端用一根能够聚集数据流的碟形无线接收传送信号，并且经由电缆将信号传送到机顶盒中，机顶盒控制系统，用智能卡处理数据流的解密。智能卡储存解密的密钥并且也存储计费信息。数字卫星传输也能将因特网带宽传输到远程地区。然而目前工作的工具仅仅是单向的设备，正在开发引入双向设备的计划。

17.5.3 卫星传输的安全问题

如前所述，卫星传输是使用高天线的无线数据传输，这使用它们容易受正常无线通信弱点的影响。无线问题在第13章详细讨论，但是这里我们将讨论一些问题，特别是卫星这一方面。

和任何无线传输一样，任何处于发送范围内的人，使用一台调整到了适当频率的设备就能够收到被发射的信号。用卫星通信，拦截的风险性被加大了，因为卫星能够传送信息到所在轨道的任何一个地方。尽管拦截有风险，但是更难的是信号劫持、阻塞或信号代理。因为相同的理由信号的劫持和干扰都是非常难的，信号的频谱传输适合于微波段，微波段使信号方向性强并且是窄带。所以劫持和干扰微波信号可能需要一台高能量的微波发射机，并且你必须将它放在适当的地方使之对准要干扰的信号，如果电波垂直射入太空，这可能非常难实现。大部分信号是单向的，所以即使你有发射机，你也不能干扰卫星服务，不能窃取数据带宽。

代理信号或使用某些装置伪造卫星信号，面临着巨大的地理上的挑战。为了实现这一点你必须在你试图模仿的卫星上定出你的发射机的位置。广播信号的窃听是卫星通信的通病，这是由于在通信范围内都能收到信号。许多人意识到了卫星电视广播设备传送信号的价值并且试图拦截和解密付了钱的普通信号，这涉及到一些接收装置标准的更改。有各种各式的方法对标准进行修改，如商业的解决方法，以及国产的免费软件。窃取卫星电视信号的详细方法本书不予以讨论。但是，更改产生了小偷与电视公司之间的猫与鼠的游戏。随着新方法的出现，公司将阻止这些方法的使用，但同时也导致了更新的方法出现。

最令人感兴趣的一点是做修正的人是非常聪明的，他们的设备接收那些将信号传送到远程站点的通道。使用卫星传输任何一个公司的私有信息可能会经常遭受拦截，因此不予以推荐。任何类型的专用网络都是以安全而获利，因为你必须拥有正确的仰角、方位角和频率来接收信号，这3个部分的结合可能使工作量相当大，但是这不是保护，仅仅是作为网络上成千上万主机中的一个。任何以无线频谱传送的信息，从安全方面考虑都应以加密的方式加以保护。

17.6 结论

不管什么类型的信号传输或信号以什么方式传输，安全都应当考虑。就你所了解的而言，工作在今天的网络统一协议可以用许多方法破解，另外，从点到点的通信传输新方法也有它本身的缺点，根据数据的机密性安全必须给予适当的考虑。

第五部分　数据网络安全问题

第18章　加 密 技 术

主要内容：

- 代码和密码
- 对称加密法
- 公共密钥加密法
- 数字签名
- 公共密钥基础结构
- 密钥提存
- 信息隐藏法

很多世纪以来，各国政府一直在试图保持国家和军事秘密不被敌人及对手所发现。公司和企业同样对商业情报及贸易秘密的安全颇感兴趣。在当今世界，随着数据和通信网络的激增，我们的信息越来越容易被获取，因此，隐私问题日益显得重要。个人信息的收集和储存牵涉到我们的身体健康、财产安全、购买习惯以及我们平时访问哪些网址。大多数人不愿意公开这些信息，只有授权或有正当要求的人才可以知道。这一章将考察在信息储存和传送中保持秘密的方法，它们要么是把信息隐藏起来，要么将其转变成另一种形式从而使原来意思不被发现。我们将特别讨论代码、密码、加密以及信息隐藏法。

18.1　代码和密码

在一个方案中，为了隐藏语句中真实意义而用一些单词或字母代替另一些单词或字母，我们称之为代码（code）。大多数人都很熟悉代码并使用过它们。在学校里学生们用隐语在朋友之间传递“秘密”；在间谍影片中，间谍们用特殊的语句和暗号互相确认身份，这些都可称为代码。关于代码，还有一个发生在二战中的有趣的例子。当时盟军分布在南太平洋一片广阔的地域中，岛与岛之间的通信非常关键。因此发明一种方法以确保通信绝对安全是必要的。当时的目标是发明一种“不可破译的代码”，于是他们采用了美洲印第安人土著语言作为代码。这种做法曾经在一战中使用过，当时采用了Choctaw语。在二战中使用了Navajo语，它一种没有书写形式的语言。词语的替代，比如说用“嗡嗡叫的鸟儿”代替“战斗机”，用“铁鱼”代替“潜艇”，以及语言本身的复杂性都被用来建立不可破译的代码系统。代码是用一个单词或字母代替另一个单词或字母，而密码（cipher）则把信息转换为另一形式。密码分为两类：替代和换位。

18.1.1　替代密码

替代密码是指用一个字或符号代替另一个字。这已经不是一个新鲜的概念，而且它也不仅

仅用于隐藏信息。摩尔斯电码和旗语（用旗帜传达信息）就是替代密码的两个例子。一种最早的用来隐藏原始信息的替代密码叫做凯撒密码。这种密码很简单，只是用每个字母后面的第三个字母代替它，因此，字母 A应该用D代替，B被E取代以此类推。那么字母表中最后三个怎么呢？X用A代替，Y用B代替，C取代Z。一种类似的在 Unix操作系统使用的加密方法是一个称为ROTB的程序，其方法是将英语字母转换成数字（ A=1，B=2，……），再加上B后转换成英文。即用一个字母后面的第十三个字母代替它。这种技术的长处是将密码还原很容易，因为整个过程都是循环往复地使用字母表。

但是，对于任何一种基于此类循环的简单替代密码都存在着一个问题，那就是容易被破译。一种能增加复杂性的改进方案就是建立一个随意次序的字母表从而完成替代。下面就是一个这样的例子。

zaqxswcdevfrbgtnhymjukilop
abcdefghijklmnopqrstuvwxyz

在这种次序下，单词“ convergence ”应该转换成“ qtgksycsgqs ”。尽管这种方法比字母表简单循环稍微好一些，其缺点还是存在于其中。某些字母使用频率多于其他字母，比如说，在英语中，字母e、t、r和n是四个最常用的，而字母 z、j、q和x则用得最少。在单词“ convergence ”的转换形式中，字母“ S ”出现了三次，而字母“ G ”和“ Q ”都出现了两次。破解密码的人通常会想到将“ S ”替换成“ E ”（因为这是在英语中最常用的字母），然后试图找出“ t ”,“ r ”,“ n ”与“ g ”和“ q ”之间的联系。通过这种方法，这个被替代的单词最终可以确定下来。如果被替代的不仅是一个单词而是大量信息，这个破译方法就变得更加容易。很明显，使用这种过于简单的密码不足以达到安全隐藏信息的要求。

凯撒密码的另外一种改进形式是利用一种叫做 Vigenere表的字母表（见图表 18-1）。选中一个单词（比如“ convergence ”），称之为密钥，也称关键字，这个单词被重复地首尾连接并置于每行需要加密的正文上方。密钥单词中每一个字母决定使用表中的哪一行来替代正文字母。例如，如短语“ four score and seven years ago ”需要以密钥“ convergence ”加密，会产生如下结果：

convergenceconvergencecon	重复的密钥
fourscoreandsevenyearsago	正文
hchlwtuvrcrfgrqieeintwcub	密文

经过这种技术处理后，如果去计算每个字母的使用频率然后用英语中具有相近使用频率的单词去代替它不会得到正确答案。在这个例子中，密文前面三个字母中有两个“ h ”，第一个代表“ c ”而第二个代表“ n ”。这个例子显示了基于字母频率的简单替代的不足之处。

尽管使用一个密钥和 Vigenere表能够大大增加破译这种密码的复杂性，但破译并不是不可能的。如果一个人试图破译它，首先要做的是猜测这个密钥的长度，然后根据所猜密钥的长度把密文中的字母分组，这样每组字母的频率分布就和英语中字母频率分布相匹配了。例如，如果密钥的正确长度被猜中，这些字母就会被这样分组：

convergence
hchlwtuvrcr

fgrqieeintw

cub

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

图18-1 Vigenere表

如果有足够长的密文，每一栏就会产生一个与英语中频率分布相近的频率分布，根据这些，加密信息就有可能被破解。

最后，关于替代密码还必须做一些补充说明。很明显，密文和密钥的长度在这种方法中很重要。如果这个密钥甚至比需要加密正文还要长，这组密码就无法破译。因为任意顺序都有可能被采用，就没有办法知道哪种是正确的。一种叫做一次填充的方法采用了这种技术的长处。这个填充密码包含着一系列任意字母，它们被用来给信息加密。填充密码每段的长度必须比所要加密信息更长。如果每段只用一次就被抛弃，那么密文就变成了很多组无法破译的信息。然而，这种方法的弱点就在于填充密码本身。一旦填充密码丢失或被盗，谁也无法解开密码。还有一种情况是，如果情报接收者在翻译密码的时候，不小心忘记撕掉前面已用过密码或一次撕掉过多的密码，这个密文同样将不能破译。

18.1.2 换位密码

替代密码是把一个字用另一个字或符号代替，而换位密码则是把这些字重新整理成一个新顺序。字还是原来的字，只是没有在原来的顺序上。很容易解释，之所以要采用换位密码是因

为密文本身字母使用频率最终还是和英语中字母出现频率相同，意味着“ e ”总是出现得最多，然后是“ t ”,“ r ”…。历史上早期使用换位密码的一个例子是把一张长纸条缠绕在一根木棍上，然后在木棍上横着写一条消息，当纸条从棍子上展开时，这些字母就会出现在一个改变的位置上，只有拥有一根同样直径的木棍的人才能解读上面的消息。

最简单的使用换位密码的例子是简单地把消息倒过来写。上面的例子会以下面形式出现：

ogasraeynevesdnaerocsruof

另一个简单的改变形式是将字母放在一个竖栏里，然后用一种不同顺序“ 打开 ”它们。

例如，如果前面那条消息被安排在一个竖栏里，然后从顶上那个字的最右边的字母按顺时针展开，就会出现如下密文：

fours
corea
ndsev
enyea
rsago
savaogasrencfoureeeyndors

这种换了位的密文看起来仅仅是一组按任意顺序排列的字母，虽然它的字母出现频率和英语中一样，但是在正确顺序知道之前，一切尝试都可能是徒劳的。

一个有趣的方法是把替代和移位两种方法联系起来，这样就会出现不但字母使用频率不同于正常英语，而且猜测密钥长度的方法也无能为力的情况。在数字化通信中，这两种方法都被频繁地采用，形成了各种复杂的加密技术。

18.2 对称加密法

最基本的数据加密技术使用一个密钥加密同时也用来解密。原始信息一般被称为原文，被加密的正文叫做密文，密钥是一系列的排列、计算以及换位变化从而形成加密算法。一个简单的例子是利用一个密钥以及异或运算 XOR（即给定两个二进制位如果其中一个为 1，但两者不全为1，它们相加则产生一个 1）。例如，下列代表一部分二进制信息，密钥为 1001。下面是加密过程：

1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 重复的密钥
1 1 1 1 0 0 0 0 1 0 1 0 0 1 0 1 0 0 0 0 原文（将进行异或运算）
0 1 1 0 1 0 0 1 0 0 1 1 1 1 0 0 1 0 0 1 密文

解密过程也是用同样方法，运用原来密钥得到原文：

1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 重复的密钥
0 1 1 0 1 0 0 1 0 0 1 1 1 1 0 0 1 0 0 1 密文（将进行异或运算）
1 1 1 1 0 0 0 0 1 0 1 0 0 1 0 1 0 0 0 0 原文

像这样用同一个密钥进行加密和解密称之为对称加密法。一次只转换原文中的一位字符的方案叫做流密码（stream cipher），而每次把成批原文字符转换成密文的方案就叫块密码（ block cipher）。像上面这样基于字符的例子，密钥的长度是加密强度的关键所在：密钥越长，破译密

文就越困难。

一种最常用的对称加密法称为 DES（数据加密标准），许多年来它都作为加密的实际标准。DES运用一个64位密钥（其中56位参与运算，8位用于错误检测）给成批64位字加密。这组字符然后经过一系列互换，移位以及16次替换，最后得到密文。

多年以来，DES规则都被认为是加密数据的一种很可靠的方法。但是在90年代末，RSA数据安全有限公司——RSA加密法的拥有者（RSA以其开发者Ron Rivest, Adi Shamir，以及Leonard Adleman命名）——发起了一起用最短时间破译DES加密文件的竞赛。在1997年，一支大学生队伍用90天时间解开了这条信息（用强制“猜测”决定这个正确的密钥），几个月之后在另一场类似的比赛中，22,000个志愿者仅用了39天就解决了这个问题。再一次，在几个月之后的1998年，又有一个队伍打破了上次的记录，他们设计了一个专门用于破译这种密码的平台（被称为 DES破译者），用这个平台去决定正确的密钥仅用56小时。在这种情况下DES似乎走到了灭亡的尽头。然而事情并不是这样，通过增加密钥长度以及多次反复加密，这种加密法又被加强了（见图18-2），这种改进型的方法被称之为三重 DES（3DES），它现在仍然广泛地使用着。如下面图表所示，它使用了三个不同的密钥（有些情况下只有两个，即在第三步时仍使用第一步的密钥）。其解密过程是加密的颠倒，解密还是用同样的密钥，但使用的顺序相反。

图18-2 3重DES加密法

不论使用哪种对称加密法，都存在一个问题，那就是密钥管理。如果两者在加密情况下进行交流，他们必须都要知道密钥。因此，密钥的传送也是一个关键的问题，必须首先保证密钥的安全，否则别人一旦知道它，就有可能破译出加密的内容。对称加密法的另一个问题是，不同个体之间的交流必须使用不用的密钥，也就是说，若两个个体交流，他们可共享一个密钥；如果是三个个体，由于每两个需要一个那就需要三个密钥；以此类推，四者之间需要六个密钥，五者之间则要十个。很容易看出，如果很多个体进行交流，那么需要相当多的密钥，这也是一件麻烦事。这两个问题促使了必须要开发一种完全不同的方法进行加密和解密。这种方法就叫做非对称性加密，也称之为公共密钥加密法，这种方法现在已经得到越来越多的支持并开始流行。

18.3 公共密钥加密法

公共密钥加密方案的基本前提就是每个用户拥有一对密钥——一个公共的，一个私有的，公共密钥可以向外公开，事实上所有想跟这个密钥拥有者在安全形式下进行交流的个体都应该知道它。其他的人知道这个密钥也没关系，因为加密交流的过程已经发生变化。如果要给某人发送一条信息，只要用他的公共密钥加密即可，但是解密必须用他的私有密钥，当然，只有那些公共密钥被用来加密的个体才知道相应的私有密钥，这就能够保证只有信息接受者才能解读这些信息。公共密钥加密的一个重要特点，就是根据公共密钥是不能推断出相应私有密钥的。公共密钥加密的过程描述如下图：