14.3.2 建立共享密钥

对称密钥加密技术的缺点之一就是发送者和接收者在互相对话之前，一定要有一个共享的保密密钥。

如果想要与 Joe 的五金商店进行保密的对话，可能是在看了公共电视台的家装节目之后，想要订购一些木工工具，那么在安全地订购任何东西之前，要先在你和 www.joes-hardware.com 之间建立一个私有的保密密钥。你需要一种产生保密密钥并将其记住的方式。你和 Joe 的五金商店，以及因特网上所有其他人，都要产生并记住数千个密钥。

比如 Alice（A）、Bob（B）和 Chris（C）都想与 Joe 的五金商店（J）对话。A、B 和 C 都要建立自己与 J 之间的保密密钥。A 可能需要密钥 K^{AJ}，B 可能需要密钥 K^{BJ}，C 可能需要密钥 K^{CJ}。每对通信实体都需要自己的私有密钥。如果有 N 个节点，每个节点都要和其他所有 N-1 个节点进行安全对话，总共大概会有 N^2 个保密密钥：这将是一个管理噩梦。

14.4 公开密钥加密技术

公开密钥加密技术没有为每对主机使用单独的加密 / 解密密钥，而是使用了两个非对称密钥：一个用来对主机报文编码，另一个用来对主机报文解码。编码密钥是众所周知的（这也是公开密钥加密这个名字的由来），但只有主机才知道私有的解密密钥（参见图 14-8）。这样，每个人都能找到某个特定主机的公开密钥，密钥的建立变得更加简单。但解码密钥是保密的，因此只有接收端才能对发送给它的报文进行解码。

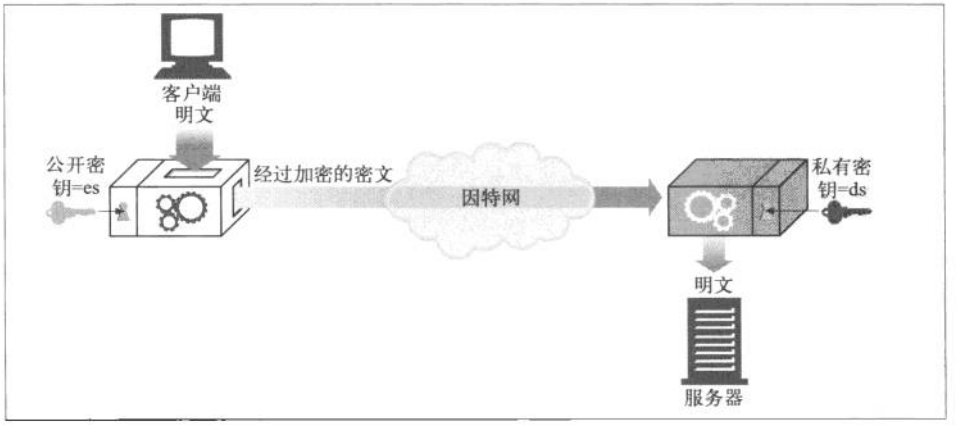

图 14-8 公开密钥加密技术是非对称的，为编码和解码使用了不同的密钥