这些问题。

SSL 经常用来为发生在 HTTP 之上的事务提供安全性。然而，因为 SSL 使 TCP 安全了，因此它能被应用于运行在 TCP 之上的任何应用程序。SSL 提供了一个简单的具有套接字的应用编程接口（API），该接口类似于 TCP 的 API。当一个应用程序要使用 SSL 时，它包括了 SSL 类/库。如在图 8-24 中所示，尽管 SSL 技术上位于应用层中，但从研发者的角度看，它是一个提供 TCP 服务的运输协议，而这里的 TCP 服务用安全性服务加强了。

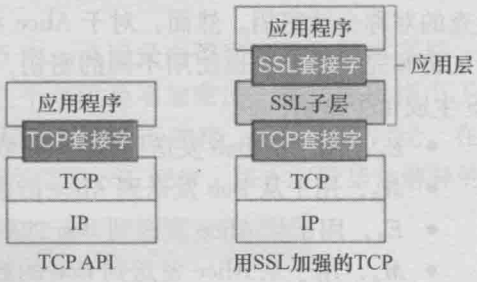

图 8-24 尽管 SSL 技术上位于应用层中，但从研发者的角度看它是一个运输协议

8.6.1 宏观描述

我们从描述一个简化的 SSL 版本开始，这将使我们从宏观上理解 SSL 的工作原理和工作过程。我们将这个 SSL 的简化版本称之为“类 SSL”。描述过类 SSL 之后，在下一小节中我们将描述真实的 SSL，填充细节。类 SSL（和 SSL）具有三个阶段：握手、密钥导出和数据传输。我们现在描述针对一个客户（Bob）和一个服务器（Alice）之间的通信会话的这三个阶段，其中 Alice 具有私钥/公钥对和将她的身份与其公钥绑定的证书。

1. 握手

在握手阶段，Bob 需要：①与 Alice 创建一条 TCP 连接；②验证 Alice 是真实的 Alice；③发送给 Alice 一个主密钥，Bob 和 Alice 持用该主密钥生成 SSL 会话所需的所有对称密钥。这三个步骤显示在图 8-25 中。注意到一旦创建了 TCP 连接，Bob 就向 Alice 发送一个 hello 报文。Alice 则用她的证书进行响应，证书中包含了她的公钥。如在 8.3 节所讨论，因为该证书已被某 CA 证实过，Bob 明白无误地知道该公钥属于 Alice。然后，Bob 产生一个主密钥（MS）（该 MS 将仅用于这个 SSL 会话），用 Alice 的公钥加密该 MS 以生成加密的主密钥（EMS），并将该 EMS 发送给 Alice。Alice 用她的私钥解密该 EMS 从而得到该 MS。在这个阶段后，Bob 和 Alice（而无别的人）均知道了用于这次 SSL 会话的主密钥。

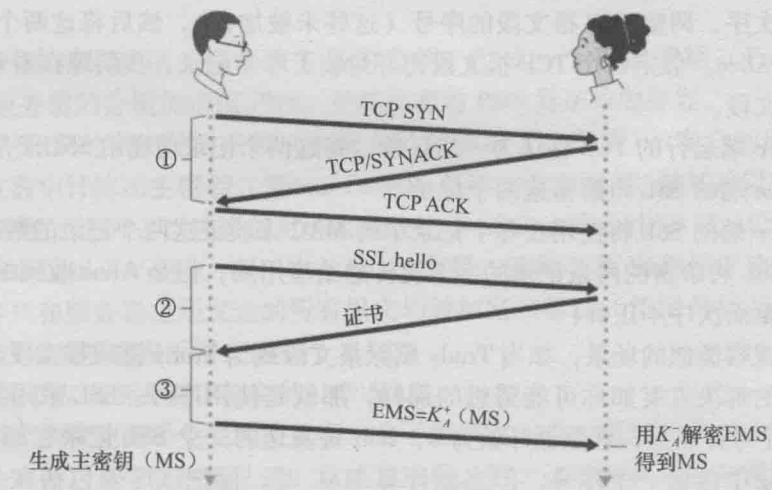

图 8-25 类 SSL 握手，首先建立一个 TCP 连接