SSL 的输入 / 输出调用取代 TCP 的调用，再增加其他几个调用来配置和管理安全信息就行了。

14.2 数字加密

在详细探讨 HTTPS 之前，我们先介绍一些 SSL 和 HTTPS 用到的加密编码技术的背景知识。在接下来的几节里，我们会对数字加密的本质进行一个快速的入门性介绍。如果你已经掌握了数字加密的技术和术语，可以直接阅读 14.7 节。

在这个数字加密技术的入门介绍中，我们会讨论以下内容。

- *密码*

对文本进行编码，使偷窥者无法识别的算法。

- *密钥*

改变密码行为的数字化参数。

- *对称密钥加密系统*

编 / 解码使用相同密钥的算法。

- *不对称密钥加密系统*

编 / 解码使用不同密钥的算法。

- *公开密钥加密系统*

一种能够使数百万计算机便捷地发送机密报文的系统。

- *数字签名*

用来验证报文未被伪造或篡改的校验和。

- *数字证书*

309 由一个可信的组织验证和签发的识别信息。

14.2.1 密码编制的机制与技巧

密码学是对报文进行编 / 解码的机制与技巧。人们用加密的方式来发送秘密信息已经有数千年了。但密码学所能做的还不仅仅是加密报文以防止好事者的读取，我们还可以用它来防止对报文的篡改，甚至还可以用密码学来证明某条报文或某个事务确实出自你手，就像支票上的手写签名或信封上的压纹封蜡一样。