14.2.1 密码编制的机制与技巧……326
14.2.2 密码……327
14.2.3 密码机……328
14.2.4 使用了密钥的密码……328
14.2.5 数字密码……328
14.3 对称密钥加密技术……330
14.3.1 密钥长度与枚举攻击……330
14.3.2 建立共享密钥……332
14.4 公开密钥加密技术……332
14.4.1 RSA……333
14.4.2 混合加密系统和会话密钥……334
14.5 数字签名……334
14.6 数字证书……336
14.6.1 证书的主要内容……336
14.6.2 X.509 v3 证书……337
14.6.3 用证书对服务器进行认证……338
14.7 HTTPS——细节介绍……339
14.7.1 HTTPS 概述……339
14.7.2 HTTPS 方案……340
14.7.3 建立安全传输……341
14.7.4 SSL 握手……341
14.7.5 服务器证书……343
14.7.6 站点证书的有效性……344
14.7.7 虚拟主机与证书……345
14.8 HTTPS 客户端实例……345
14.8.1 OpenSSL……346
14.8.2 简单的 HTTPS 客户端……347
14.8.3 执行 OpenSSL 客户端……350
14.9 通过代理以隧道形式传输安全流量……351
14.10 更多信息……353
14.10.1 HTTP 安全性……353
14.10.2 SSL 与 TLS……353
14.10.3 公开密钥基础设施……354
14.10.4 数字密码……354

第四部分 实体、编码和国际化

第 15 章 实体和编码……357

15.1 报文是箱子，实体是货物……359
15.2 Content-Length：实体的大小……361