据他们自己的机构需求，通过修改现有的特征或通过创建全新的特征来裁剪某个特征。

8.10 小结

在本章中，我们考察了秘密情人 Bob 和 Alice 能够用于安全通信的各种机制。我们看到 Bob 和 Alice 对下列因素感兴趣：机密性（因此只有他们才能理解传输的报文内容）、端点鉴别（因此他们确信正在与对方交谈）和报文完整性（因此他们确信在传输过程中他们的报文未被篡改）。当然，安全通信的需求并不限于秘密情人。的确，我们在 8.5 ~ 8.8 节中看到，可以在网络体系结构中的各个层次使用安全性，使之免受采用各种各样攻击手段的“坏家伙”的侵扰。

本章前面部分给出了安全通信所依赖的各种原理。在 8.2 节中，我们涉及了加密和解密数据的密码技术，包括对称密钥密码和公开密钥密码。作为今天网络中两种重要的密码技术的特定的学习案例，我们考察了 DES 和 RSA。

在 8.3 节中，我们研究了提供报文完整性的两种方法：报文鉴别码（MAC）和数字签名。这两种方法有一些共同之处。它们都使用了密码散列函数，这两种技术都使我们能够验证报文的源以及报文自身的完整性。一个重要的差异是 MAC 不依赖于加密，而数字签名要求公钥基础设施。如我们在 8.5 ~ 8.8 节所见，这两种技术广泛在实际中都得到了广泛应用。此外，数字签名用于生成数字证书，数字证书对于证实公钥的合法性是重要的。在 8.4 节中，我们考察了端点鉴别并引入了不重数以防御重放攻击。

在 8.5 ~ 8.8 节中，我们研究了几种在实践中得到广泛使用的安全性网络协议。我们看到了对称密钥密码在 PGP、SSL、IPsec 和无线安全性中的核心地位。我们看到了公开密钥密码对 PGP 和 SSL 是至关重要的。我们看到 PGP 使用数字签名而 SSL 和 IPsec 使用 MAC 来保证报文完整性。在目前理解了密码学的基本原理以及学习了这些原理的实际应用方法之后，你现在已经有能力设计你自己的安全网络协议了！

利用 8.2 ~ 8.4 节所包含的技术，Bob 和 Alice 就能够安全通信了。（只希望他们是学习了这些材料的网络专业学生，因此能够使他们的约会不会被 Trudy 发现！）而机密性仅是整个网络安全的一小部分。如我们在 8.9 节中所学习，现在网络安全的焦点越来越多地关注网络基础设施的安全性，以防止“坏家伙”的潜在猛烈攻击。在本章的后面部分，我们因此学习了防火墙和 IDS 系统，它们检查进入和离开一个机构网络的分组。

本章已经涉及了许多基础性问题，同时关注了现代网络安全性中最为重要的主题。希望深入钻研的读者最好研究本章中引用的文献。特别是，我们推荐以下读物：关于攻击和运行安全性的［Skoudis 2006］，关于密码学及其如何应用于网络安全的［Kaufman 1995］，关于 SSL 处理的有深度且可读性强的［Rescorla 2001］，以及透彻地讨论 802.11 安全性的［Edney 2003］（其中包括对 WEP 及其缺陷的深入研究）。

课后习题和问题

复习题

8.1 节

R1. 报文机密性和报文完整性之间的区别是什么？你能具有机密性而没有完整性吗？你能具有完整性而