如我们将看到的那样，除非采取适当的措施，否则上述能力使入侵者可以用多种方式发动各种各样的安全攻击：窃听通信内容（可能窃取口令和数据），假冒另一个实体，“劫持”一个正在进行的会话，通过使系统资源过载拒绝合法网络用户的服务请求等等。CERT 协调中心对已报道的攻击进行了总结［CERT 2012］。

已经知道在因特网中某处的确存在真实的威胁，则 Alice 和 Bob（我们的两个需要安全通信的朋友）在因特网上的对应实体是什么呢？当然，Alice 和 Bob 可以是位于两个端系统的人类用户，例如，真实的 Alice 和真实的 Bob 真的需要交换安全电子邮件。他们也可以参与电子商务事务。例如，一个真实的 Bob 希望安全地向一台 Web 服务器传输他的信用卡号码，以在线购买商品。类似地，真实的 Alice 要与银行在线交互。需要安全通信的各方自身也可能是网络基础设施的一部分。前面讲过，域名系统（DNS，参见 2.5 节）或交换路由选择信息的路由选择守护程序（参见 4.6 节）需要在两方之间安全通信。对于网络管理应用也有相同的情况，网络管理是第 9 章学习的主题。能主动干扰 DNS 查找和更新（如在 2.5 节中讨论的那样）、路由选择计算［RFC 4272］或网络管理功能［RFC 3414］的入侵者能够给因特网造成不可估量的破坏。

建立了上述框架，明确了一些重要定义以及网络安全需求之后，我们将深入学习密码学。应用密码学来提供机密性是不言而喻的，同时我们很快将看到它对于提供端点鉴别、报文完整性也起到了核心作用，这使得密码学成为网络安全的基石。

8.2 密码学的原则

尽管密码学的漫长历史可以追溯到朱利叶斯·凯撒（Julius Caesar）时代，但现代密码技术（包括正在今天的因特网中应用的许多技术）基于的是过去 30 年所取得的进展。Kahn 的著作《破译者（The Codebreakers）》（［Kahn 1967］和 Singh 的著作《编码技术：保密的科学——从古埃及到量子密码（The Code Book：The Science of Secrecy from Ancient Egypt to Quantum Cryptography）》［Singh 1999］回顾了引人入胜的密码学的悠久历史。对密码学全面的讨论需要一本完整的书［Kaufman 1995；Schneier 1995］，所以我们只能初步了解密码学的基本方面，特别是因为这些东西正在今天的因特网上发挥作用。我们也注意到尽管本节的重点是密码学在机密性方面的应用，但我们将很快看到密码学技术与鉴别、报文完整性和不可否认性等是紧密相关的。

密码技术使得发送方可以伪装数据，使入侵者不能从截取到的数据中获得任何信息。当然，接收方必须能够从伪装的数据中恢复出初始数据。图 8-2 说明了一些重要的术语。

现在假设 Alice 要向 Bob 发送一个报文。Alice 报文的最初形式（例如，“Bob，I love you. Alice”）被称为**明文**（plaintext，cleartext）。Alice 使用**加密算法**（encryption algorithm）加密其明文报文，生成的加密报文被称为**密文**（ciphertext），该密文对任何入侵者看起来是不可懂的。有趣的是在许多现代密码系统中，包括因特网上所使用的那些，加密技术本身是已知的，即公开发行的、标准化的和任何人都可使用的（例如［RFC 1321；RFC 3447；RFC 2420；NIST 2001］），即使对潜在的入侵者也是如此！显然，如果任何人都知道数据编码的方法，则一定有一些秘密信息可以阻止入侵者解密被传输的数据。这些秘密信息就是密钥。