件报文）并核对该数字签名。通过这种方式，Alice 确信是 Bob 而不是某些青少年恶作剧者下的比萨订单。

在聪明的 Trudy 出现之前，这一切看起来进行得相当好。如在图 8-13 中所示，Trudy 沉溺于一场恶作剧中。Trudy 向 Alice 发送一个报文，在这个报文中她说她是 Bob，给出了 Bob 家的地址并订购了一个比萨。在这个报文中，她也包括了她（Trudy）的公钥，虽然 Alice 自然地假定它就是 Bob 的公钥。Trudy 也附加了一个签名，但是这是用她自己（Trudy）的私钥生成的。在收到该报文后，Alice 就会用 Trudy 的公钥（Alice 认为它是 Bob 的公钥）来解密该数字签名，并得到结论：这个明文报文确实是由 Bob 生成的。而当外送人员带着具有意大利辣香肠和凤尾鱼的比萨到达 Bob 家时，他会感到非常惊讶！

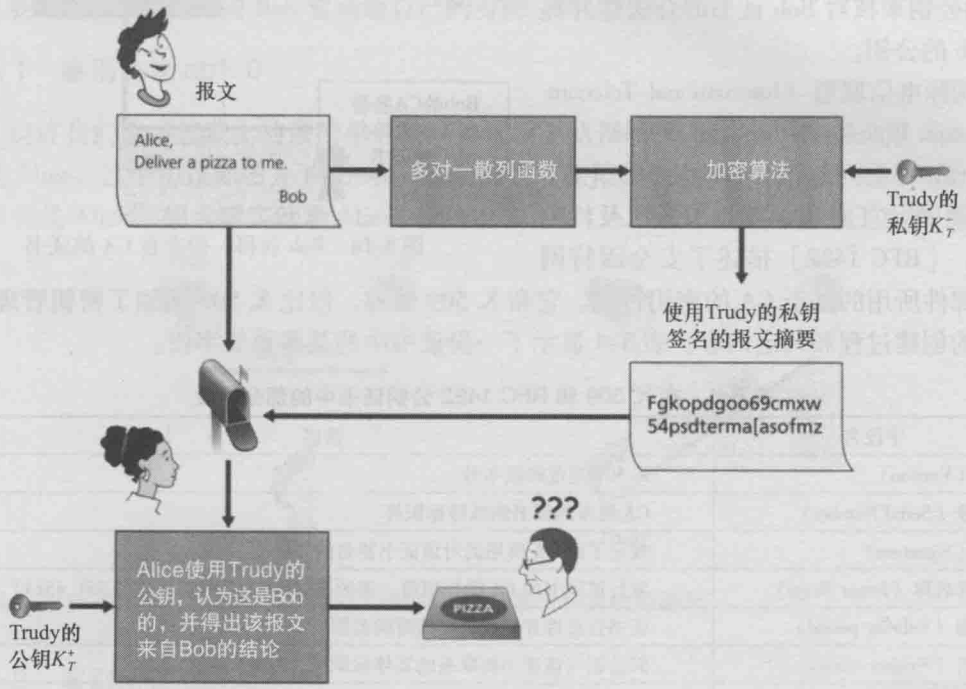

图 8-13　Trudy 用公钥密码冒充 Bob

从这个例子我们看到，要使公钥密码有用，需要能够证实你具有的公钥实际上就是与你要进行通信的实体（人员、路由器、浏览器等）的公钥。例如，当 Alice 与 Bob 使用公钥密码通信时，她需要证实她假定是 Bob 的那个公钥确实就是 Bob 的公钥。

将公钥与特定实体绑定通常是由**认证中心**（Certification Authority，CA）完成的，CA 的职责就是使识别和发行证书合法化。CA 具有下列作用：

1）CA 证实一个实体（一个人、一台路由器等）的真实身份。如何进行认证并没有强制的过程。当与一个 CA 打交道时，一方必须信任这个 CA 能够执行适当的严格身份验证。例如，如果 Trudy 可以走进名为 Fly-by-Night 的证书权威机构并只是宣称“我是 Alice”，就可以得到该机构颁发的与 Alice 的身份相关联证书的话，则人们不会对 Fly-by-Night 证书权威机构所签发的公钥证书有太多的信任。在另一方面，人们可能愿意（或不愿意!）信任某个 CA，如果这个 CA 是联邦或州计划的一部分的话。你对与公钥相联系的身份的信任程度，仅能达到你对 CA 及其身份验证技术的信任程度。我们编织了多么混乱