把这个预备包看作一个报文，再用图 8-19 中的发送方的步骤发送这个新报文，即生成一个新包发给 Bob。Alice 所做的这些步骤如图 8-21 所示。当 Bob 接收到这个包后，他首先应用图 8-19 中他这一侧的步骤，然后再应用图 8-20 中他这一侧的步骤。应当明确这一设计的目标是提供机密性、发送方鉴别和报文完整性。注意到在这一方案中，Alice 两次使用了公开密钥密码：一次用了她的私钥，另一次用了 Bob 的公钥。同样，Bob 也两次使用了公开密钥密码：一次用了他的私钥，一次用了 Alice 的公钥。

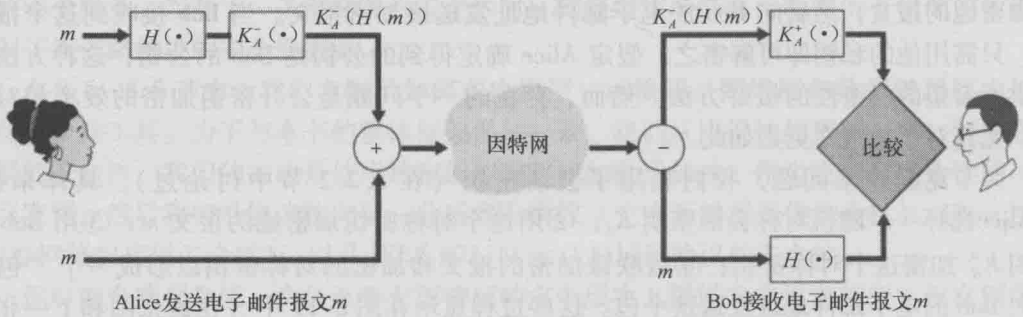

图 8-20 使用散列函数和数字签名来提供发送方鉴别和报文完整性

图 8-21 所示的安全电子邮件系统可能在大多数情况下都能为大多数电子邮件用户提供满意的安全性。但是仍有一个重要的问题没有解决。图 8-21 中的设计要求 Alice 获得 Bob 的公钥，也要求 Bob 获得 Alice 的公钥。但这些公钥的分发并不是一个小问题。例如，Trudy 可能假冒 Bob，发给 Alice 她自己的公钥，并告诉 Alice 这个公钥是 Bob 的公钥，使得 Trudy 就能接收到 Alice 发给 Bob 的报文。如我们在 8.3 节所学，安全地分发公钥的一种常用方法是通过 CA 验证该公钥。

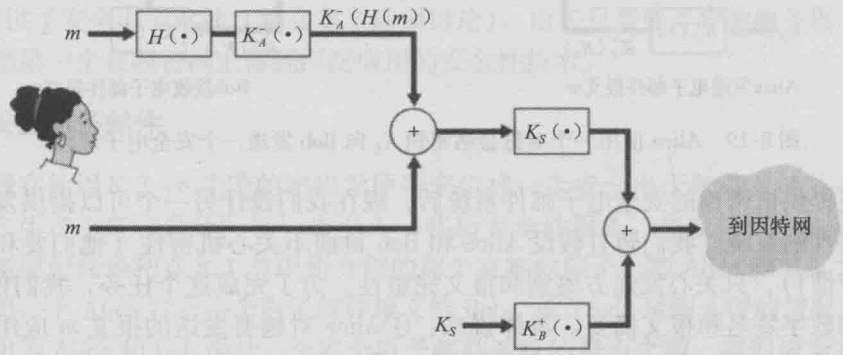

图 8-21 Alice 使用对称密钥密码、公开密钥密码、散列函数和数字签名来提供安全性、发送方鉴别和报文完整性

历史事件

Philip Zimmermann 和 PGP

Philip R. Zimmermann 是 PGP（Pretty Good Privacy）的创造者。他因此在长达三年的时间里成为犯罪调查的目标，因为美国政府认为在 1991 年以后的时间里，PGP 在世界范围内以免费软件形式发布，违反了美国对加密软件出口的限制。在 PGP 作为共享软件