发该秘密鉴别密钥。(注意到所有路由器能够都使用相同的鉴别密钥。)一名网络管理员能够通过物理上访问每台路由器来实际完成这项工作。或者,如果这名网络管理员不够勤快,并且如果每台路由器都有它自己的公钥,那么该网络管理员能够用路由器的公钥加密该鉴别密钥并分发给任何一台路由器,从而通过网络向路由器发送加密的密钥。

8.3.3 数字签名

回想在过去的一周中,你在纸上已经签过多少次你的名字?你可能经常会在支票、信用卡收据、法律文件和信件上签名。你的签名证明你(而不是其他人)承认和/或同意这些文件的内容。在数字领域,人们通常需要指出一个文件的所有者或创作者,或者表明某人认可一个文件内容。**数字签名**(digital signature)就是在数字领域实现这些目标的一种密码技术。

正如人手签字一样,数字签名也应当以可鉴别的、不可伪造的方式进行。这就是说,必须能够证明由某个人在一个文档上的签名确实是由该人签署的(该签名必须是可证实的),且只有那个人能够签署那个文件(该签名无法伪造)。

我们现在来考虑怎样设计一个数字签名方案。当 Bob 签署一个报文时,可以观察到 Bob 必须将某些对他是独特的东西放置在该报文上。Bob 能够考虑附加一个 MAC 用作签名,其中 MAC 是由他的密钥(对他是独特的)作用到该报文上而生成的,然后得到该散列值。而 Alice 为了验证该签名,她必须也具有该密钥的副本,在这种情况下该密钥对 Bob 将不是唯一的。因此,此时 MAC 是无法胜任这项工作的。

前面讲过使用公钥密码,Bob 具有公钥和私钥,这两种密钥对 Bob 均为独特的。因此,公钥密钥是一种提供数字签名的优秀候选者。我们现在来研究一下这是怎样完成的。

假设 Bob 要以数字方式签署一个文档 m。我们能够想象这个文档是 Bob 打算签署并发送的一个文件或一个报文。如图 8-10 所示,为了签署这个文档,Bob 直接使用他的私钥 K_B^- 计算 $K_B^-(m)$。乍一看,会感觉很奇怪,Bob 怎么会用他的私钥(在 8.2 节中,我们用私钥解密用其公钥加密的报文)签署文档!但是回想加密和解密都只不过是数学运算而已(RSA 中所做的 e 或 d 指数幂运算;参见 8.2 节),并且 Bob 的目的不是弄乱或掩盖文档的内容,而只是要以可鉴别的、不可伪造的方式签署这个文档。Bob 对文档 m 签名之后所得的文档就是 $K_B^-(m)$。

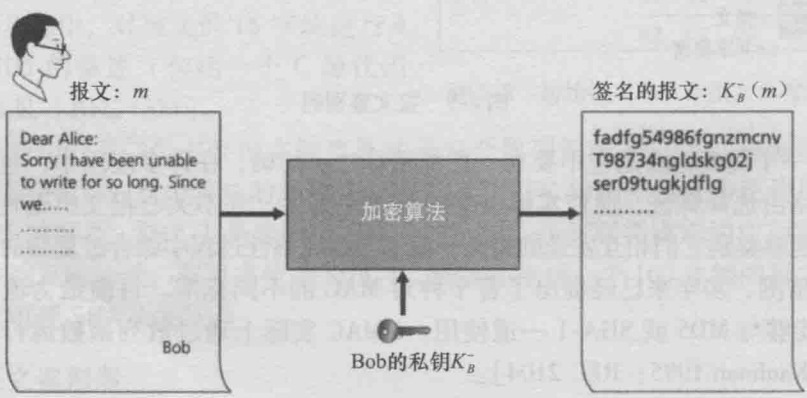

图 8-10 对一个文档生成一个数据签名