执行报文完整性：

1）Alice 生成报文 $m$ 并计算散列 $H(m)$（例如使用 SHA-1）。

2）Alice 则将 $H(m)$ 附加到报文 $m$ 上，生成一个扩展报文（$m$，$H(m)$），并将该扩展报文发给 Bob。

3）Bob 接收到一个扩展报文（$m$，$h$）并计算 $H(m)$。如果 $H(m)=h$，Bob 得到结论：一切正常。

这种方法存在明显缺陷。Trudy 能够生成虚假报文 $m'$，在其中声称她就是 Alice，计算 $H(m')$ 并发送给 Bob（$m'$，$H(m')$）。当 Bob 接收到该报文，一切将在步骤 3 中核对通过，并且 Bob 无法猜出这种不轨的行为。

为了执行报文完整性，除了使用密码散列函数，Alice 和 Bob 将需要共享秘密 $s$。这个共享的秘密只不过是一个比特串，它被称为**鉴别密钥**（authentication key）。使用这个共享秘密，报文完整性能够执行如下：

1）Alice 生成报文 $m$，用 $s$ 级联 $m$ 以生成 $m+s$，并计算散列 $H(m+s)$（例如使用 SHA-1）。$H(m+s)$ 被称为**报文鉴别码**（Message Authentication Code，MAC）。

2）Alice 则将 MAC 附加到报文 $m$ 上，生成扩展报文（$m$，$H(m+s)$），并将该扩展报文发送给 Bob。

3）Bob 接收到一个扩展报文（$m$，$h$），由于知道 $s$，计算出报文鉴别码 $H(m+s)$。如果 $H(m+s)=h$，Bob 得到结论：一切正常。

图 8-9 中显示了上述过程的总结。读者们应当注意到这里的 MAC（表示“报文鉴别码”）与用于数据链路层中的 MAC（表示“媒体访问控制”）是不一样的！

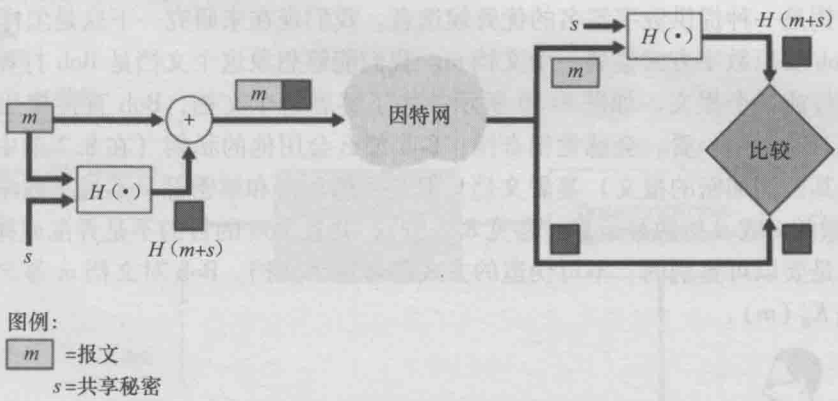


图 8-9 报文鉴别码

MAC 的一个优良特点是它不要求一种加密算法。的确，在许多应用中，包括前面讨论的链路状态路由选择算法，通信实体仅关心报文完整性，并不关心报文机密性。使用一个 MAC，实体能够鉴别它们相互发送的报文，而不必在完整性过程中综合进复杂的加密过程。

如你所猜测，多年来已经提出了若干种对 MAC 的不同标准。目前最为流行的标准是 HMAC，它能够与 MD5 或 SHA-1 一道使用。HMAC 实际上通过散列函数运行数据和鉴别密钥两次［Kaufman 1995；RFC 2104］。

这里还遗留下一个重要问题。我们怎样向通信实体分发这个共享的鉴别密钥呢？例如，在链路状态路由选择算法中，我们将在某种程度上需要向自治系统中的每台路由器分