密钥技术（如 DES 或 AES）加密所要传输的报文，而 Bob 则在接收时对报文解密。如 8.2 节讨论的那样，如果对称密钥足够长，且仅有 Alice 和 Bob 拥有该密钥，则其他人（包括 Trudy）要想读懂这条报文极为困难。尽管这种方法直截了当，但因为仅有 Alice 和 Bob 具有该密钥的副本，这使得分发对称密钥非常困难（我们在 8.2 节中讨论过）。因此我们自然就考虑用其他方法——公开密钥密码（例如使用 RSA）。在公开密钥方法中，Bob 使得他的公钥为公众所用（例如，从一台公钥服务器或其个人网页上得到），Alice 用 Bob 的公钥加密她的报文，然后向 Bob 的电子邮件地址发送该加密报文。当 Bob 接收到这个报文时，只需用他的私钥即可解密之。假定 Alice 确定得到的公钥是 Bob 的公钥，这种方法是提供所希望的机密性的极好方法。然而，存在的一个问题是公开密钥加密的效率相对低下，尤其对于长报文更是如此。

为了克服效率问题，我们利用了会话密钥（在 8.2.2 节中讨论过）。具体来说：①Alice选择一个随机对称会话密钥 K_S；②用这个对称密钥加密她的报文 m；③用 Bob 的公钥 K_B^+ 加密这个对称密钥；④级联该加密的报文和加密的对称密钥以形成一个“包”；⑤向 Bob 的电子邮件地址发送这个包。这些过程显示在图 8-19 中（在这张图和下一张图中，带圈的“+”表示级联，带圈的“-”表示级联的分解）。当 Bob 接收到这个包时：①他使用其私钥 K_B^- 得到对称密钥 K_S；②使用这个对称密钥 K_S 解密报文 m。

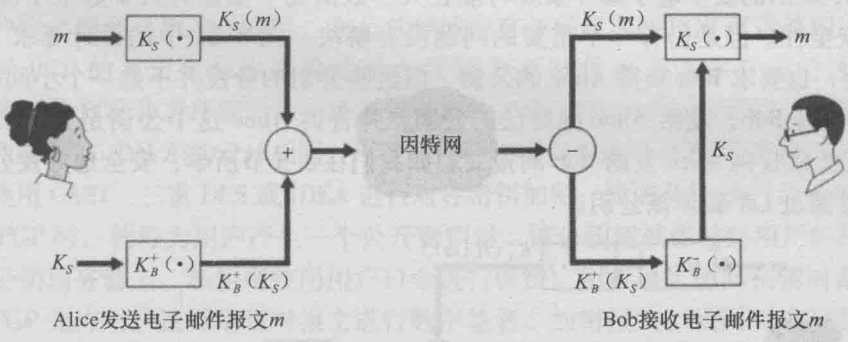

图 8-19 Alice 使用一个对称会话密钥 K_S 向 Bob 发送一个安全电子邮件

设计完提供机密性的安全电子邮件系统后，现在我们设计另一个可以提供发送方鉴别和报文完整性的系统。我们暂且假设 Alice 和 Bob 目前不关心机密性（他们要和其他人分享他们的爱情!），只关心发送方鉴别和报文完整性。为了完成这个任务，我们使用如 8.3 节所描述的数字签名和报文摘要。具体说来：①Alice 对她要发送的报文 m 应用一个散列函数 H（例如 MD5），从而得到一个报文摘要；②用她的私钥 K_A^- 对散列函数的结果进行签名，从而得到一个数字签名；③把初始报文（未加密）和该数字签名级联起来生成一个包；④向 Bob 的电子邮件地址发送这个包。当 Bob 接收到这个包时：①他将 Alice 的公钥 K_A^+ 应用到被签名的报文摘要上；②将该操作的结果与他自己对该报的散列 H 进行比较。在图 8-20 中阐述了这些步骤。如 8.3 节中所讨论，如果这两个结果相同，则 Bob 完全可以确信这个报文来自 Alice 且未被篡改。

现在我们考虑设计一个提供机密性、发送方鉴别和报文完整性的电子邮件系统。这可以通过把图 8-19 和图 8-20 中的过程结合起来而实现。Alice 首先生成一个预备包，它与图 8-20 中的包完全相同，其中包含她的初始报文和该报文数字签名过的散列。然后 Alice