在该端点的SAD中人工键入SA信息（加密/鉴别算法和密钥及SPI）。这样的“人工密钥法”对于一个大型VPN显然是不切实际的，因为大型VPN可能由成百甚至上千台IPsec路由器和主机组成。大型的、地理上分散的部署要求一个自动的机制来生成SA。IPsec使用**因特网密钥交换**（Internet Key Exchange，IKE）协议来从事这项工作，IKE由RFC 5996定义。

IKE与SSL（参见8.6节）中的握手具有某些类似。每个IPsec实体具有一个证书，该证书包括了该实体的公开密钥。如同使用SSL一样，IKE协议让两个实体交换证书，协商鉴别和加密算法，并安全地交换用于在IPsec SA中生成会话密钥的密钥材料。与SSL不同的是，IKE应用两个阶段来执行这些任务。

我们来研究图8-28中两台路由器R1和R2场景下的这两个阶段。第一个阶段由R1和R2之间报文对的两次交换组成：

- 在报文的第一次交换期间，两侧使用Diffie-Hellman（参见课后习题）在路由器之间生成一个双向的**IKE SA**。为了防止混淆，这个双向IKE SA完全不同于8.6.3节和8.6.4节所讨论的IPsec SA。该IKE SA在这两台路由器之间提供了一个鉴别的和加密的信道。在首个报文对交换期间，创建用于IKE SA的加密和鉴别的密钥。还创建了将用于计算后期在阶段2使用的IPsec SA密钥的一个主密钥。观察在第一步骤期间，没有使用RSA公钥和私钥。特别是，R1或R2都没有通过用它们的私钥对报文签字而泄露其身份。
- 在报文的第二次交换期间，两侧通过对其报文签名而透漏了它们的身份。然而，这些身份并未透漏给被动的嗅探者，因为这些报文是经过安全的IKE SA信道发送的。同时在这个阶段期间，两侧协商由IPsec SA应用的IPsec加密和鉴别算法。

在IKE的第二个阶段，两侧生成在每个方向的一个SA。在阶段2结束时，对这两个SA的每一侧都建立了加密和鉴别会话密钥。然后这两侧都能使用SA来发送安全的数据报，如同8.7.3节和8.7.4节描述的那样。在IKE中有两个阶段的基本动机是计算成本，即因为第二阶段并不涉及任何公钥密码，IKE能够以相对低的计算成本在两个IPsec实体之间生成大量SA。

8.8 使无线LAN安全

在无线网络中安全性是特别重要的关注因素，因为这时携带数据帧的无线电波可以传播到远离包含无线基站和主机的建筑物以外的地方。在本节中，我们简要介绍了无线安全性。对于更为深入地探讨，参见由Edney和Arbaugh撰写的可读性很强的书［Edney 2003］。

在802.11中的安全性问题受到了技术界和媒体界的极大关注。在进行大量讨论的同时，一个几乎没有争论的事实是，看起来被广泛认同的初始802.11规范具有一些严重的安全性缺陷。现在的确能够下载利用这些漏洞的公共域软件，使得那些使用该普通802.11安全性机制的用户面对安全性攻击，就像根本没有使用安全性措施的网络用户一样，门户洞开。

在下面一节中，我们讨论最初在802.11规范中标准化的安全性机制，该规范统称为**有线等效保密**（Wired Equivalent Privacy，WEP）。顾名思义，WEP意欲提供类似于在有线网络中的安全性水平。接下来我们将讨论WEP中的安全性漏洞并讨论802.11i标准，后者是在2004年采纳的802.11的本质上更为安全的版本。