1. 在下面的空格中填入“谁的什么密钥”：
2. A向B发送一个一次性会话密钥，A用 B的公钥 加密该会话密钥。
3. Certifier.com用 自己的私钥 为foo.com签发公钥证书。
4. A向B发送一个签名的报文，A用 自己的私钥 生成这个数字签名。
5. A向B发送一个可供鉴别的报文，A用 与B共享的密钥 生成报文鉴别码。
6. 在下面的空格中填入可实现相应安全服务的安全机制：

机密性 数据加密 完整性 报文鉴别

防抵赖 数字签名 防假冒 端点鉴别

1. 在下面的空格中填入需要用到的算法或函数的序号：①对称密钥算法，②公开密钥算法，③密码散列函数。（报文鉴别码写出一种方法即可）

生成数字签名 ②③ 数据加密 ①

生成报文鉴别码 ③① 或 ③ 加密会话密钥 ②

1. 是非判断题：
2. 一对主机通过IPSec运行TCP，封装重发的TCP包时，ESP头中的序号不同。

对

1. 一对主机通过IPSec传输分组流，对每个发送的分组都要创建一个新的SA。

错