1. 在下面的空格中填入“谁的什么密钥”：

（1） 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。

（2） Certifier.com 用 自己的私钥 为 foo.com 签发公钥证书。

（3） 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。

（4） 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（写出一种方法即可）。

2. 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

3. 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散列函数，④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 ③② 数据加密 ①

生成报文鉴别码 ③① 或 ④ 或 ③② 加密会话密钥 ②

4. 是非判断题：

1） 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

2） 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