密

封

线

C. 如果主体的身份对于某个消息的意义来说是必要的，那么应该谨慎处理主体的身份信息

D. 应清楚的知道协议使用加密的目的，因为加密不是一种简单的运算，他需要的计算量较大，不清楚加密的目的可能会导致冗余。而且加密不等于安全，不正确的使用加密会导致协议的错误

E. 如果主体对已加密的信息进行了签名操作，那么不能由此推断出主体知道该消息的内容。反之，如果主体对消息先签名然后再加密，那么可以推断出主体知道该消息的内容

得分	评卷人	复查人

三、名词解释 （每小题3分，共12分）

1. 信息

2. 站点认证

3. 虚拟专用网

4. 计算机犯罪

得分	评卷人	复查人

四、简答题 （每小题5分，共20分）

1. 什么是对称密码体制，其特点包括哪些？

2. DES 的 IP 与 IP^{-1} 作用是什么？

3. 证书存档的目的有哪些？

4. 简述今后入侵检测技术可能的发展方向。