1. 什么是数字签名？请给出一个采用公开密码技术进行数字签名的方案，写出发送方和接收方对消息处理的步骤。

2. IPv4 存在的缺陷体现在哪些方面？

3. 写出 4 种拒绝服务攻击（DoS）攻击方式及详细过程。

4. 下图是 ESP 协议的报文封装格式，请回答以下问题：

1）其中哪个字段可用于防范 IP 包的重发攻击？其原理是什么？

2）简述“安全参数引 SPI”的作用。

3）哪部分数据以密文的形式出现？

4）简单描述“认证数据”是如何计算出来的?

5. IPSec 的安全协议—— AH 为 IP 数据包提供什么安全服务？说明在 Ipv4 下 AH 的两种运行模式及包的封装方式。AH 与 NAT 会发生冲突，为什么？

6. 某公司需要通过 Internet 进行商务活动，要将自己的内部网与 Internet 相连接，内部网包括电子邮件服务器、文件服务器和数据库服务器，为了方便 B2B 业务，还要增加 Web 服务器和应用服务器。现在请你为之设计网络结构以及安全接入方案（结合防火墙等防御技术），请描述你采用的拓扑结构，说明每台服务器在网络中的位置，并且给出部署方案依据的原理。

7. 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。请写出发送方发送邮件以及接收方接收邮件的过程。

8. 假定 Alice 要与 Bob 使用一个会话密钥 KS 通信，请设计一个采用对称密钥体制解决会话密钥分发的方案。

9. 简述缓冲区溢出产生的原因。

10. 请简述基于误用检测和异常检测的 IDS 的工作原理。Snort 系统是基于什么检测原理的？

11. Netfilter/IPtable 是如何工作的？

12. HTTPS 是如何实现数据安全的？

13. windows 系统是如何实现访问控制的？

14 各信息安全风险因素之间的关系是怎样的？