1、填空题

（1）数据保密性可以分为**连接保密性**、**无连接保密性**、**选择字段保密性**、**通信业务流保密性**。

（2）IPSec的两种工作模式分别为**传输模式**、**隧道模式**。

（3）基于实体的安全体系结构中，安全属性包括：**标识属性**、**认证属性**、**访问控制属性**、**保密及完整性属性**。

（4）安全模型用于准确描述系统在和上的安全特性，它反映了一定的**安全策略**。

2、选择题（单选和多选）

（1）4.在7层OSI网络协议中，以下哪一层不能执行数据来源认证（**B**）

A.网络层；B.物理层；C.传输层；D.应用层

（2）在7层OSI网络协议中，以下哪一层能够执行选择字段保密性（**E**）

A.物理层；B.数据链路层；C.网络层；D.传输层；E.应用层

（3）基于实体的安全体系结构中，以下不属于其安全属性的是（**B**）

A.标识属性；B.资源属性；C.认证属性；E.访问控制属性；F.保密及完整性属性

（4）以下不属于认证属性的是（**C**）

A.口令；B.对称密钥；C.加密；D.公钥；E.私钥

（5）实施最小特权时，采用的技术有（**C**）**ABD**

A.模块化编程；B.结构化设计；C.功能模块的耦合性小；D.面向资源的访问控制.

3、问答题

（1）为什么从系统设计之初就考虑安全性很重要？

**如果没有在建立系统时就考虑到各种安全问题，在后续的完善中会面临一些安全设计无法很好地集成到系统中的问题，为了解决这些问题通常要付出更高昂的代价，比如补丁修复、另外建立专门的安全系统等。而这样会带来系统可靠性安全性下降、成本代价高昂。所以应当在设计系统时充分考虑安全性，并考虑到未来可能会出现的安全问题，为安全策略预留空间。**

（2）如何在系统设计时预设安全问题？

**预设的安全问题不能太特殊或太具体，因为安全漏洞与攻击是多种多样的，过于具体的安全问题预设会让系统的设计陷入局限性；**

**从抽象层次理解安全问题，而不是针对具体的问题，这样可以让所设计的系统具有通用性普适性，能够更加全面地进行安全防御；**

**关注安全策略地制定，一旦改变，可能对系统造成灾难性地影响。**

（3）入侵检测系统能否芯片化？为什么？

**不可以，入侵检测系统是基于零信任的安全体系架构，那么就建立在环境假设已被攻陷的基础上，所有的数据源和计算资源都应被视为资源。将入侵检测系统芯片化，部署在非信任区域内，入侵检测结果不可信，那么就失去了入侵检测的意义。**