**第六章**

一、选择题

1.以下哪一项不是安全协议的安全功能()

1. 端到端的可靠传输
2. 双向身份鉴别
3. 数据完整性检测
4. 数据加密

答案：选A，端到端传输不是，在书上134页

2.IPsec中安全关联(SA)的三元组包括()

A.安全参数索引SPI、源IP地址、数字证书

B.安全参数索引SPI、目的IP地址、数字证书

C.安全参数索引SPI、目的IP地址、安全协议

D.安全参数索引SPI、源IP地址、安全协议

答案：选C，IPsec中安全关联SA用安全参数索引SPI、目的IP地址、安全协议唯一标识；在书上136页

1. ESP采用和AII相同的MAC算法鉴别数据，但计算鉴别数据时覆盖的字段不包括下列哪一项？（）
2. ESP手部
3. 净荷
4. ESP尾部
5. 外层IP首部中的不变字段
6. 答案：选D，包括ESP手部、净荷、ESP尾部；在书上142页

二、判断题

1.IPSec属于传输层的安全解决方案（）

答：错，IPSec属于网络层的安全解决方案，书上135页，最下面一段话的第一句，IPSec是网际层实现IP分组端到端的安全传输的机制，由一组安全协议组成。

2.SMTP只能传输7位ASCII码，无法传输由任意二进制位流构成的邮件体（）

答案：对；书上171页

1. 传输模式用于保证数据端到端安全传输，并对数据源端进行鉴别。（）

答案：对；书上137页传输模式第一句话。

三、名词解释

1.什么是安全关联？

答：为了实现数据发送者至接受者的安全传输，需要建立发送者与接受者之间的关联，这种以实现端源鉴别、数据加密和完整性检测为目的的关联称为安全关联。

在书上136页第一段话

2.什么是安全电子交易（SET）

答：安全电子交易（SET）是一种协议，是为了解决持卡人、商家和银行之间基于Internet进行的电子交易过程中的安全性而设计的协议。

书上158页

1. 什么是TLS握手协议

答：TLS握手协议是一种实现身份鉴别和安全参数协商的协议。客户端和服务器端通过TLS记录协议传输数据前，需要通过TLS握手协议完成双向身份鉴别过程，并约定压缩算法、加密算法、MAC算法、加密密钥、MAC密钥等安全参数。

书上146页

四、简述

1.简述TLS的作用

传输层安全协议，建立安全连接，实现数据在两个进程之间的安全传输过程。用于完成双向身份鉴别和安全参数协商的协议.（TLS实现两个进程之间的双向鉴别和安全传输。安全传输的数据类型可以是直接作为TCP报文净荷的应用层消息，如HTTP消息、FTP消息等），实现双向身份鉴别与保证相互交换的数据的保密性和完整性。

在书上145页，中间那一段

1. 简述安全协议的功能

①用于双向身份鉴别

身份鉴别过程就是一方向另一方证明自己身份的过程。

②数据加密

安全协议需要实现密钥分发、加密算法协商等功能。

③数据完整性检测

安全协议需要实现密钥分发和报文摘要算法、加密算法协商等功能，用于数据完整性检测。

④防重放攻击机制

安全协议为了实现防重放攻击功能，一是在报文中增加序号字段，二是能够动态调整接收端的序号窗口。

3.SET的电子交易过程

①颁发证书

②选择商品

③初始请求和响应

④购买请求

⑤授权请求和响应

⑥购货响应

⑦支付请求和响应

书上P163-168