**2018年春季学期《网络与信息安全》期末复习文档**

**一.简答题**

1.防火墙体系结构通常分为哪几类？

2.操作系统的安全机制有哪些？

3.防火墙从实现方式上有几种？

4.ISO7498-2建议的安全机制有哪几种？

5.什么是虚拟专用网技术？

6.什么是数据包过滤技术？

7.什么是Linux？

8．什么是PKI？它由哪几部分组成？

9.数字签名的功能和作用是什么？

**二．叙述题**

1. 电子商务交易系统实现过程有哪几步？

2.目前有几种加密方法？

3.用户或系统通过哪几种方法证明其身份？

4.单钥加密体制中，用户A和B获得共享密钥的方法有几种？

**三.画图说明题**

1.请画图说明具有保密性和认证性的密钥分配并说明建立会话密钥的步骤。

**参考答案：**

**一．简答题**

1．答：防火墙体系结构通常分为四类：

（1）．屏蔽路由器

（2）．屏蔽主机网关

（3）．双宿主机网关

（4）．屏蔽子网

2．答：操作系统的安全机制由本地安全策略、安全账号管理器、安全证明监视器等。

3．答：大多数防火墙实际使用中实现方式可以分为以下四种类型:

（1）.嵌入式防火墙

（2）．软件防火墙

（3）．硬件防火墙

（4）．应用程序防火墙

4．答：ISO7498-2建议的安全机制：

(1)．加密机制

加密机制用于加密数据或流通中的信息，其可以单独使用。

(2)．数字签名机制

数字签名机制是由对信息进行签字和对已签字的信息进行证实这样两个过程组成。

(3)．访问控制机制

访问控制机制是根据实体的身份及其有关信息来决定该实体的访问权限。

(4)．数据完整性机制

(5)．认证机制

(6)．通信业务填充机制

(7)．路由控制机制

(8)．公证机制

公证机制是由第三方参与的签名机制。

5．答：虚拟专用网VPN是企业内部网在Internet等公共网络上的延伸，通过一个专用的通道来创建一个安全的专用连接，从而可将远程用户、企业分支机构、公司的业务合作伙伴等与公司的内部网连接起来，构成一个扩展的企业内部网。

6．答：数据包过滤技术是在网络层对数据包进行分析、选择，选择的依据是系统内设置的过滤的逻辑，称为访问控制表。通过检查数据流中每一个数据包的源地址、目的地址、所用端口号、协议状态等因素，或它们的组合来确定是否允许数据包通过。

7．答：Linux是一套免费使用和自由传播的类UNIX操作系统，它主要用于基于Intel x86系列CPU的计算机上。这个系统是由世界各地成千上万的程序员设计和实现的。其目的是建立不受任何商品化软件的版权制约能自由使用的UNIX兼容产品。

8.答：PKI就是用公钥技术实施和提供安全服务的安全基础设施。

PKI是一种新的安全技术，它由公开密钥密码技术、数字证书、证书发放机构（CA）和关于公开密钥的安全策略等基本成分共同组成的。

9.答：信息鉴别的方法可以使信息接收者确定信息发送者的身份以及信息在传送过程中是否被改动过。为解决这一问题，就必须利用数字签名技术。签名必须达到如下效果：在信息通信的过程中，接收方能够对公正的第三方证明其收到的报文内容是真的，而且确实是由那个发送方发送过来的；签名还必须保证发送方事后不能根据自己的利益否认它所发送过的报文，而收方也不能根据自己的利益来伪造报文或签名。

**二．叙述题**

1．答：假设在交易之前，企业客户已经申请获得了电子商务站点所颁发的客户消费证书。

1）．客户浏览电子商务站点，初始化请求，客户端认证

2）．验证客户身份，确定客户购买权限，返回应答请求，用户进入购买状态

3）．完成购物，发送订单

4）．服务器收到订单，请求获取安全时间戳，记录交易信息

5）．向商家发送订单通知，确认交易成功信息

2.答：目前有三种加密的方法：

（1）       对称加密：

使用同样的密钥进行加密和解密。

（2）       非对称加密：

也称公钥加密。使用一对密钥来加密数据。一个用于加密，一个用于解密。

（3）       单向加密：

也称HASH加密。其使用一个叫HASH函数的数学方程式去加密数据。理论上HASH函数把信息进行混杂，使得它不可能恢复原状。

3.答：用户或系统能够通过四种方法来证明其身份，即实物认证、密码认证、生物特征认证和位置认证。

1）．实物认证

实物认证是采用基于所拥有的某些东西作为认证的方法。

2）．密码认证

在计算机网络系统中密码认证通常是用口令。

3）．生物特征认证

该方法可以使用指纹、声音、图像以及签名等方式进行认证。

4）．位置认证

该认证的策略是根据用户的位置来决定其身份。

4.答：用户A和B获得共享密钥的方法基本上有以下几种：

（1）       密钥由A选取并通过物理手段发送给B

（2）       密钥由第三方选取并通过物理手段发送给A和B

（3）       如果A、B事先已有一密钥，则其中一方选取新密钥后，用已有的密钥加密新密钥并发送给另一方。

（4）       如果A和B与第三方C分别有一保密信道，则C为A、B选取密钥后，分别在两个保密信道上发送给A、B。

**三．画图说明题**

1.答：

若用户A和B双方已完成公钥交换，可按以下步骤建立会话密钥。

1）A用B的公开钥加密A的身份IDA和一个一次性随机数N1后发给B，其中N1用于唯一地标识此次业务。

2）B用A的公开钥PKA加密A的一次性随机数N1和B新产生的一次性随机数N2后发给A。因为只有B能解读A发给B的消息，而B所发的消息中N1的存在可使A相信对方的确是B。

3）A用B的公钥PKB对N2加密后返回给B，以使B相信对方的确是A。

4）A选一会话密钥KS，然后将其M=EpkB[EskA[KS]]发给B，其中用B的公开钥加密是为了保证只有B能解读加密结果，用A的秘密钥加密是保证该加密结果只有A能发送。

5）B以DskA[DskB[M]]恢复会话密钥。

