全国 2010 年 1 月自学考试电子商务安全导论试题

课程代码：00997

一、单项选择题(本大题共 20 小题，每小题 1 分，共 20 分)

在每小题列出的四个备选项中只有一个是符合题目要求的，请将其代码填写在题后的括号内。错选、多选或未选均无分。

l. 美国的橘皮书中计算机安全 B 级的子级中，从高到低依次是(　C　)1-19

A.Bl B2 B.B2 B1

C.B1 B2 B3 D.B3 B2 B1

2. 现在常用的密钥托管算法是(　A　)2-51

A.DES 算法　B.EES 算法

C.RAS 算法　D.SHA 算法

3.SHA 算法输出的哈希值长度为(　C　)3-64

A.96 比特　B.128 比特

C.160 比特　D.192 比特

4.使用数字摘要和数字签名技术不能解决的电子商务安全问题是(　A　)3-65

A.机密性B.完整性

C.认证性D.不可否认性

5.在服务器中经常使用偶数块硬盘，通过磁盘镜像技术来提升系统的安全性，这种磁盘冗余技术称为(　B　)4-72

A.RAID 0　B.RAID 1

C.RAID 3　D.RAID 5

6.防火墙技术中处理效率最低的是(　C　)5-82

A.包过滤型　B.包检验型

C.应用层网关型　D.状态检测型

7.目前，对数据库的加密方法主要有(　B　)6-96

A.2 种　B.3 种

C.4 种　D.5 种

8.身份证明系统的质量指标中的 II 型错误率是(　C　)7-100

A.通过率B.拒绝率

C.漏报率D.虚报率

9.在对公钥证书格式的定义中已被广泛接受的标准是(　A　)8-115

A.X.500　B.X.502

C.X.509　D. X. 600

10.使用者在更新自己的数字证书时不可以采用的方式是(　　A　　)8-125

A.电话申请　B.E-Mail 申请

C.Web 申请　D.当面申请

11. 在 PKI 的构成模型中，其功能不包含在 PKI 中的机构是(　D　　)9-128

A.CA　　B.ORA

C.PAA　D. PMA

12.用于客户——服务器之间相互认证的协议是(　　B　　)10-140

A.SSL 警告协议　B.SSL 握手协议

C.SSL 更改密码协议　D.SSL 记录协议

13.目前 CTCA 提供安全电子邮件证书，其密钥位长为(　D　　)11-164

A.64 位　B.128 位

C.256 位 D.512 位

14.SHECA 证书的对称加密算法支持(B　　)11-169

A.64 位　B.128 位

C.256 位 D.512 位

15.通过破坏计算机系统中的硬件、软件或线路，使得系统不能正常工作，这种电子商务系统可能遭受的攻击是(　　B　　)1-11

A.系统穿透　B.中断

C.拒绝服务　D.通信窜扰

16.计算机病毒的最基本特征是(　C　　)4-75

A.自我复制性B.潜伏性

C.传染性D.隐蔽性

17.在 VPN 的具体实现方式中，通过在公网上开出各种隧道，模拟专线来建立的 VPN 称为(　　A　　)5-89

A.VLL　B.VPDN

C.VPLS　D.VPRN

18.数据库加密桥具有可以在不同的操作系统之间移植的特性，主要是因为加密桥的编写语言是(　　B　　)6-98

A.C 语言B.C++

C.JAVA　D..NET

19.在域内认证中，TGS 生成用于 Client 和 Server 之间通信的会话密钥 Ks 发生在(　C　　)7-105

A.第 1 个阶段第 2 个步骤　B.第 2 个阶段第 1 个步骤

C.第 2 个阶段第 2 个步骤　D.第 3 个阶段第 1 个步骤

20.在下列选项中，属于实现递送的不可否认性的机制的是(　B　　)9-136

A.可信赖第三方数字签名　B.可信赖第三方递送代理

C.可信赖第三方持证　D.线内可信赖第三方

二、多项选择题(**本大题共 5 小题，每小题 2 分，共 10 分**)

在每小题列出的五个备选项中至少有两个是符合题目要求的，请将其代码填写在题后的括号内。错选、多选、少选或未选均无分。

21.下列选项中，属于电子商务安全的中心内容的有(　BCDE　　)1-11

A.商务系统的健壮性　B.商务数据的机密性

C.商务对象的认证性　D.商务服务的不可否认性

E.商务信息的完整性

22.数字签名可以解决的鉴别问题有(　BCDE　　)3-67

A.发送方伪造B.发送方否认

C.接收方篡改D.第三方冒充

E.接收方伪造

23.Internet 的接入控制主要对付(　ABC　　)6-93

A.伪装者B.违法者

C.地下用户　D.病毒

E.木马

24.SET 交易成员有(　ABCDE　　)10-142

A.持卡人B.网上商店

C.收单银行　D.认证中心 CA

E.支付网关

25.CFCA 金融认证服务相关业务规则按电子商务中的角色不同，可划分为(　ABCD　　)11-170

A.网关业务规则　B.商户(企业)业务规则

C.持卡人业务规则D.中介业务规则

E.通信业务规则

三、填空题(**本大题共 5 小题，每小题 2 分，共 l0 分**)

请在每小题的空格中填上正确答案。填错、不填均无分。

26.数字时间戳技术利用___单向杂凑函数_____和___数字签名协议_____来实现其解决有关签署文件的时间方面的仲裁。3-70

27.接入控制机构由用户的认证与__识别_____、对认证的用户进行___授权_____两部分组成。6-93

28.为了防止数据丢失，并保证数据备份的效率，除了定期(如一周)对数据进行完全备份外，还要定期(如一天)对数据进行__定时备份__或___归档_____。4-73

29.在我国，制约 VPN 的发展的客观因素包括_因特网带宽_____和___服务质量 QoS_____。5-90

30.为了对证书进行有效的管理，证书实行____分级_____管理，认证机构采用了_____树型_____结构，证书可以通过一个完整的安全体系得以验证。8-126

四、名词解释题(**本大题共 5 小题**, 每小题 3 **分**，**共** 15 **分**)

31.商务服务的不可否认性 1-12

答：

商务服务的不可否认性是指信息的发送方不能否认已发送的信息，接受方不能否认已收到的信息，这是一种法律有效性要求。

32.数字认证 8-109

答：

数字认证是指用数字办法确认、鉴定、认证网络上参与信息交流者或服务器的身份。

33.网络系统物理安全 4-71

答：

网络系统物理设备的可靠、稳定、安全是电子商务命案的基础。网络系统物理设备的可靠、稳定、安全，包括运行环境、容错、备份、归档和数据完整性预防。

34.受信网络 5-79

答：

受信网络指防火墙内的网络。

35.SET10-141

答：

SET 是一种用来保护在 Internet 上付款交易的开放式规范，它包含交易双方身份的确认、个人和金融信息隐密性及传输数据完整性的保护，其规格融合了由 RSA 数据的双钥密码体制编成密码文件的使用，以保护任何开放互联网络上个人和金融信息的隐密性。

五、简答题(**本大题共 6 小题，每小题 5 分，共 30 分**)

36.作为 VPN 的基础的隧道协议主要包括哪几种?5-84

答：

隧道协议主要包括以下几种：

（1）互联网协议安全 IPSec(Internet Protocol Security)：它位于第 3 层，是一个与互联网密钥交换 IKE(Internet Key Exchange)有关的框架协议，由 IETFRFCs 2401 -2409 定义，主要用于基于防火墙的 VPN 系统。

（2）第 2 层转发协议 L2F(Layer 2 Forwarding)：它由 Cisco 系统公司提出，可以在多种媒介，如 ATM、帧中继、IP 网上建立多协议的安全 VPN 通信方式。第 2 层隧道协议 L2TP(Layer 2 Tunneling Protocol)：它综合了 PPTP 和 L2F 的优点，并提交 IETF 进行标准化操作。

（3）点对点隧道协议 PPTP(Point to Point Tunneling Protocol)：它由 3Com、Access、As-cend、Microsoft 和 ECI Telematics 公司共同制定，用于 PPTP 客户机和 PPTP 服务器之间的安全通信。

（4）通用路由封装协议 GRE（Generic Routing Encapsulation）：GRE 在 RFC1701/RFC1702 中定义，它规定了怎样用一种网络层协议去封装另一种网络层协议的方法，GRE 的隧道由其两端的源 IP 地址和目的 IP 地址来定义。它允许用户使用 IP 封装 IP、IPX、Apple-Talk 并支持全部的路由协议如 RIP、OSPF、IGRP 和 EIGRP。

37. 一个大的实际系统中，通行字的选择原则是什么？7-101

答：

一个大系统的通行字的选择原则为：

(1) 易记；

(2) 难于被别人猜中或发现；

(3) 抗分析能力强。在实际系统中，需要考虑和规定选择方法、使用期限、字符长度、分配和管理以及在计算机系统内的保护等。根据系统对安全水平的要求可有不同的选取。

38．数字签名与手书签名有什么不同？3-66

答：

数字签名与手书签名的区别在于：手写签名（包括盖章）是模拟的，因人而异，即使同一个人也有细微差别，比较容易伪造，要区别是否是伪造，往往需要特殊的专家。而数字签名是 0 和 1 的数字串，极难伪造，要区别是否为伪造，不需专豪。对不同的信息摘要，即使是同一人，其数字签名也是不同的。这样就实现了文件与签署的最紧密的“捆绑”。

39．简述密钥管理中存在的威胁。9-133

答：

（1）密钥的泄露。

（2）密钥或公钥的确证性(Authenticity)的丧失，确证性包括共享或有关一个密钥的实体身份的知识或可证实性。

（3）密钥或公钥未经授权使用，如使用失效的密钥或违例使用密钥。

40．如何对密钥进行安全保护？8-113

答：

（1）密钥按算法产生后，首先将私钥送给用户，如需备份，应保证安全性，将公钥送给 CA，用以生成相应证书。

（2）为了防止未授权用户对密钥的访问，应将密钥存人防窜扰硬件或卡（如 IC 卡或 PCM-CIA 卡）中．或加密后存人计算机的文件中。

（3）此外，定期更换密钥对是保证安全的重要措施。

41．SET 的主要安全保障来自哪几个方面？10-145

答：

目前 SET 的主要安全保障来自以下三个方面：

（1）将所有消息文本用双钥密码体制加密；

（2）将上述密钥的公钥和私钥的字长增加到 512B - 2048B;

（3）采用联机动态的授权(Authority)和认证检查(Certificate)，以确保交易过程的安全可靠。

六、论述题(本大题共 1 小题，15 分)

42．试从实用的角度，比较 DES 算法和 RSA 算法的特点。2-26, 2-47

答：

（1）DES 算法是由 IBM 公司开发出来的，他将两种基本的加密算法（替换加密和转换加密）完美地结合起来。这种算法的强度是通过反复应用这种技术，将一种基本算法施于另一种基本算法之上，并进行 16 次循 I 不迭代来完成的。DES 的加密算法本身并不保密而是完全公开的必须绝对保密的是密钥，且密钥可由使用者随时更换。只要密钥不泄露，用 DES 算法加南的密文的可靠性是很高的．不过，随着计算机技术的发展，对 DES 算法的穷举分析，已使 DES 的安全性遭到严重威胁，似至美国国家安全局宣布从 1988 年起不再保证 DES 标准的安全，，即使如此，至今仍无人发现 DES 算法中的任何严重缺陷，因此， DES 仍然被广泛应用。

（2）1978 年就出现了 RSA 算法，它是第一个既能用于数据加密也能用于数字签名的算法。RSA 密码体制是基于群 Z_n。中大整数因子分解的困难性。RSA 算法的安全性依赖于大数分

解的困难性，公钥和私钥都是两个大素数（大于 100 介十进制位）。随着大整数的分解算法和计算能力的提高，RSA 需要采用足够大的整数。如 512 位、664 位、L024 位等。