全国 2011 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。

1. 网上商店的模式为(　B　)1-3

A.B-B　B.B-C

C.C-C　D.B-G

2. 下列选项中不属于 Internet 系统构件的是(　D　)1-13

A. 客户端的局域网　B. 服务器的局域网

C. Internet 网络　D. VPN 网络

3. 双钥密码体制算法中既能用于数据加密，也能用于数字签名的算法是(　C　)2-47

A.AES　B.DES

C.RSA　D.RC-5

4. 托管加密标准 EES 的托管方案是通过什么芯片来实现的?(　B　)2-52

A. DES 算法芯片　B. 防窜扰芯片

C. RSA 算法芯片　D. VPN 算法芯片

5. 数字信封中采用的加密算法是(　B　)3-69

A.AES　B.DES

C.RC-5　D.RSA

6. 关于散列函数的概念，下列阐述中正确的是(A　)3-54

A. 散列函数的算法是公开的

B. 散列函数的算法是保密的

C. 散列函数中给定长度不确定的输入串，很难计算出散列值

D. 散列函数中给定散列函数值，能计算出输入串

7. 下列选项中不是病毒的特征的是(　D　)4-75

A. 传染性　B. 隐蔽性

C. 非授权可执行性　D. 安全性

8. 下列选项中属于病毒防治技术规范的是(　A　)4-77

A. 严禁玩电子游戏　B. 严禁运行合法授权程序

C. 严禁归档　D. 严禁 UPS

9. 下列选项中，属于防火墙所涉及的概念是(　　A　　)5-79

A.DMZ　B.VPN

C.Kerberos　　D.DES

10. Internet 入侵者中，乔装成合法用户渗透进入系统的是(A　　)6-93

A. 伪装者　　B. 违法者

C. 地下用户　D. 黑客

11. 公钥证书的格式定义在 ITU 的 X.500 系列标准中的哪个标准里?(　B　　)8-112

A.X.501　B.X.509

C.X.511　D.X.519

12. CA 设置的地区注册 CA 不具有的功能是(A　　)8-114

A. 制作证书　B. 撤销证书注册

C. 吊销证书　D. 恢复备份密钥

13. 认证机构对密钥的注册、证书的制作、密钥更新、吊销进行记录处理使用的技术是(　　D　　)9-133

A. 加密技术　B. 数字签名技术

C. 身份认证技术　D. 审计追踪技术

14. 在 SSL 的协议层次中，首先运行的是(　　A　　)10-139

A. 握手协议　B. 更改密码规格协议

C. 警告协议　D. 记录协议

15. 信息在网络上传送或存储的过程中不被他人窃取、不被泄露或披露给未经授权的人或组织，或者经过加密伪装后，使未经授权者无法了解其内容，这种电子商务安全内容称(　　A　　)1-11

A. 商务数据的机密性　B. 商务数据的完整性

C. 商务对象的认证性　D. 商务服务的不可否认性

16. 早期提出的密钥交换体制是用模一个素数的指数运算来进行直接密钥交换，这种体制通常称为(　　D　　)2-50

A. Kerberos 协议　B. LEAF 协议

C. Skipjack 协议　D. Diffie-Hellman 协议

17. 为了保证电子商务安全中的认证性和不可否认性，必须采用的技术是(　A　　)3-65

A. 数字签名　B. 散列函数

C. 身份认证　D. 数字时间戳

18. 防火墙能解决的问题是(　A　)5-82

A. 防止从外部传送来的病毒软件进入

B. 防范来自内部网络的蓄意破坏者

C. 提供内部网络与外部网络之间的访问控制

D. 防止内部网络用户不经心带来的威胁

19. CA 服务器产生自身的私钥和公钥，其密钥长度至少为(　C　)8-124

A. 256 位　　B. 512 位

C. 1024 位　　D. 2048 位

20. 作为对 PKI 的最基本要求，PKI 必须具备的性能是(　B　)9-129

A. 支持多政策　　B. 透明性和易用性

C. 互操作性　D. 支持多平台

二、多项选择题（本大题共 5 小题，每小题 2 分，共 10 分）

在每小题写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. 电子商务在英语中的不同叫法有(　ABCDE　)1-1

A.E-Commerce　B.Digital Commerce

C.E-Trade　D.E-Business

E.EDI

22. 散列函数不同的叫法有(　ABCDE　)3-54

A. 哈希函数　B. 杂凑函数

C. 收缩函数　D. 消息摘要

E. 数字指纹

23. 加密桥技术能实现对不同环境下数据库数据加密以后的数据操作，这里的不同环境包括(　ABCD　)6-97

A. 不同主机　B. 不同操作系统

C. 不同数据库管理系统　　D. 不同语言

E. 不同应用开发环境

24. Kerberos 系统的组成包括(　ABDE　)7-104

A. 用户 Client　　B. 服务器 Server

C. 认证中心 CA　D. 认证服务器 AS

E. 票据授权服务器 TGS

25. CTCA 采用分级结构管理，其组成包括(　ACE　　)11-163

A. 全国 CA 中心　B. 省级 CA 中心

C. 省级 RA 中心　D. 地市级 RA 中心

E. 地市级业务受理点

三、填空题 (本大题共 5 小题，每小题 2 分，共 10 分)

请在每小题的空格中填上正确答案。填错、不填均无分。

26. 在一次信息传递过程中，可以综合利用消息加密、数字信封、散列函数和数字签名实现安全性、完整性、_可鉴别_____和__不可否认____，这种方法一般称为混合加密系统。3-69

27. Intranet 是指基于___TCP/IP___协议的内部网络。它通过__防火墙____或其他安全机制与 Internet 建立连接。1-4/5

28. 采用密码技术保护的现代信息系统，其安全性取决于对__密钥____的保护，而不是对__算法____和硬件本身的保护。9-132

29. SHECA 提供了两种证书系统，分别是_SET 证书系统_____和__通用证书系统_____。11-168

30. 计算机病毒按照寄生方式分为__引导型_____病毒、__文件型_____病毒和复合型病毒。4-75

四、名词解释(本大题共 5 小题，每小题 3 分，共 15 分)

31. 多字母加密 2-24

答：

多字母加密是使用密钥进行加密。密钥是一组信息（一串字符）。同一个明文经过不同的密钥加密后，其密文也会不同。

32. 复合型病毒 4-76

答：

复合型病毒是指具有引导型病毒和文件型病毒寄生方式的计算机病毒。

33. Intranet VPN5-87

答：

即企业的总部与分支机构间通过公网构筑的虚拟网。

34. 接入控制 6-93

答：

接入或访问控制是保证网络安全的重要手段，它通过一组机制控制不同级别的主体对目标资源的不同授权访问，在对主体认证之后实施网络资源安全管理使用。

35. 证书政策 9-128

答：

证书政策是一组规则；指出一个证书对一组特定用户或应用的可适用性，表明它对于一个特定的应用和目的是否是可用的，它构成了交叉验证的基础。

五、简答题(本大题共 6 小题，每小题 5 分，共 30 分)

36. 电子商务的真实性的含义是什么？2-21

答：

真实性是指商务活动中交易者身份的真实性，亦即是交易双方确实是存在的，不是假冒的。网上交易的双方相隔很远，互不了解，要使交易成功，必须互相信任，确认对方是真实的，对商家要考虑客户是不是骗子，发货后会不会收不回货款；对客户要考虑商家是不是黑店，付款后会不会收不到货，或者收到货后质量是否能有保证。因此，能否方便而又可靠地确认交易双方身份的真实性，是顺利进行电子商务交易的前提。

37. 数字签名的作用是什么？3-66

答：

一、数字签名可以证明：

1、如果他人可以用公钥正确地解开数字签名，则表示数字签名的确是由签名者产生的。

2、如果消息 M 是用散列函数 H 得到的消息摘要 H(M)，和消息的接收方从接收到的消息 M’计算出散列值 H(M’)，这两种信息摘要相同表示文件具有完整性。

二、数字签名机制提供了一种数字鉴别方法，普遍用于银行、电子商务、电子办公等。

三、数字签名可以解决下述安全鉴别问题：

1、接收方伪造：接收方伪造一份文件，并声称这是发送方发送的；

2、发送者或接收者否认：发送者或接收者事后不承认自己曾经发送或接收过文件；

3、第三方冒充：网上的第三方用户冒充发送或接收文件；

4、接收方篡改：接收方对收到的文件进行改动。

38. 防火墙与 VPN 之间的本质区别是什么？7-79/83

答：

防火墙与 VPN 之间的本质区别是：堵 / 通；或防范别人 / 保护自己。

（1）防火墙的主要作用是防止发生网络安全事件引起的损害，使入侵更难实现，来防止非法用户，比如防止黑客、网络破坏者等进入内部网络。。

（2）虚拟专用网 VPN（Virtual Private Network）通常被定义为通过一个公共网络(通常是 Intemet)建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道，它是对企业内部网的扩展。

39. 简述身份证明系统普遍应该达到的要求。7-99

答：

（1）验证者正确识别合法示证者的概率极大化。

（2）不具可传递性，验证者 B 不可能重用示证者 A 提供给他的信息，伪装示证者 A 成功地骗取其他人的验证，得到信任。

（3）攻击者伪装示证者欺骗验证者成功的概率小到可以忽略，特别是要能抗已知密文攻击，即攻击者在截获到示证者和验证者多次（多次式表示）通信下，伪装示证者欺骗验证者。

（4）计算有效性，为实现身份证明所需的计算量要小。

（5）通信有效性，为实现身份证明所需通信次数和数据量要小。

（6）秘密参数安全存储。

（7）交互识别，有些应用中要求双方互相进行身份认证。

（8）第三方的实时参与，如在线公钥检索服务。

（9）第三方的可信赖性。

（10）可证明安全性。

后 4 条是某些身份识别系统提出的要求。

40. 简述认证机构的证书吊销功能。8-125

答：

证书是网上交易各方在交易进行前对各自身份进行确认的一种手段。当证书持有者违反证书使用政策、证书丢失或受到攻击、证书过期或服务提供者停止服务等情况下，应吊销其证书并予以公布。吊销有主动申请吊销和被动强制性吊销两种形式。

（1）证书持有者申请吊销

当证书持有者认为不再用此证书参与网上事务，主动上网申请吊销或亲自到认证机构吊销此证书。证书持有者通过 WWW 或 E- Mail 的方式通过网络申请吊销。证书吊销后，认证机构必须更新证书吊销表，将吊销证书放人证书吊销表，并在网上及时公布。以证机构以正式的信函或 E - Mail 通知证书持有者此证书已作废。

（2）认证机构强制吊销证书

这是一种强制性的吊销方式。认证机构吊销证书持有者的证书，将其放人证书吊销表，并在网上予以公布。

当认证机构认为证书持有者的证书过期或违反证书使用政策时，主动吊销证书持有者的证书　证书吊销后，认证机构更新证书吊销表，并在网上及时公布。认证机构以正式信函或 E - Mail 通知证书持有者该证书已作废。

41. 简述数字证书中公钥—私钥对应满足的要求。8-113

答：

RSA 的公钥一私钥对既可用于加密，又可用于签名，但实际上公钥一私钥对的功能是不一样的。因此在要求上要考虑不一致的情况：

（1）需要采用两个不同的密钥对分别作为加密一解密和数字签名一验证签名用。

（2）一般公钥体制的加密用密钥的长度要比签名用的密钥短，有的国家对出口加密用算法的密钥的长度有限制，而对签名用密钥无限制。

（3）由于实际商务的需要或其他原因，需要用不同的密钥和证书（如有多个信用卡一样），例如一般消息加密用的密钥比较短，加密时间可快一些；而对短消息（如单钥密码体制的加密密码）加密用的密钥可以长一些，有利于防止攻击。

（4）密钥对的使用期限不同：加密密钥使用频度比签名用密钥的使用频度大得多，因此更换周期要短。

（5）并非所有公钥算法都具有 RSA 的特点，例如 DSA 算法可以用做签名，但无须建立密钥。未来系统要能支持多种算法，因而应支持采用不同签名密钥对和不同密钥的建立。

（6）加密算法可能支持密钥托管和密钥恢复，以及可能的法律监听。但数字签名的密钥则不允许泄露给他人，其中也包括法律机构。

六、论述题(本大题共 1 小题，15 分)

42. 试述在网上书店遵循 SET 协议进行购物的动态认证过程。10-151

答：

双方都获得数字证书后就开始购书。以持卡人 A 到网上书店 B 购买书 X 为例说明 SET 的运作过程。

（1）持卡人订货：A 进入购物网站 B 高店里面选择了货物 X，填写了在线商店名称、购买物品名称及订购数量、送货地址和日期时间等订单信息。

（2）通过电子商务服务器与有关在线商店联系，在线商店做出应答，告诉消费者所填写的订货单的货物单价、应付款数、交货方式等信息是否准确，是否有变化。

（3）持卡人选择付款方式，确认订单，签发付款指令，此时 SET 介入；这时“电子钱包”软件自动打开；在 SET 中，消费者必须对订单和付款指令进行数字签名，同时利用双重签名技术以保证商家看不到消费者的账号信息；并将信用卡信息以及订单信息分别加密传送给商店 B。

（4）商店 B 通过收单银行检查信用卡的有效性：商店 B 接收到加密后的订单与信用卡数据后，将信用卡数据原封不动地通过支付网关传送给收单银行，再到电子货币发行公司确认，请其检查信用卡的有效性。注意：当商店 B 虽然收到信用卡信息，但是无法解

密时，也就看不到信用卡信息。

（5）收单银行的确认：收单银行向发卡银行确认信用卡数据无误后，发出信息通知商店，商店就可以安全地接下这笔订单了。

（6）在线商店发送订单确认信息给持卡人，持卡人端的软件可以记录交易日志，以备将来查询。

（7）结账。A 会接到发卡银行的信用卡账单，而商店发送货物成提供服务给持卡人，并通知收单银行将钱从持卡人的账号转移到商店账号，或通知发卡银行请求支付。