全国 2010 年 10 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. 计算机安全等级中，C2 级称为（　B　）1-20

A. 酌情安全保护级　　B. 访问控制保护级

C. 结构化保护级　D. 验证保护级

2. 在电子商务的发展过程中，零售业上网成为电子商务发展的热点，这一现象发生在（　C　）1-6

A. 1996 年　　B. 1997 年

C. 1998 年　　D. 1999 年

3. 电子商务的安全需求中，保证电子商务系统数据传输、数据存储的正确性的根基是（　A　）2-21

A. 可靠性　　B. 完整性

C. 真实性　　D. 有效性

4. 最早提出的公开的密钥交换协议是（　B　）2-51

A. Blom　B. Diffie-Hellman

C. ELGamal　D. Shipjack

5. ISO/IEC9796 和 ANSI X9.30-199X 建议的数字签名的标准算法是（　D　）3-67

A. HAVAL　B. MD-4

C. MD-5　D. RSA

6. 发送方使用一个随机产生的 DES 密钥加密消息，然后用接受方的公钥加密 DES 密钥，这种技术称为（　B　）3-69

A. 双重加密　B. 数字信封

C. 双联签名　D. 混合加密

7. 在以下主要的隧道协议中，属于第二层协议的是（ D　）5-84

A. GRE　B. IGRP

C. IPSec　D. PPTP

8. 使用专有软件加密数据库数据的是（　B　）6-96

A. Access　　B. Domino

自考备考三件宝：自考笔记、真题及答案、录音课件！

qq593777538 examebook.com

C. Exchange　D. Oracle

9. 在下列选项中，不是每一种身份证明系统都必须要求的是（　D　）7-100

A. 不具可传递性　B. 计算有效性

C. 通信有效性　　D. 可证明安全性

10. Kerberos 的局限性中，通过采用基于公钥体制的安全认证方式可以解决的是（ D　　）7-108

A. 时间同步　B. 重放攻击

C. 口令字猜测攻击　　D. 密钥的存储

11. 在下列选项中，不属于公钥证书的证书数据的是（ A　　）8-112

A. CA 的数字签名　B. CA 的签名算法

C. CA 的识别码　　D. 使用者的识别码

12. 在公钥证书发行时规定了失效期，决定失效期的值的是（　B　）8-115

A. 用户根据应用逻辑　B. CA 根据安全策略

C. 用户根据 CA 服务器D. CA 根据数据库服务器

13. 在 PKI 的性能要求中，电子商务通信的关键是（　C　）9-130

A. 支持多政策　　B. 支持多应用

C. 互操作性　D. 透明性

14. 主要用于购买信息的交流，传递电子商贸信息的协议是（　B　　）10-152

A. SET　B. SSL

C. TLS　D. HTTP

15. 在下列计算机系统安全隐患中，属于电子商务系统所独有的是（　D　　）1-10

A. 硬件的安全　　B. 软件的安全

C. 数据的安全　　D. 交易的安全

16. 第一个既能用于数据加密、又能用于数字签名的算法是（　D　　）2-47

A. DES　B. EES

C. IDEA　D. RSA

17. 在下列安全鉴别问题中，数字签名技术不能解决的是（　A　　）3-67

A. 发送者伪造　　B. 接收者伪造

C. 发送者否认　　D. 接收者否认

18. 在 VeriSign 申请个人数字证书，其试用期为（　B　　）8-123

A. 45 天　B. 60 天

C. 75 天　D. 90 天

自考备考三件宝：自考笔记、真题及答案、录音课件！

qq593777558 examebook.com

19. 不可否认业务中，用来保护收信人的是（　A　）9-134

A. 源的不可否认性　　B. 递送的不可否认性

C. 提交的不可否认性　D. 委托的不可否认性

20. 在整个交易过程中，从持卡人到商家端、商家到支付网关、到银行网络都能保护安全性的协议是（ A　）10-152

A. SET　B. SSL

C. TLS　D. HTTP

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. 在 20 世纪 90 年代末期，大力推动电子商务发展的有（　ABCD　）1-7

A. 信息产品硬件制造商　　B. 大型网上服务厂商

C. 政府　D. 银行及金融机构

E. 零售服务商

22. 在下列加密算法中，属于使用两个密钥进行加密的单钥密码体制的是（　AB　）2-26

A. 双重 DES　B. 三重 DES

C. RSA　D. IDEA

E. RC-5

23. 计算机病毒按照寄生方式，可以分为（　BDE　）4-75

A. 外壳型病毒　　B. 引导型病毒

C. 操作系统型病毒　　D. 文件型病毒

E. 复合型病毒

24. 接入控制技术在入网访问控制方面具体的实现手段有（ ABCDE　）6-94

A. 用户名的识别　B. 用户名的验证

C. 用户口令的识别　　D. 用户口令的验证

E. 用户帐号默认限制检查

25. 在现实生活中，需要用 CFCA 的典型应用有（　ABCD　）11-156

A. 网上银行　B. 网上证券

C. 网上申报与缴税　　D. 网上企业购销

E. 网上搜索与查询

自考备考三件宝：自考笔记、真题及答案、录音课件！

qq593777558 examebook.com

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. IDEA 加密算法中，输入和输出的数据块的长度是_____64_____位，密钥长度是___128_____位。2-26

27. 电子商务的技术要素组成中，首先要有_____网络_____，其次必须有各种各样的___应用软件_____，当然也少不了以各种服务器为核心组成的计算机系统。1-3

28. 密钥管理是最困难的安全性问题，其中密钥的_____分配_____和___存储_____可能是最棘手的。2-50

29. 安全电子邮件证书是指个人用户收发电子邮件时，采用____证书_____机制保证安全。它的申请不需要通过业务受理点，由用户直接通过自己的浏览器完成，用户的___密钥对_____由浏览器产生和管理。11-164

30. 身份证明可以依靠___所知_____、__所有_____和个人特征这 3 种基本途径之一或它们的组合来实现。7-100

四、名词解释题（本大题共 5 小题，每小题 3 分，共 15 分）

31.盲签名 3-67

答：

有时需要某人对一个文件签名，而又不让他知道文件内容，称为盲签名。

32.身份证实 7-100

答：

身份证实是对个人身份进行肯定或否定。

33.接入权限 6-93

答：

接入权限表示主体对客体访问时可拥有的权利。

34.递送的不可否认性 9-134

答：

用于防止或解决出现有关是否一个特定实体收到了一个特定的数据项、递送在特定时刻出现、或两者皆有的分歧。

35.SSL 握手协议 10-140

答：

握手(Handshake)协议用于客户一服务器之间相互认证，协商加密和 MAC 算法，传送所需的公钥证书，建立 SSL 记录协议处理完整性校验和加密所需的会话密钥。

五、简答题（本大题共 6 小题，每小题 5 分，共 30 分）

自考备考三件宝：自考笔记、真题及答案、录音课件！

qq593777553 examebook.com

36.简述双钥密码体制的加密和解密过程及其特点。2-47

答：

一、双钥密码体制又称作公共密钥体制或非对称加密体制。这种加密法在加密和解密过程中要使用一对（两个）密钥，一个用与加密，另一个用于解密，即通过一个密钥加密的信息，只有使用另一个密钥才能够解密。这样每个用户都拥有两个（一对）密钥：公共密钥和个人密钥，公共密钥用于加密，个人密钥用于解密。用户将公共密钥交给发送方或公开，信息发送者使用接收人的公共密钥加密的信息只有接收人才能解密。

二、双钥密码体制算法的特点：

1、遁合密钥的分配和管理；

2、算法速度慢，只适合加密小数量的信息。

37.简述证书合法性验证链。8-126

答：

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。每份证书都与上一级的签名证书相关联，最终通过安全链追溯到一个已知的可信赖的机构。由此便可对各级证书的有效性进行验证。例如，客户证书与发乍行证书相关联，发卡行证书又通过品牌证书和根证书相关联。根证书是一个自签名证书，根证书的签名公开密钥对所有的交易方公开，它是安全系统的最高层，它的存在使整个交易方的证书得以实观。

38.数字签名与消息的真实性认证有什么不同？3-65

答：

数字签名与消息的真实性认证是不同的。消息认证是使接收方能验证消息发送者及所发信息内容是否被篡改过。当收发者之间没有利害冲突时，这对于防止第三者的破坏来说是足够了。但当接收者和发送者之间相互有利害冲突时，单纯用消息认证技术就无法解决他们之间的纠纷，此时需借助数字签名技术。

39.列举计算机病毒的主要来源。4-76

答：

病毒的主要来源：

（1）引进的计算机系统和软件中带有病毒。

（2）各类出国人员带回的机器和软件染有病毒。

（3） -些染有病毒的游戏软件。

（4）非法拷贝中毒。

（5）计算机生产、经营单位销售的机器和软仵染有病毒。

自考备考三件宝：自考笔记、真题及答案、录音课件！

本文档资源由考试真题软件网（down.examebook.com）搜集整理二次制作！

（6）维修部门交叉感染。

（7）有人研制、改造病毒。

（8）敌对分子以病毒进行宣传和破坏。

（9）通过互联网络传人。

40.密钥对生成的途径有哪些？8-113

答：

密钥对生成的两种途径

（1）密钥对持有者自己生成：用户自己用硬件或软件生成密钥对。如果该密钥对用于数字签名时，应支持不可否认性。

（2）密钥对由通用系统生成：由用户依赖的、可信赖的某一中心机构（如 CA）生成，然后要安全地送到特定用户的设备中。利用这类中心的资源，可产生高质量密钥对，易于备份和管理。

41.基于 SET 协议的电子商务系统的业务过程有哪几步？10-143

答：

基于 SET 协议电子商务系统的业务过程可分为以下个业务过程：

（1）SET 认证之一：注册登记

一个机构如要加入到基于 SET 协议的安全电子商务系统中，必须先上网申请登记注册，申请数字证书。

（2）SET 认证之二：动态认证

一旦注册成功，就可以随意地在网络上从事电子商务活动了。

（3）SET 认证之三：商业机构处理流程

六、论述题（本大题共 1 小题，15 分）

42.试述组建 VPN 应该遵循的设计原则。5-90

答：

VPN 的设计应该遵循以下原则：安全性、网络优化、VPN 管理等。

（1）在安全性方面，由于 VPN 直接构建在公用网上，实现简单、方便、灵活，但同时其安全问题也更为突出。企业必须确保其 VPN 上传送的数据不被攻击者窥视和篡改，并且要防止非法用户对网络资源或私有信息的访问　Extranet VPN 将企业网扩展到合作伙伴和客户，对安全性提出了更高的要求。安全问题是 VPN 的核心问题。目前，VPN 的安全保证主要是通过防火墙技术、路由器配以隧道技术、加密协议和安全密钥来实现的，可以保证企业员工安全地访问公司网络。

（2）在网络优化方面，构建 VPN 的另一重要需求是充分有效地利用有限的广域网资源，

自考备考三件宝：自考笔记、真题及答案、录音课件！

qq953771558 examebook.com

为重要数据提供可靠的带宽。广域网流量的不确定性使其带宽的利用率很低，在流量高峰时引起网络阻塞，产生网络瓶颈，使实时性要求高的数据得不到及时发送；而在流量低谷时又造成大量的网络带宽空闲。QoS 通过流量预测与流量控制策略，可以按照优先级分配带宽资源，实现带宽管理，使得各类数据能够被合理地先后发送，并预防阻塞的发生。

（3）在 VPN 管理方面，VPN 要求企业将其网络管理功能从局域网无缝地延伸到公用网，甚至是客户和合作伙伴。虽然可以将一些次要的网络管理任务交给服务提供商去完成，企业自己仍需要完成许多网络管理任务。所以，一个完善的 VPN 管理系统是必不可少的。VPN 管理的目标为：减小网络风险、具有高扩展性、经济性、高可靠性等优点二事实上，VPN 管理主要包括安全管理、设备管理、配置管理、访问控制列表管理、QoS 服务质量管理等内容。

考试课件网：http://www.examebook.cn/
——我们专业提供自考易考题库课件集、自考免费电子书、自考历年真题及标准答案！

考试真题软件网：http://down.examebook.com/
——我们专业提供自考历年真题及答案整理版、自考考前模拟试题！

考试学习软件商城：http://www.examebook.com/
——为您提供各种考试学习软件课件更为便利的购买通道！

自考备考三件宝：自考笔记、真题及答案、录音课件！