绝密 ★ 考试结束前

全国2015年4月高等教育自学考试

电子商务安全导论试题

课程代码:00997

请考生按规定用笔将所有试题的答案涂、写在答题纸上。

选择题部分

注意事项:

1. 答题前,考生务必将自己的考试课程名称、姓名、准考证号用黑色字迹的签字笔或钢笔填写在答题纸规定的位置上。

2. 每小题选出答案后,用2B铅笔把答题纸上对应题目的答案标号涂黑。如需改动,用橡皮擦干净后,再选涂其他答案标号。不能答在试题卷上。

www.zikao365.com

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,请将其选出并将"答题纸"的相应代码涂黑。错涂、多涂或未涂均无分。

1. 电子商务发展的第一个浪潮是指

A. 网络基础设施大量兴建　　B. 应用软件及服务成为热点

C. portal公司的出现　　D. 零售业上网

2. 以下选项中不属于电子商务安全中心内容的是

A. 商务数据的完整性　　B. 商务数据的机密性

C. 商务服务的不可否认性　　D. 商务对象的匿名性

3. 使用凯撒密码,Key=3,原文m=ecommerce,则密文是

A. ECOMMERCE　　B. HFRPPHUFH　　C. ecommerce　　D. hfrpphufh

4. 最早提出的公开的密钥交换协议是

A. Blom协议　　B. Euclid协议

C. Skipjack协议　　D. Diffie-Hellman协议

5. 散列函数SHA的输出压缩值为

A. 64比特　　B. 128比特　　C. 160比特　　D. 192比特

6. 在数字信封技术中,加密发送方随机产生的DES密钥采用的密钥是

A. 发送方的公钥　　B. 接受方的公钥　　C. 发送方的私钥　　D. 接受方的私钥

7. 计算机机房设计中，机房环境、电源及防雷接地应满足

A. 电子计算机机房设计规范

B. 计算机房场、地、站安全要求

C. 建筑与建筑群综合布线系统工程设计规范

D. 电器装置安装工程、接地装置施工及验收规范

8. 下列防病毒软件中属于国产的是

A. kv3000　　B. nod32　　C. Norton　　D. McAfee

9. 在使用防火墙技术加强网络安全后，DMZ 位于

A. 内网　　B. 外网　　C. Intranet　　D. Internet

10. 下列选项中，不属于 VPN 具有的功能是

A. 加密数据　　B. 信息认证　　C. 信息过滤　　D. 身份认证

11. 接入控制机构的建立主要根据三种类型的信息，其中主体又可为多种实体，以下实体中属于主体的是

A. 用户　　B. 数据文件

C. 程序组　　D. 数据库

www.zikao365.com

12. 对数据库的加密方法通常有多种，将加密方法嵌入 DBMS 的源代码，使加密方法与数据库永久地捆绑的方法属于

A. 使用加密软件加密数据库　　B. 使用专用硬件加密数据库

C. 使用专用软件加密数据库数据　　D. 使用加密桥技术

13. 实现身份证明的途径有多种，出示个人所具有的东西，如护照属于

A. 所知　　B. 所有　　C. 个人特征　　D. 动作特征

14. 在 Kerberos 的认证过程中，Client 向本域内的服务器申请服务的过程为三个阶段，以下描述属于第 2 阶段的是

A. 客户向 TGS 请求服务的服务许可证　　B. 客户向 AS 申请服务

C. 客户向 AS 申请得到注册许可证　　D. 客户向 Server 申请服务

15. 证实电子邮件用户身份和公钥的证书为

A. 客户证书　　B. 服务证书　　C. 服务器证书　　D. 安全邮件证书

16. CA 系统由多个部分构成，其中负责证书的签发的服务器是

A. 安全服务器　　B. CA 服务器　　C. 数据库服务器　　D. LDAP 服务器

17. 提供安全的电子商务数据交换的协议是

A. SSL　　B. SET　　C. TLS　　D. IP

18. 关于 SET 与 SSL 说法正确的是

A. SSL 的安全性要求更高　　B. SSL 的客户和商家都必须申请数字证书

C. SET 的普及率更高　　D. SET 需要安装专门的软件

19. CFCA 金融认证服务的相关规则中要求持卡人网上业务的资格包含

A. 拥有数字证书　　B. 拥有微信

C. 拥有 5 万的定期存单　　D. 拥有信用卡

20. 上海市电子商务安全证书管理中心的简称是

A. SHEC　　B. SHECA　　C. SHECB　　D. CTCA

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，请将其选出并将“答题纸”的相应代码涂黑。错涂、多涂、少涂或未涂均无分。

21．接入控制策略包含多种，其中多级安全策略的主体和客体划分为多级，具体包含

A．内部　　B．秘密　　C．机密

D．绝密　　E．普通

22．证书的网上申请方式包含

A．离线申请　　B. E-mail 申请　　C. WEB 申请

D．微信申请　　E. QQ 在线申请

23．以下哪些性能是 PKI 必须具有的？

A．多政策支持　　B．易用性　　C．多平台

D．完整性　　E．机密性

www.zikao365.com

24．SSL 体系结构包含的协议有

A．SSL 连接协议　　B．SSL 警告协议　　C．SSL 认证协议

D．SSL 握手协议　　E．SSL 记录协议

25．参与建立 CFCA 的银行有

A．招商银行　　B．光大银行　　C．汇丰银行

D．华夏银行　　E．平安银行

非选择题部分

注意事项：

用黑色字迹的签字笔或钢笔将答案写在答题纸上，不能答在试题卷上。

三、填空题　（本大题共 5 小题，每小题 2 分，共 10 分）

26．我们一般把电子数据交换看做是_____或_____的电子商务。

27．密码技术是保证_____、_____安全的核心技术。

28．MD-4 散列算法的输入消息可以为任意长，按_____比特分组，最后的分组长度不足时，用数 0 填充，使其成为_____比特的整数倍。

29．IPSec 提供的安全服务包括私有性、_____、_____和重传保护，并制定了密钥管理的方法。

30．公钥-私钥对的管理包含公钥-私钥对的生成、_____、_____、更新、暂停使用、吊销注册等。

四、名词解释题　（本大题共 5 小题，每小题 3 分，共 15 分）

31．远程镜像磁盘

32．良性病毒

33．单位注册机构

34．TGS

35．根通行字

www.zikao365.com

五、简答题　（本大题共 6 小题，每小题 5 分，共 30 分）

36．什么是数据机密性？

37．数据的完整被破坏以后，会产生什么样的严重后果？

38．Access VPN 对用户的吸引力体现在哪些方面？

39．简述证书链中证书复本的传播方式。

40．简述公钥-私钥对生成的两种途径。

41．简述 SSL 保证 Internet 上浏览器/服务器会话中认证性的机制。

六、论述题　（本大题共 1 小题，15 分）

42．比较 DES 与 RSA 算法的区别，并说明其不同的应用领域。