绝密 ★ 考试结束前

全国2019年10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。

一、单项选择题:本大题共20小题,每小题1分,共20分。在每小题列出的备选项中只有一项是最符合题目要求的,请将其选出。

1. 美国的橘皮书中为计算机安全的不同级别制定了4个标准:A、B、C、D级,其中B级又分为B1、B2、B3三个子级,C级又分为C1、C2两个子级。以下按照安全等级由低到高排列正确的是

A. A、B1、B2、B3、C1、C2、D

B. A、B3、B2、B1、C2、C1、D

C. D、C1、C2、B1、B2、B3、A

D. D、C2、C1、B3、B2、B1、A

2. 以下不属于电子商务遭受的攻击是

A. 病毒　　B. 植入　　C. 加密　　D. 中断

3. 第一个既能用于数据加密、又能用于数字签名的算法是

A. DES　　B. EES　　C. IDEA　　D. RSA

4. 下列属于单钥密码体制算法的是

A. RC-5加密算法　　B. RSA密码算法

C. ELGamal密码体制　　D. 椭圆曲线密码体制

5. MD5散列算法的分组长度是

A. 16比特　　B. 64比特　　C. 128比特　　D. 512比特

6. 充分发挥了 DES 和 RSA 两种加密体制的优点，妥善解决了密钥传送过程中的安全问题的技术是

A. 数字签名　　B. 数字指纹

C. 数字信封　　D. 数字时间戳

7.《电气装置安装工程、接地装置施工及验收规范》的国家标准代码是

A. GB50174-93　　B. GB9361-88

C. GB2887-89　　D. GB50169-92

8. 按照《建筑与建筑群综合布线系统工程设计规范》（CECS 72：97）的要求，设备间室温应保持的温度范围是

A. 0℃-10℃　　B. 10℃-25℃　　C. 0℃-25℃　　D. 25℃-50℃

9. 内网是指

A. 受信网络　　B. 非受信网络　　C. 防火墙外的网络　　D. 互联网

10. 检查所有进出防火墙的包标头内容的控制方式是

A. 包过滤型　　B. 包检验型　　C. 应用层网关型　　D. 代理型

11. 对数据库的加密方法通常有多种，以下软件中，属于使用专用加密软件加密数据库数据的软件是

A. Microsoft Access　　B. Microsoft Excel

C. DOMINO　　D. LOTUS

12. Kerberos 域内认证过程的第一个阶段是

A. 客户向 AS 申请得到注册许可证

B. 客户向 TGS 申请得到注册许可证

C. 客户向 Server 申请得到注册许可证

D. 客户向 Workstation 申请得到注册许可证

13. Client 向本 Kerberos 的认证域以外的 Server 申请服务的过程分为

A. 4 个阶段，共 6 个步骤　　B. 3 个阶段，共 6 个步骤

C. 3 个阶段，共 8 个步骤　　D. 4 个阶段，共 8 个步骤

14. 下列哪一项是将公钥体制用于大规模电子商务安全的基本要素？

A. 数字证书　　B. 密钥　　C. 公钥证书　　D. 公钥对

15. 对 PKI 的最基本要求是

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

16. 在 PKI 的构成模型中，其功能不包含在 PKI 中的机构是

A. CA　　B. ORA　　C. PAA　　D. PMA

17. 在 Internet 上建立秘密传输信息的信道，保障传输信息的机密性、完整性与认证性的协议是

A. HTTP　　B. FTP　　C. SMTP　　D. SSL

18. 在 SET 协议中用来确保交易各方身份真实性的技术是

A. 加密方式

B. 数字化签名

C. 数字化签名与商家认证

D. 传统的纸质上手工签名认证

19. 牵头建立中国金融认证中心的银行是

A. 中国银行　　B. 中国人民银行

C. 中国建设银行　　D. 中国工商银行

20. CFCA 推出的一套保障网上信息安全传递的完整解决方案是

A. TruePass　　B. Entelligence　　C. Direct　　D. LDAP

二、多项选择题：本大题共 5 小题，每小题 2 分，共 10 分。在每小题列出的备选项中至少有两项是符合题目要求的，请将其选出，错选、多选或少选均无分。

21. 将自然语言格式转换成密文的基本加密方法有

A. 替换加密　　B. 转换加密

C. DES 加密　　D. RSA 加密

E. IDEA 加密

22. 数字签名可以解决下述哪些安全鉴别问题？

A. 发送者伪造　　B. 发送者或接收者否认

C. 第三方冒充　　D. 接收方篡改

E. 传输过程中被非法截取

23. 计算机病毒的主要来源有

A. 非法拷贝引起的病毒　　B. 通过互联网络传入的病毒

C. 有人研制和改造的病毒　　D. 一些游戏软件染有的病毒

E. 引进的计算机系统和软件中带有的病毒

24. 防火墙的基本组成有

A. 安全操作系统　　B. 过滤器

C. 网关　　D. 域名服务和 E-mail 处理

E. 网络管理员

25. 为保证电子商务交易的有效性，在技术手段上必须要

A. 采用加密措施　　B. 反映交易者的身份

C. 保证数据的完整性　　D. 提供数字签名功能

E. 保证交易信息的安全

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. 商务对象的认证性是指网络两端的使用者在沟通之前相互确定对方的身份，保证身份的正确性，分辨参与者所声称身份的真伪，防止_____攻击。认证性用_____和身份认证技术实现。

27. 对数据库的加密方法有三种：使用加密软件加密、_____、_____。

28. 身份证明可以依靠_____、_____和个人特征这 3 种基本途径之一或它们的组合来实现。

29. SET 是一种以_____为基础的、在 Internet 上交易的付款协议，是授权业务信息传输的安全标准，它采用 RSA 密码算法，利用_____体系对通信双方进行认证。

30. 中国金融认证中心（China Financial Certification Authority，简称 CFCA）专门负责为电子商务的各种认证需求提供_____服务，为参与网上交易的各方提供信息安全保障，实现互联网上电子交易的保密性、真实性、_____和不可否认性。

四、名词解释题：本大题共 5 小题，每小题 3 分，共 15 分。

31. VPN

32. 接入控制

33. 多公钥证书系统

34. 源的不可否认性

35. 网上银行

五、简答题：本大题共 6 小题，每小题 5 分，共 30 分。

36. 简述 RSA 数字签名体制的安全性。

37. 数据文件和系统的备份要注意什么？

38. 作为 VPN 的基础的隧道协议主要包括哪几种？

39. 简述通过广播方式公布 CRL 存在的问题。

40. 简述解决纠纷的步骤。

41. SET 的主要安全保障来自哪几个方面？

六、论述题：本大题共 1 小题，共 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。