绝密★启用前

2022年4月高等教育自学考试全国统一命题考试

电子商务安全导论

（课程代码　00997）

注意事项：

1. **本试卷分为两部分，第一部分为选择题，第二部分为非选择题。**
2. **应考者必须按试题顺序在答题卡（纸）指定位置上作答，答在试卷上无效。**
3. **涂写部分、画图部分必须使用2B铅笔，书写部分必须使用黑色字迹签字笔。**

第一部分　选择题

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. 电子邮件的安全问题主要是
   A. 传输丢失　　B. 传输到错误地址
   C. 传输错误　　D. 传输时可能被人窃取
2. 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，是电子商务安全六项中的
   A. 商务服务的不可否认性　　B. 商务服务的不可拒绝性
   C. 商务对象的认证性　　D. 商务数据的完整性
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
   A. AES　　B. DES
   C. RSA　　D. RC-5
4. 在电子商务的安全需求中，交易过程中必须保证信息不会泄露给非授权的人或实体指的是
   A. 可靠性　　B. 真实性
   C. 机密性　　D. 完整性
5. 在数字时间戳仲裁方案里，下列选项中与时戳一起返还的是
   A. 明文　　B. 密文
   C. 杂凑函数值　　D. 加密函数
6. SHA的含义是
   A. 安全散列算法　　B. 密钥
   C. 数字签名　　D. 消息摘要

7. 《计算机场、地、站技术要求》的国家标准代码是
   A. GB50174-93　　B. GB9361-88
   C. GB2887-89　　D. GB50169-92
8. UPS电源应该提供的后备供电能力不低于
   A. 1小时　　B. 2小时
   C. 3小时　　D. 4小时
9. 用来解决网络延迟和阻塞等问题的一种技术是
   A. QoS　　B. DMZ
   C. IPSec　　D. RIP
10. 防火墙能解决的问题是
    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
11. 在接入控制中，对目标进行访问的实体是
    A. 程序组　　B. 客体
    C. 数据库　　D. 主体
12. 为数据库加密字段的存储、检索、索引、运算、删除、修改等功能的实现提供接口的技术是
    A. 数字签名　　B. 消息摘要
    C. 双密钥机制　　D. 加密桥技术
13. CA服务器产生自身的私钥和公钥，密钥长度至少为
    A. 128位　　B. 256位
    C. 512位　　D. 1024位
14. 在VeriSign申请个人数字证书，其试用期为
    A. 45天　　B. 60天
    C. 75天　　D. 90天
15. 在PKI构成模式中，制定整个体系结构的安全政策和所有下级机构都需要遵循的规章制度的是
    A. 证书管理机构　　B. 政策审批机构
    C. 单位注册机构　　D. 政策管理机构
16. PKI的服务不包括
    A. 数据压缩　　B. 数据完整性
    C. 数据保密性　　D. 不可否认性
17. Visa和Master Card公司为了确保SET软件符合规范要求，在SET发表后，建立的规则是
    A. SETCo　　B. SSL
    C. SET Toolkit　　D. GCA

18. 确保交易各方身份的真实性是通过数字签名和

A. 加密　　B. 商家认证

C. SET　　D. SSL

19. 在 CFCA 体系结构中，由 CA 系统和证书注册审批机构组成的是

A. 运营 CA　　B. 政策 CA

C. 根 CA　　D. 技术 CA

20. 承担证书签发、审批、废止等服务的系统是

A. RA 系统　　B. CA 系统

C. CFCA 认证系统　　D. PKI 系统

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. 攻击 Web 站点的方式有

A. 安全信息被破译

B. 非法访问

C. 交易信息被截获

D. 软件漏洞被攻击者利用

E. 远程下载

22. 单钥密码体制的算法有

A. DES 加密算法　　B. IDEA 加密算法

C. RC-5 加密算法　　D. AES 加密算法

E. RSA 加密算法

23. 数字签名可以解决下列哪些安全鉴别问题？

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. 文件内容加密

24. 防火墙的基本组成包括

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. 参与中国金融认证中心建设的机构有

A. 中国工商银行　　B. 深圳发展银行

C. 广东发展银行　　D. 上海浦东发展银行

E. 汉口银行

第二部分　非选择题

三、填空题：本大题共 5 小题，每小题 2 分，共 10 分。

26. 数据库加密软件的特点是将_____和_____永久捆绑在一起。

27. Kerberos 系统由_____、_____、Client、Server 共 4 个部分组成。

28. 公钥证书系统按用户所需的 CA 个数分类，可分为_____和_____。

29. 电子钱包软件可以从_____和_____得到。

30. SHECA 数字证书根据应用对象可以将其分为_____和_____。

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

32. 归档

33. 域内认证

34. 单公钥证书系统

35. 源的不可否认性

五、简答题：本大题共 6 小题，每小题 5 分，共 30 分。

36. 简述电子商务安全的中心内容。

37. 简述 IDEA 加密算法的基本运算、设计思想及加密过程。

38. 简述数据文件和系统的备份需要注意的问题。

39. VPN 提供的功能有哪些？

40. 有效证书应满足的条件有哪些？

41. 简述 SSL 加密协议的用途。

六、论述题：本大题共 1 小题，15 分。

42. 试述 SET 和 SSL 在现实网上交易中的异同。