机密 ★ 考试结束前

2024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

1. 请考生按规定用笔将所有试题的答案涂、写在答题纸上。

2. 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。

选择题部分

注意事项:

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. 未经授权通过一定手段假冒合法用户接入系统,对文件进行篡改、窃取机密信息、非法使用资源,这是电子商务系统遭到了

A. 病毒攻击　　B. 植入攻击

C. 通信窜扰攻击　　D. 系统穿透攻击

2. 美国的橘黄皮书中为计算机安全的不同级别制定了4个标准:D级、C级、B级、A级,由低到高。B级分为B1、B2、B3三个子级,B2级也称为

A. 访问控制保护级　　B. 带标签的安全性保护

C. 结构化防护　　D. 安全域级

3. IDEA的输入与密钥长度分别为

A. 64位,64位　　B. 64位,128位　　C. 32位,64位　　D. 32位,32位

4. 美国政府在1993年公布的EES技术所属的密钥管理技术是

A. 密钥的托管　　B. 密钥的存储　　C. 密钥的分配　　D. 密钥的设置

5. 在签名人合作下才能验证签名的签名为

A. 双联签名　　B. 盲签名　　C. RSA签名体制　　D. 无可争辩签名

6. 计算机机房的设备间室温和相对湿度应分别保持在

A. 10℃~25℃,40%~60%　　B. 20℃~30℃,40%~60%

C. 10℃~25℃,60%~80%　　D. 20℃~30℃,60%~80%

7. 下列选项中全部属于恶性病毒的是

A. 小球病毒、扬基病毒　　B. 黑色星期五病毒、火炬病毒

C. 火炬病毒、扬基病毒　　D. 黑色星期五病毒、Dabi 病毒

8. 在防火墙技术中,非军事化区这一概念通常指的是

A. 互联网与内部网中的隔离带　　B. 非受信网络

C. 受信网络　　D. INTERNET

9. 企业员工或企业的小分支机构通过公网远程拨号的方式构筑的虚拟网称为

A. Intranet VPN　　B. Access VPN

C. Extranet VPN　　D. Internet VPN

10. MAC 的含义是

A. 自主式接入控制　　B. 强制式接入控制

C. 数据存储控制　　D. 数据自动控制

11. 将加密方法嵌入 DBMS 的源代码,使其和数据库永久地捆绑在一起的方法属于

A. 使用加密软件加密　　B. 使用加密桥技术

C. 使用专用软件加密数据库数据　　D. 使用专用硬件加密

12. Client 向本 Kerberos 的认证域以外的 Server~申请服务的过程分为 4 个阶段,以下描述属于第 2 阶段的是

A. Client↔AS　　B. Client↔TGS~

C. Client↔TGS　　D. Client↔Server~

13. 证实电子邮件用户身份和公钥的证书为

A. 客户证书　　B. 服务器证书　　C. CA 证书　　D. 安全邮件证书

14. 一个典型的 CA 系统由多个服务器组成,负责证书签发的服务器是

A. 安全服务器　　B. 数据库服务器

C. LDAP 服务器　　D. CA 服务器

15. 作为网络环境的基础设施,PKI 必须具有良好的

A. 透明性和易用性　　B. 简单的风险管理

C. 互操作性　　D. 支持多政策

16. 不可否认业务中,用来保护收信人的是

A. 源的不可否认性　　B. 提交的不可否认性

C. 委托的不可否认性　　D. 递送的不可否认性

17. SET 协议中能确保数据完整性的安全保障措施是

A. 单密钥加密　　B. 双密钥加密　　C. 密钥分配　　D. 数字化签名

18. 最常见的用来保护 HTTP 通信的协议是

A. TCP/IP　　B. FTP　　C. SSL　　D. SMTP

19. CFCA 认证系统采用国际领先的 PKI 技术,总体为三层 CA 结构,第二层为

A. 权限 CA　　B. 根 CA　　C. 政策 CA　　D. 运营 CA

20. SHECA 证书的对称加密算法支持

A. 64 位　　B. 128 位　　C. 256 位　　D. 512 位

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. 下列选项中属于单钥密码体制算法的有

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

22. 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

A. 不同主机　　B. 不同操作系统　　C. 不同数据库管理系统

D. 不同国家语言　　E. 不同应用开发环境

23. 公钥证书数据的组成,包括

A. 版本信息　　B. 证书序列号　　C. CA 所使用的签名算法

D. 有效使用期限　　E. 证书主题名称

24. PKI 应用实例包括

A. 虚拟专用网络　　B. 安全电子邮件　　C. Web 安全

D. 电子商务的应用　　E. 应用编程接口 API

25. SET 安全协议要达到的主要目标有

A. 信息的安全传输　　B. 信息的相互隔离　　C. 多方认证的解决

D. 证书的安全发放　　E. 交易的实时性

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. 双钥密码体制又称作_____体制或_____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,一个用于加密,另一个用于解密。

27. 计算机病毒按寄生方式分为_____病毒、_____病毒和复合型病毒。

28. Kerberos 是一种典型的用于_____和_____认证的认证体系协议,它是一种基于对称密码体制的安全认证服务系统。

29. 散列函数是将一个长度不确定的输入串转换成一个长度确定的输出串——称为_____,也叫哈希值、杂凑值和_____。

30. CRL 吊销的方式有_____和_____。

四、名词解释(本大题共 5 小题,每小题 3 分,共 15 分)

31. 电子商务 B-C 模式

32. 加密算法

33. 计算机病毒

34. 防火墙

35. 支付网关

五、简答题(本大题共 6 小题,每小题 5 分,共 30 分)

36. 简述 DES 的加密运算法则。

37. 简述数字签名可以解决的安全鉴别问题。

38. 简述对密钥进行安全保护的措施。

39. 简述一个大系统的通行字的选择原则。

40. 简述选择 VPN 解决方案时需要考虑的要点。

41. 简述 SSL 协议的用途。

六、论述题(本大题 15 分)

42. 请说明从机制上如何实现电子商务的不可否认性。