绝密 ★ 考试结束前

全国2017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. 网上商店的模式为

A. B-B　　B. B-C　　C. C-C　　D. B-G

2. 为了确保数据的完整性,SET协议是通过

A. 单密钥加密来实现　　B. 双密钥加密来实现

C. 密钥分配来实现　　D. 数字化签名来实现

3. 下面不属于SET交易成员的是

A. 持卡人　　B. 电子钱包　　C. 支付网关　　D. 发卡银行

4. CFCA认证系统的第二层为

A. 根CA　　B. 政策CA　　C. 运营CA　　D. 审批CA

5. 托管加密标准EES的托管方案是通过什么芯片来实现的?

A. DES算法芯片　　B. 防窜扰芯片

C. RSA算法芯片　　D. VPN算法芯片

6. 数字信封中采用的加密算法是

A. AES　　B. DES　　C. RC-5　　D. RSA

7. 在电子商务中,保证认证性和不可否认性的电子商务安全技术是

A. 数字签名　　B. 数字摘要　　C. 数字指纹　　D. 数字信封

8．在防火墙技术中，非军事化区这一概念通常指的是

A．受信网络　　B．非受信网络

C．内网和外网中的隔离带　　D．互联网

9．下列不属于 Internet 的接入控制技术主要对付的入侵者是

A．伪装者　　B．病毒　　C．违法者　　D．地下用户

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

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．CA 不能提供以下哪种证书?

A．SET 服务器证书　　B．SSL 服务器证书

C．安全电子邮件证书　　D．个人数字证书

12．LDAP 服务器提供

A．目录服务　　B．公钥服务　　C．私钥服务　　D．证书服务

13．在 PKI 的性能要求中，电子商务通信的关键是

A．支持多政策　　B．支持多应用　　C．互操作性　　D．透明性

14．根据《建筑与建筑群综合布线系统工程设计规范》(CECS72：97)的要求，计算机机房室温应该保持的温度范围为

A．0℃～5℃　　B．5℃～10℃

C．5℃～15℃　　D．10℃～25℃

15．在域内认证中，TGS 生成用于 Client 和 Server 之间通信的会话密钥 Ks 发生在

A．第 1 个阶段第 2 个步骤

B．第 2 个阶段第 1 个步骤

C．第 2 个阶段第 2 个步骤

D．第 3 个阶段第 1 个步骤

16．在 PKI 的性能中，下列哪些服务是指从技术上保证实体对其行为的认可？

A．认证　　B．数据完整性

C．数据保密性　　D．不可否认性

17．对 Internet 的攻击的四种类型不包括

A．截断信息　　B．伪造　　C．病毒　　D．　篡改

18．AES 支持的密钥长度不可能是

A．64　　B．128　　C．192　　D．256

19．以下不是计算机病毒主要来源的是

A．非法拷贝中毒

B．引进的计算机系统和软件中带有病毒

C．通过 Internet 传入

D．隔离不当

20．VPN 不能提供的功能是

A．加密数据　　B．信息认证和身份认证

C．提供访问控制　　D．包过滤

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．实现递送的不可否认性的方式有

A．收信人签字认可　　B．收信人利用持证认可

C．可信赖递送代理　　D．逐级递送报告

E．数字加密

22．电子商务系统可能遭受的攻击有

A．系统穿透　　B．违反授权原则

C．植入　　D．通信监视

E．拒绝服务

23．SET 交易成员有

A．持卡人　　B．网上商店

C．收单银行　　D．认证中心 CA

E．支付网关

24．CTCA 采用分级结构管理，其组成包括

A．全国 CA 中心　　B．省级 CA 中心

C．省级 RA 中心　　D．地市级 RA 中心

E．地市级业务受理点

25．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

A．双重 DES　　B．三重 DES

C．RSA　　D．IDEA

E．RC-5

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 10 空，每空 1 分，共 10 分。

26．网上银行业务中，用户对其发出的指令用其_____进行签名，银行校验签名并保存此次签名，从而使银行用户所发出的指令具有_____。

27．数字签名分为两种，其中 RSA 和 Rabin 签名属于_____签名，ELGamal 签名属于_____签名。

28．数字信封既克服了两种加密体制的缺点，发挥了两种加密体制的优点，又妥善的解决了_____的传送的_____问题。

29．为了对证书进行有效的管理，证书实行_____管理，认证机构采用了_____结构，证书可以通过一个完整的安全体系得以验证。

30．根据近代密码学的观点，一个密码系统的安全性取决于对_____的保护，而不取决于对_____的保密。

四、名词解释题：本大题共 5 小题，每小题 3 分，共 15 分。

31．Externet

32．TLS 协议

33．数据完整性

34．IPSec

35．域间认证

五、简答题：本大题共 6 小题，每小题 5 分，共 30 分。

36．简述三种基本的备份系统。

37．防火墙不能解决的问题有哪些？

38．接入控制策略有哪几种？

39．一个大的实际系统中，通行字的选择原则是什么？

40．请列出公钥证书的类型并简述其作用。

41．电子商务的真实性的含义是什么？

六、论述题：本大题共 1 小题，15 分。

42．论述证书系统的组成并分析证书机构的管理功能。