全国 2014 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。

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．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、Cl、D

C.D、Cl、C2、B1、B2、B3、A

D.D、C2、C1、B3、B2、Bl、A

2.在维护系统的安全措施中，保护数据不被未授权者建立的业务是

A.保密业务 B.认证业务

C.数据完整性业务 D.不可否认业务

3.Diffie 与 Hellman 早期提出的密钥交换体制的名称是

A.DES B.EES

C.RSA D.Diffie-Hellman

4.以下加密体制中，属于双密钥体制的是

A.RSA B.IDEA

C.AES D.DES

5.对不知道内容的文件签名称为

A.RSA 签名 B.ELgamal 签名

C.盲签名 D.双联签名

6.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

7.按照《建筑与建筑群综合布线系统工程设计规范》(CECS72：97)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℃

8.通过公共网络建立的临时、安全的连接，被称为

A.EDI B.DSL

C.VLN D.VPN

9.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

10.在接入控制策略中，按主体执行任务所知道的信息最小化的原则分配权力的策略是

A.最小权益策略 B.最大权益策略

C.最小泄露策略 D.多级安全策略

11.Microsoft Access 数据库的加密方法属于

A.单钥加密算法 B.双钥加密算法

C.加密桥技术 D.使用专用软件加密数据

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.Kerberos 域间认证分为 4 个阶段，其中第 3 阶段是（～代表其它 Kerberos 的认证域）

A. Client↔AS B. Client↔TGS～

C. Client↔TGS D. Client↔Server～

14.证明双钥体制中公钥的所有者就是证书上所记录的使用者的证书是

A.双钥证书 B.公钥证书

C.私钥证书 D.CA 证书

15.通常将用于创建和发放证书的机构称为

A.RA B.LDAP

C.SSL D.CA

16.在 PKI 的构成中，负责制定整个体系结构的安全政策的机构是

A.CA B.PAA

C.OPA 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.计算机病毒的特征有

A.非授权可执行

B.隐蔽性

C.潜伏性

D.不可触发性

E.表现性

22.接入控制的功能有

A.阻止非法用户进入系统

B.强制接入

C.自主接入

D.允许合法用户进入系统

E.使合法人按其权限进行各种信息活动

23.Kerberos 域内认证过程的第一阶段的第一步中 Client 向 AS 传递的信息有

A.IDc

B.IDserver

C.IDTGS

D.时间戳 a

E.ADclient

24.检验证书有效必须满足的条件有

A.证书没有超过有效期

B.密钥没有被修改

C.证书没有使用过

D.证书持有者合法

E.证书不在 CA 发行的无效证书清单中

25.SET 安全协议要达到的主要的目标是

A.结构的简单性

B.信息的相互隔离

C.多方认证的解决

D.交易的实时性

E.信息的安全传递

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.DES加密算法中，每次取明文的连续_____位数据，利用64位密钥，经过_____轮循环加密运算，将其变成64位的密文数据。

28.IPsec有两种工作模式，_____为源到目的之间已存在的IP包提供安全性；_____则把一个IP包放到一个新的IP包中，并以IPsec格式发往目的地。

29.关于公钥证书的吊销，_____方式有一定的延迟，_____可以避免此风险。

30.SSL依靠证书来检验通信双方的身份，在检验证书时，_____和_____都检验证书，看它是否由它们所信任的CA发行。如果CA是可信任的，则证书被接受。

四、名词解释题（本大题共5小题，每小题3分，共15分）

31.系统穿透

32.良性病毒

33.Kerberos

34.单公钥证书系统

35.认证服务

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六项中心内容。

37.简述双密钥体制的特点。

38.简述RSA数字签名体制的安全性。

39.简述按照VPN的部署模式，VPN可以分为哪三类？

40.简述PKI作为安全基础设施，为不同的用户按不同的安全需求提供的安全服务包括哪些？

41.简述在不可否认业务中，源的不可否认性可以提供证据解决哪些可能的纠纷？

六、论述题（本大题共1小题，15分）

42.详述数字签名的原理及其现实意义。