绝密 ★ 考试结束前

全国2020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. 电子商务安全的中心内容中，用来保证为用户提供稳定服务的是

A. 商务数据的完整性　　B. 商务对象的认证性

C. 商务服务的不可否认性　　D. 商务服务的不可拒绝性

2. 通过破坏计算机系统中的硬件、软件或线路，使得系统不能正常工作，这种电子商务系统可能遭受的攻击是

A. 系统穿透　　B. 中断

C. 拒绝服务　　D. 通信窜扰

3. 最早提出的公开的密钥交换协议是

A. Blom　　B. ELGamal

C. Diffie-Hellman　　D. Shipjack

4. DES的加密算法是每次取明文中的连续

A. 256位　　B. 128位

C. 64位　　D. 32位

5. 在签名人合作下才能验证的签名为

A. 无可争辩签名　　B. 双联签名

C. 盲签名　　D. RSA签名

6. 为了保证电子商务安全中的认证性和不可否认性，必须采用的技术是

A. 数字签名　　B. 散列函数

C. 身份认证　　D. 数字时间戳

7．建立计算机及其网络设备的物理环境，必须要满足《建筑与建筑群综合布线系统工程设计规范》的要求，计算机机房的室温应保持在

A．8℃至20℃之间　　B．10℃至25℃之间

C．10℃至28℃之间　　D．15℃至30℃之间

8．在计算机机房设计中，设备间应采用UPS不间断电源，UPS功率大小应根据网络设备功率进行计算，并应具有的余量是

A．5%～10%　　B．10%～20%

C．15%～20%　　D．20%～30%

9．在防火墙使用的控制技术中通过一个检验模组对包中的各个层次作检验的是

A．包过滤型　　B．包检验型

C．应用层网关型　　D．代理服务型

10．内网指的是

A．受信网络　　B．非受信网络

C．防火墙外的网络　　D．互联网

11．使用加密软件加密数据时，往往使用数据库系统自带的加密方法加密数据，实施

A．DAC　　B．DCA

C．MAC　　D．CAM

12．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

13．在下列选项中，不是每一种身份证明系统都必须要求的是

A．不具可传递性　　B．计算有效性

C．通信有效性　　D．可证明安全性

14．Kerberos的域内认证过程共分3个阶段，共6个步骤。在第1个阶段的第1个步骤，客户向AS发送的信息不包含

A．IDClient　　B．IDTGS

C．IDServer　　D．时间戳a

15．公钥证书的内容包含

A．版本信息　　B．私钥

C．用户的签名算法　　D．CA的公钥信息

16．以下不属于PKI的性能要求的是

A．透明性和易用性　　B．可操作性

C．可移植性　　D．支持多平台

17．下列选项中，给Internet上很多软件提供签名认证服务的公司是

A．Baltimore　　B．Entrust

C．VeriSign　　D．Sun

18．SSL 握手协议的主要步骤有

A．三个　　B．四个

C．五个　　D．六个

19．牵头建立中国金融认证中心（CFCA）的机构是

A．招商银行　　B．中国电信

C．中国移动　　D．中国人民银行

20．下列不属于 SHECA 证书管理器的操作范围的是

A．个人证书的操作　　B．对根证书的操作

C．对他人证书的操作　　D．服务器证书的操作

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．在 20 世纪 90 年代末期，大力推动电子商务发展的有

A．信息产品硬件制造商　　B．大型网上服务厂商

C．政府　　D．银行及金融机构

E．零售服务商

22．防雷接地设置接地体时，保护地线的接地电阻值分别不应大于

A．1Ω　　B．2Ω

C．3Ω　　D．4Ω

E．5Ω

23．Internet 的接入控制主要对付

A．伪装者　　B．违法者

C．地下用户　　D．病毒

E．木马

24．VeriSign 将数字证书分为多类，具体包含

A．个人　　B．单位

C．服务器　　D．计算机网络

E．软件

25．在 SET 文件中规范了商店服务器的核心功能是

A．联系客户端的电子钱包

B．联系支付网关

C．向商店的认证中心查询数字证书的状态

D．处理 SET 的错误信息

E．处理客户的付款信息

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. 计算机病毒的特征包括非授权可执行性、隐蔽性、_____、_____、破坏性、可触发性。
27. 接入控制机构由用户的认证与_____、对认证的用户进行_____两部分组成。
28. Client 向本 Kerberos 的认证域以外的 Server 申请服务的过程分为_____个阶段，共_____个步骤。
29. 密钥管理是最困难的安全性问题，其中密钥的_____和_____可能是最棘手的。
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. 数字签名
32. 网络系统物理安全
33. Intranet VPN
34. 单公钥证书系统
35. 公证服务

五、简答题：本大题共 6 小题，每小题 5 分，共 30 分。

36. 电子邮件的安全问题是什么？
37. 简述双钥密码体制的加密和解密过程。
38. 数字签名与消息的真实性认证有什么不同？
39. 简述选择 VPN 解决方案时需要考虑的要点。
40. 简述有效证书应满足的条件。
41. 简述 SSL 加密协议的用途及其工作原理。

六、论述题：本大题共 1 小题，15 分。

42. SET 与 SSL 都是为了实现一种安全的网上交易，试述它们的不同点。