绝密★启用前

2023年10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．网上商店的模式为

A．B-B　　B．B-C

C．C-C　　D．B-G

2．对Internet的攻击的四种类型不包括

A．截断信息　　B．伪造

C．篡改　　D．病毒

3．最早提出的公开的密钥交换协议是

A．Blom　　B．Diffie-Hellman

C．ELGamal　　D．Shipjack

4．目前常用的密钥托管算法是

A．EES算法　　B．Skipjack算法

C．Diffie-Hellman算法　　D．RSA算法

5．利用双钥密码体制的RSA加密算法实现数字签名的是

A．RSA签名体制　　B．无可争辩签名

C．盲签名　　D．双联签名

6．在数字信封中，先用来打开数字信封的是

A．公钥　　B．私钥

C．DES密钥　　D．RSA密钥

7．消息用散列函数处理得到的是

A．公钥　　B．私钥

C．消息摘要　　D．数字签名

8．具有引导型病毒和文件型病毒寄生方式的计算机病毒称为

A．引导型病毒　　B．文件型病毒

C．恶性病毒　　D．复合型病毒

9．《电气装置安装工程、接地装置施工及验收规范》的国家标准代码是

A．GB9361-88　　B．GB2887-89

C．GB50169-92　　D．GB50174-93

10．下列不是防火墙控制技术的是

A．包过滤　　B．包检验

C．VPN　　D．应用层网关

11．由资源拥有者分配接入权的接入控制方式是

A．自主式接入控制　　B．强制式接入控制

C．随机式接入控制　　D．半强制式接入控制

12．下列不属于接入控制功能的是

A．阻止非法用户进入系统

B．允许合法用户进入系统

C．防止用户浏览信息

D．使合法人按其权限进行各种信息活动

13．身份认证中证书的发行者是

A．政府机构　　B．认证授权机构

C．非盈利自发机构　　D．个人

14．Client向Kerberos的认证以外的Server申请服务的过程分为

A．3个阶段，共6个步骤　　B．3个阶段，共8个步骤

C．4个阶段，共6个步骤　　D．4个阶段，共8个步骤

15．网上交易各方在交易进行前对各自身份进行确认的一种手段是

A．证书　　B．公钥

C．私钥　　D．公钥-私钥对

16．Internet上很多软件的签名认证都来自

A．Baltimore公司　　B．Entrust公司

C．VeriSign公司　　D．Sun公司

17．在下列选项中，实现递送不可否认性的机制是

A．可信赖第三方数字签名　　B．可信赖第三方递送代理

C．可信赖第三方持证　　D．线内可信赖第三方

18．在 SET 系统运作中，支付网关安装在哪一方的计算机中？

A．持卡人　　B．网上商店

C．银行　　D．认证中心

19．CFCA 金融认证服务的相关规则中要求持卡人基本资格包含拥有

A．自己的有效身份证件　　B．数字证书

C．5 万的定期存单　　D．信用卡

20．以下不属于 SHECA 证书管理器的操作范围的是

A．对根证书的操作　　B．对个人证书的操作

C．对服务器证书的操作　　D．对他人证书的操作

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．Internet 系统包含的组成构件有

A．客户端软件　　B．客户端的操作系统

C．客户端的局域网　　D．服务器端的局域网

E．服务器上的 Web 服务器软件

22．单钥密码体制的特点有

A．加密和解密速度快　　B．加密和解密使用同一个密钥

C．加密和解密双方不需要保护密钥　　D．适用于大规模机器的相互通信

E．加密和解密效率不高

23．病毒的特征有

A．非授权可执行性　　B．隐蔽性

C．传染性　　D．潜伏性

E．可触发性

24．美国 LOTUS 公司的 DOMINO 群件开发系统的特点有

A．开发方便　　B．自带身份认证

C．自带密码系统　　D．操作方便

E．权限控制严格

25．得到电子钱包软件的方式有

A．银行网站下载　　B．SET 交易网站免费下载

C．软件开发商处购买　　D．软件开发商处下载

E．从他人拷贝

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．电子商务系统中，商务对象的认证用_____和_____技术实现。

27．电子商务的安全需求有_____、_____、机密性、完整性、有效性、不可抵赖性等。

28．一般来说，VPN 有_____、供应商—企业和_____三种部署模式。

29．SSL 协议中使用了_____、_____和数字签名与认证技术。

30．CFCA 证书包括_____、_____、手机证书和安全 E-mail 证书。

四、名词解释题：本大题共 5 小题，每小题 3 分，共 15 分。

31．访问的控制性

32．虚拟专用网 VPN

33．AS

34．公证服务

35．不可否认

五、简答题：本大题共 6 小题，每小题 5 分，共 30 分。

36．简述数据的完整性被破坏的严重后果。

37．简述双钥密码体制算法的特点。

38．简述数字签名可证明内容。

39．简述数据库的加密方法的种类。

40．简述隧道协议主要分类。

41．简述证书的类型。

六、论述题：本大题共 1 小题，15 分。

42．谈谈目前国内应用 SSL 和 SET 的情况。