座位号：

姓名：

机密★启用前

2025年10月高等教育自学考试全国统一考试

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．网上二手商品拍卖是

A．B—B电子商务　　B．B—C电子商务

C．C—C电子商务　　D．B—G电子商务

2．Extranet含义是

A．外联网　　B．物联网

C．互联网　　D．内联网

3．如果系统的IP地址为200.0.0.200，则可以推算出这个网络是

A．A级网　　B．B级网

C．C级网　　D．D级网

4．加密和解密用同一把密钥的密码体制是

A．单钥密码体制　　B．双钥密码体制

C．多钥密码体制　　D．混钥密码体制

5．DES算法输出密文数据为

A．56位　　B．64位

C．128位　　D．1024位

6．2000年9月，美国国家标准技术局用AES加密标准替代了

A．RC-5　　B．DES

C．IDEA　　D．RSA

7．Diffie-Hellman协议实现密钥交换适用于

A．对称密钥交换　　B．公钥密钥交换

C．RSA密钥交换　　D．凯撒密钥交换

8．安全散列算法的简称是

A．SHA　　B．HAS

C．HTTPS　　D．SET

9．VPN部署模式有

A．3种　　B．4种

C．5种　　D．6种

10．强制式接入控制简称为

A．DAC　　B．EAC

C．MAC　　D．PAC

11．古代调兵用的虎符相当于计算机认证系统中

A．通行字　　B．安全阀

C．账号　　D．护身符

12．身份认证中个人特征不包括

A．指纹　　B．笔迹

C．身份证　　D．脸型

13．通行字的来源不包括

A．用户个人设定　　B．系统自动产生

C．管理员选定　　D．加密产生

14．Kerberos系统是

A．认证服务系统　　B．加密服务系统

C．票据服务系统　　D．签名服务系统

15．证书吊销表简称为

A．CLR　　B．CRL

C．RLC　　D．LRC

16．PKI含义为

A．公钥加密服务　　B．公钥基础设施

C．公钥签名服务　　D．公钥管理服务

17．PKI 构成的体系结构是

A．环形结构　　B．总线型结构

C．树形结构　　D．柱状结构

18．SSL 协议不能保证浏览器到服务器之间的

A．机密性　　B．认证性

C．完整性　　D．接入控制性

19．SET 协议中文简称

A．安全数据交换协议　　B．安全电子服务协议

C．安全套接层协议　　D．安全信用卡协议

20．CFCA 证书采用高强度双向认证，其采用的 RSA 密钥长度达到

A．256 比特　　B．512 比特

C．1024 比特　　D．2048 比特

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．美国橘黄皮书中为计算机安全制定不同等级标准，它们分别为

A．A 级　　B．B 级

C．C 级　　D．D 级

E．E 级

22．病毒具有的特征包括

A．隐蔽性　　B．传染性

C．潜伏性　　D．可触发性

E．表现性

23．提供数据完整性的预防措施主要有

A．镜像技术　　B．奇偶校验

C．电源保障　　D．隔离不安全人员

E．故障前兆分析

24．防火墙按照控制技术可以分为

A．包过滤型　　B．包检验型

C．VPN 型　　D．DNS 型

E．UPD 型

25．VPN 具有的功能包括

A．数据加密　　B．访问控制

C．信息认证　　D．密钥分配

E．身份认证

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．SMTP 协议中文含义是_____，它支持计算机之间传送_____位 ASCII 字符。

27．MD-5 每一轮运算要进行_____步迭代运算，其压缩后输出数据长度为_____比特。

28．计算机病毒按照破坏性可分为_____和_____。

29．IPSec 有_____和_____两种工作模式。

30．身份证实是对个人身份进行_____或_____。

四、名词解释题：本大题共 5 小题，每小题 3 分，共 15 分。

31．商务数据的机密性

32．数据备份

33．防火墙

34．IPSec

35．数字认证

五、简答题：本大题共 6 小题，每小题 5 分，共 30 分。

36．电子商务安全需求涉及哪几个方面？

37．简述 RSA 密码体制公钥和私钥产生过程。

38．散列函数具有什么特性？

39．数据加密起到哪些作用？

40．证书有效必须满足哪些条件？

41．简述认证机构的功能。

六、论述题：本大题共 1 小题，每小题 15 分，共 15 分。

42．论述双联签名签名过程，并说明其验证签名原理。