座位号：

姓名：

机密★启用前

2024年4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．电子邮件的安全问题主要是

A．网上传送时随时可能被人窃取到

B．传输到错误地址

C．传输错误

D．传输丢失

2．美国的橘黄皮书中为计算机安全的不同级别制定了标准，它们从高到低依次是

A．DCBA级　　B．ABCD级

C．CBA级　　D．ABC级

3．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

4．收发双方持有不同密钥的体制是

A．对称密钥　　B．数字签名

C．公钥　　D．完整性

5．现在常用的密钥托管算法是

A．EES　　B．Skipjack

C．Diffie-Hellman　　D．RSA

6．SHA的含义是

A．安全散列算法　　B．密钥

C．数字签名　　D．消息摘要

7．不是散列函数的名字的是

A．压缩函数　　B．数字签名

C．消息摘要　　D．数字指纹

8．《电子计算机房设计规范》的国家标准代码是

A．GB50174-93　　B．GB9361-88

C．GB2887-89　　D．GB50169-92

9．外网指的是

A．受信网络　　B．非受信网络

C．防火墙内的网络　　D．局域网

10．属于IPSec工作模式的是

A．传输模式　　B．安全模式

C．保险模式　　D．恢复模式

11．DAC的含义是

A．自主式接入控制　　B．数据存取控制

C．强制式接入控制　　D．都不对

12．对数据库的加密方法有

A．2种　　B．3种

C．4种　　D．5种

13．系统将通行字表划分成两部分，为了减少暴露的危险性，每部分仅含的通行字有

A．半个　　B．1个

C．2个　　D．4个

14．通行字的最小长度至少为

A．4~12B　　B．6~12B

C．6~8B　　D．4~8B

15．身份认证中的证书发行方是

A．个人　　B．政府机构

C．非营利自发机构　　D．认证授权机构

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. SET 协议确保数据的完整性是通过

A．单密钥加密　　B．双密钥加密

C．密钥分配　　D．数字化签名

18. HTTPS 是 HTTP 使用了

A．SSL　　B．SSH

C．Security　　D．TCP

19. 中国金融认证中心的缩写是

A．CFCA　　B．CTCA

C．SHECA　　D．CPCA

20. 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．服务器证书的操作

C．对他人证书的操作　　D．对根证书的操作

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. 双钥密码体制算法的特点有

A．算法速度慢　　B．只适合加密小数量的信息

C．适合密钥的分配　　D．适合密钥的管理

E．算法速度快

22. 散列值也称为

A．哈希值　　B．杂凑值

C．密钥　　D．消息摘要

E．数字签名

23. Internet 的接入控制主要对付

A．伪装者　　B．病毒

C．违法者　　D．地下用户

E．木马

24. 一个身份证明系统一般组成方有

A．示证者　　B．验证者

C．可信赖者　　D．使用者

E．访问者

25. PKI 技术能够有效地解决电子商务应用中的问题包括

A．机密性　　B．真实性

C．完整性　　D．不可否认性

E．存取控制

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. 客户机和服务器遵循的_____协议是一个“无记忆状态”的协议。

27. 如果他人可以用公钥正确地解开数字签名，则表示数字签名的确是由_____产生的。

28. VPN 利用_____协议在网络之间建立一个虚拟通道。

29. 安全服务器面向普通用户，用于提供_____、浏览、证书吊销表及证书下载等安全服务。

30. 为了保证电子交易过程中无欺骗发生，需要通过网络确认各自的身份以及动态地得到对方的_____，以便把送到对方的信息进行加密。

四、名词解释题：本大题共 5 小题，每小题 3 分，共 15 分。

31. 明文

32. 散列函数

33. 归档

34. 接入控制

35. PKI

五、简答题：本大题共 6 小题，每小题 5 分，共 30 分。

36. 计算机病毒是如何产生的？

37. 简述通行字的选择原则。

38. 如何对密钥进行安全保护？

39. 简述 PKI 的应用范围。

40. SSL 协议中使用了哪些加密技术？

41. 企业、个人如何获得 CFCA 证书？

六、论述题：本大题共 1 小题，每小题 15 分，共 15 分。

42. 论述组建 VPN 应该遵循的设计原则。