座位号：_____

姓名：_____

机密★启用前

2025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．保护数据不被未授权者修改、建立、嵌入、删除、重复传送或由于其他原因使原始数据被更改是

A．数据的机密性　　B．访问的控制性

C．数据的认证性　　D．数据的完整性

2．IDEA加密算法的输入、输出和密钥长度分别为

A．128位, 128位, 128位　　B．64位, 64位, 64位

C．128位, 128位, 64位　　D．64位, 64位, 128位

3．IDEA加密算法首先将明文分为若干位的数据块，然后进行若干轮迭代和一个输出变换，数据块的位数和迭代的轮数分别是

A．64, 8　　B．64, 16

C．128, 8　　D．128, 16

4．消息用散列函数处理后得到的是

A．公钥　　B．私钥

C．消息摘要　　D．数字签字

5．MD-4散列算法，输入消息可为任意长，分组的位数是

A．512位　　B．64位

C．128位　　D．256位

6．《计算机房场、地、站技术要求》的国家标准代码是

A．GB50174-93　　B．GB9361-88

C．GB2887-89　　D．GB50169-92

7．DES的加密运算法则是：每次取明文中的连续64位（二进制位，以下同）数据，利用64位密钥，经过16次循环（每一次循环包括一次替换和一次转换）加密运算，将其变为密文数据的位数是

A．32位　　B．64位

C．128位　　D．256位

8．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

9．不属于防火墙的控制技术的是

A．包过滤型　　B．包检验型

C．应用层网关型　　D．关联规则型

10．接入控制的功能不包括

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．使合法用户按其权限进行各种信息活动

11．接入控制机构的建立主要根据的信息类型有

A．2种　　B．3种

C．4种　　D．5种

12．Kerberos最头疼的问题源自整个Kerberos协议都严重地依赖于

A．服务器　　B．Password

C．时钟　　D．密钥

13．Client向本Kerberos的认证域以外的Server申请服务的过程分为

A．4个阶段，共6个步骤　　B．3个阶段，共6个步骤

C．3个阶段，共8个步骤　　D．4个阶段，其8个步骤

14．将公钥体制用于大规模电子商务安全的基本要素是

A．数字证书　　B．密钥

C．公钥证书　　D．公钥对

15．能够证明在网络上具体的公钥拥有者就是证书上记载的使用者，可以作为鉴别个人身份的证明的是

A．公钥数字证书　　B．公钥对

C．持有者身份信息　　D．私钥对

16．通常 PKI 的最高管理的体现是通过

A．政策审批机构　　B．证书作废系统

C．应用接口　　D．证书中心 CA

17．确保交易各方身份的真实性是通过数字化签名和

A．加密　　B．商家认证

C．数字化验证　　D．SSL

18．安装在客户端的电子钱包一般是一个

A．独立运行的程序　　B．浏览器的插件

C．客户端程序　　D．单独的浏览器

19．CFCA 证书种类包括

A．个人高级证书　　B．代码签名证书

C．个人普通证书　　D．以上都对

20．CTCA 目前提供的安全电子邮件证书，密钥位长为

A．64 位　　B．128 位

C．256 位　　D．512 位

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．电子商务系统可能遭受的攻击有

A．系统穿透　　B．违反授权原则

C．植入　　D．通信监视

E．病毒

22．散列函数也称为

A．哈希函数　　B．杂凑函数

C．哈希值　　D．散列值

E．认证函数

23．证书数据的组成，包括

A．版本信息　　B．证书序列号

C．签名算法　　D．有效使用期限

E．证书主题名称

24．SSL 所提供的安全业务类似于 S-HTTP：除了可通过数字签名提供不可否认性，还有

A．可靠性　　B．实体认证

C．不可抵赖性　　D．保密性

E．完整性

25．下面的服务器和浏览器提供对 SSL 支持的是

A．Netscape Communicator　　B．Microsoft Internet Explorer

C．Microsoft IIS　　D．Lotus Notes Server

E．DOS

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．未授权者非法访问了 Web 上的文件，损害了电子商务中的_____、机密性和完整性。

27．数字签名分确定性数字签名和_____数字签名。

28．接入控制实现有两种方式，分别为自主式接入控制和_____接入控制。

29．身份证明可以依靠“所知”、“所有”以及“_____”这三种基本途径之一或它们的组合实现。

30．在电子商务环境下，_____是实现公钥认证和分配的有效工具。

四、名词解释题：本大题共 5 小题，每小题 3 分，共 15 分。

31．EDI

32．数字签名

33．奇偶校验

34．DMZ

35．电子钱包

五、简答题：本大题共 6 小题，每小题 5 分，共 30 分。

36．简述归档与备份的区别。

37．简述隧道的基本组成。

38．为什么 DAC 易受到攻击？

39．公钥证书有哪些类型？

40．仲裁包括的活动有哪些？

41．SET 安全协议要达到的目标有哪五个？

六、论述题：本大题共 1 小题，每小题 15 分，共 15 分。

42．请说明证书机构（CA）的组成及各部分作用。