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。在每小题列出的各选项中只有一项是最符合题目要求的，请将其选出。

1.称为访问控制保护级别的是

A .Cl B . Bl C .C2 D .B2

2 通常 PKI 的最高管理是通过

A .政策管理机构来体现的 B .证书作废系统来体现的

C .应用接口来体现的 D .证书中心 CA 来体现的

3.IDEA 加密算法首先将明文分为

A. l6 位数据块 B .32 位数据块

C .64 位数据块 D .128 位数据块

4. 美国的橘黄皮书中给计算机安全的不同级别制定了标准，由低到高排列正确的是

A .Cl、 Bl 、C2、B2 B .Bl 、B2、 Cl 、C2

C. A 、B2、C2、D D .Cl 、C2、 Bl 、B2

5. 《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 .GB50174-93 B. GB9361-88

C .GB2887-89 D .GB50169-92

6. 下列提高数据完整性的安全措施中，不属于预防性措施的是

A. 归档 B .镜像 C .RAID D .网络备份

7.SHA 算法输出的啥希值长度为

A .96 比特 B .128 比特 C .160 比特 D . 192 比特

8 .不可否认业务中，用来保护收信人的是

A .源的不可否认性 B .递送的不可否认性

C .提交的不可否认性 D .委托的不可否认性

9.在密钥管理系统中最核心、最重要的部分是

A .工作密钥 B .数据加密密钥

C .密钥加密密钥 D .主密钥

10. 在 Kerberos 中， Client 向本 Kerberos 的认证域以外的 Server 申请服务的过程分为

A .四个阶段 B. 五个阶段 C .六个阶段 D .七个阶段

11.点对点隧道协议 PPTP 是第几层的隧道协议 ？

A .第一层 B. 第二层 C .第三层 D .第四层

12. CA 对已经过了有效期的证书采取的措施是

A .直接删除 B .记入吊销证书表 C .选择性删除 D .不作处理

13. DAC 由资源拥有者分配接入权，在辨别各用户的基础上实现

A .密码控制 B .智能控制 C .数据控制 D .接入控制

14.使用专有软件加密数据库数据的是

A .Access B .Domino C .Exchange D .Oracle

15.在下列安全鉴别闻题中，数字签名技术不能解决的是

A .发送者伪造 B .接收者伪造

C .发送者否认 D .接收者否认

16. SET 安全协议要达到的目标主要有

A .三个 B .四个 C .五个 D .六个

17.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

18.身份认证中的证书的发行单位是

A .个人 B .政府机构

C .非营利自发机构 D .认证授权机构

19.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 .数字化签名 D . SSL

20 .下列选项中，哪一项不属于 SHECA 证书管理器的操作范围 ？

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 l0 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. 使用两个密钥的算法有

A .双密钥加密 B .单密钥加密

C .双重 DES D .三重 DES

E. 双重 RSA

22.在下列计算机病毒中，属于良性病毒的有

A .小球病毒 B. 扬基病毒

C .黑色星期五病毒 D .救护车病毒

E .火炬病毒

23. Kerberos 系统的组成包括

A .用户 Client B .服务器 Server

C .认证中心 CA D .认证服务器 AS

E .票据授权服务器 TGS

24.组成电子商务的技术要素主要有

A .网络 B .应用软件

C .硬件 D .商品

E .仓库

25.接入控制的实现方法有

A .DAC B .DCA

C .MAC D .CAM

E .GE 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.美国的橘黄皮书中为计算机安全的不圈级别制定了 _____个标准，其中 C2 级又称 _____.

27.Kerberos 服务任务被分配到鼕个相对独立的服务器：_____服务器和_____服务器，它同时应该连接并维护一个中央数据库存放用户口令、标识等重要信息。

28.双钥密码体制又称之为 _____或_____.

29.目前有三种基本的网络备份系统：简单的网络备份系统， _____和_____。

30.密钥对生成的两种途径是： _____和 _____。

四、名词解释题：本大题共 5 小题，每小题 3 分。共 15 分。

31.电子商务

32.良性病毒

33. 解密

34. 数字签名

35.网上银行业务

五、简答题：本大题共 6 小题，每小题 5 分，共 30 分。

36. 设置防火墙的目的及主要作用是什么 ？

37. Web 客户机的任务是什么 ？

38.数字签名和手书签名有什么不同 ？

39.说出你知道的 PKI 的应用范围。

40. SET 安全协议要达到的目标有哪五个 ？

41. SHECA 证书的特点和类型是什么 ？

六、论述题：本大题共 I 小题。 15 分。

42.试述组建 VPN 应该遵循的设计原则。