2008年10月自考试题电子商务安全导论全国

课程代码：00997

一、单项选择题(本大题共20小题，每小题1分，共20分)

在每小题列出的四个备选项中只有一个是符合题目要求的，请将其代码填写在题后的括号内。错选、多选或未选均无分。

1.电子商务的技术要素组成中不包含(　B　　)1-3

A.网络　B.用户

C.应用软件　D.硬件

2.电子商务的发展分成很多阶段，其第一阶段是(　A　　)1-6

A.网络基础设施大量兴建　B.应用软件与服务兴起

C.网址与内容管理的建设发展　D.网上零售业的发展

3.下列选项中属于双密钥体制算法特点的是(　C　　)2-47

A.算法速度快　　B.适合大量数据的加密

C.适合密钥的分配与管理　D.算法的效率高

4.美国政府在1993年公布的EES技术所属的密钥管理技术是(　D　　)2-51

A.密钥设置　B.密钥的分配

C.密钥的分存　　D.密钥的托管

5.实现数据完整性的主要手段的是(　D　　)3-53

A.对称加密算法　B.非对称加密算法

C.混合加密算法　D.散列算法

6.数字签名技术不能解决的安全问题是(C　　)3-67

A.第三方冒充　　B.接收方篡改

C.传输安全　D.接收方伪造

7.根据《建筑与建筑群综合布线系统工程设计规范》(CECS　72：97)的要求，计算机机房室温应该保持的温度范围为(　B　　)4-71

A.0℃—25℃ B.10℃—25℃

C.0℃—35℃ D.10℃—35℃

8.判断一段程序代码是否为计算机病毒，其依据是看这段代码是否具有(　B　)4-75

A.隐蔽性　　B.传染性

C.破坏性　　D.可触发性

9.下列隧道协议中，基于防火墙的 VPN 系统的协议是(　A　)5-84

A.IPSec　B.L2F

C.PPTP　D.GRE

10.在中国，制约 VPN 发展、普及的客观因素是(　D　)5-90

A.客户自身的应用　　B.网络规模

C.客户担心传输安全　D.网络带宽

11.由资源拥有者分配接人权的接入控制方式是(　A　)6-94

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.在加密／解密卡的基础上开发的数据库加密应用设计平台是(　C　)6-97

A.使用加密软件加密数据　B.使用专用软件加密数据

C.使用加密桥技术　　D.使用 Domino 加密技术

13.以下关于通行字的选取原则错误的是(B　)7-101

A.易记　B.易理解

C.难以被猜中　　D.抗分析能力强

14.Kerberos 系统的四个组成部分中不包含(A　)7-104

A.BS　　B.TGS

C.Client　D.Server

15.在单公钥证书系统中，签发根 CA 证书的机构是(　C　)8-110

A.国家主管部门　B.用户

C.根 CA 自己　　D.其它 CA

16.CA 系统一般由多个部分构成，其核心部分为(　B　)8-124

A.安全服务器　　B.CA 服务器

C.注册机构 RA　D.LDAP 服务器

17.推出 SET 的两个组织是(　A　)10-141

A.Visa 和 Mastercard　B.Visa 和 Microsoft

C.Mastercard 和 Microsoft　D.Visa 和 RSA

18.SSL 握手协议包含四个主要步骤，其中第三个步骤为(　D　　)10-140

A.客户机 Hello　B.服务器 Hello

C.HTTP 数据流　D.加密解密数据

19.CTCA 安全认证系统所属的机构是(　D　　)11-162

A.中国银行　B.招商银行

C.中国移动　D.中国电信

20.SHECA 证书包含许多具体内容，下列选项中不包含在其中的是(　C　　)11-168

A.版本号　　B.公钥信息

C.私钥信息　D.签名算法

二、多项选择题(本大题共 5 小题，每小题 2 分，共 10 分)

在每小题列出的五个备选项中至少有两个是符合题目要求的，请将其代码填写在题后的括号内。错选、多选、少选或未选均无分。

21.下列属于单密钥体制算法的有(　　ACE　　)2-26

A.DES　B.RSA

C.AES　D.SHA

E.IDEA

22.下列属于接入控制策略的有(　　ABC　　)6-94

A.最小权益策略　B.最小泄露策略

C.多级安全策略　D.强制安全策略

E.最少用户策略

23.下列公钥—私钥对的生成途径合理的有(　CD　　)8-113

A.网络管理员生成

B.CA 生成

C.用户依赖的、可信的中心机构生成

D.密钥对的持有者生成

E.网络管理员与用户共同生成

24.属于数据通信的不可否认性业务的有(　　BCDE　　)9-134

A.签名的不可否认性　B.递送的不可否认性

C.提交的不可否认性　D.传递的不可否认性

E.源的不可否认性

25.SET 要达到的主要目标有(　　ACDE　　)10-141

A.信息的安全传输　　B.证书的安全发放

C.信息的相互隔离　　D.交易的实时性

E.多方认证的解决

三、填空题(本大题共 5 小题，每小题 2 分，共 10 分)

请在每小题的空格中填上正确答案，错填、不填均无分。

26.美国橘黄皮书中为计算机安全的不同级别制定了 4 个共__D, C, B, A_____级标准，其中___D_____级为最低级别。1-19

27.数字签名分为两种，其中 RSA 和 Rabin 签名属于__确定性数字_____签名，ELGamal 签名属于___随机化式数字_____签名。3-66

28.IPSec 是一系列保护 IP 通信的规则的集合，它包含___传输模式____与__隧道模式_____两种工作模式。5-85

29.证书申请包括了用户证书的申请与商家证书的申请，其申请方式包括_网上申请_____和__亲自到认证机构当面申请_____。8-125

30.中国金融认证中心的英文简写为___CFCA_____，它是由__中国人民银行_____牵头，联合多家商业银行共同建立的国家级权威金融认证机构。11-153

四、名词解释题（本大题共 5 小题，每小题 3 分，共 15 分）

31. 容错技术 4-72

答：容错技术的目的是当系统发生某些错误或故障时，在不排除错误和故障的条件下使系统能够继续正常工作或者进入应急工作状态。

32. 奇偶校验 4-74

答：奇偶校验是服务器的一个特性，它提供一种机器机制来保证对内存错误的检测，因此，不会引起由于服务器出错而造成数据完整性的丧失。

33. 身份识别 7-100

答：输入个人信息，经处理提取成模板信息，试着在存储数据库中搜索找出一个与之匹配的模板，而后给出结论。

34. 域间认证 7-106

答：Client 向本 Kerberos 的认证域以外的 Server 申靖服务的过程。

35. 认证服务 9-130

答：认证服务即身份识别与鉴别，就是确认实体即为自己所声明的实体，鉴别身份的真伪。

五、简答题（本大题共 6 小题，每小题 5 分，共 30 分）

36. 简述电子商务系统可能遭受攻击的类型。1-10

答：一般说来，电子商务系统可能遭受的攻击有以下几种：

（1）系统穿透：未经授权人通过一定手段假冒合法用户接人系统，对文件进行篡改、窃取机密信息、非法使用资源等。

（2）违反授权原则：一个被授权进入系统做某件事的用户，在系统中做未经授权的其他事情。

（3）植入：在系统穿透或违反授权攻击成功后，入侵者常要在系统中植入一种能力，为其以后攻击系统提供方便条件。

（4）通信监视：这是一种在通信过程中从信道进行搭线窃听(Interception)的方式。

（5）通信窜扰：攻击者对通信数据或通信过程进行干预，对完整性进行攻击，篡改系统中数据的内容，修正消息次序、时间（延时和重放），注入伪造消息。

（6）中断：对可用性进行攻击，破坏系统中的硬件、硬盘、线路、文件系统等，使系统不能正常工作，破坏信息和网络资源。

（7）拒绝服务：指合法接人信息、业务或其他资源受阻。

（8）否认：一个实体进行某种通信或交易活动，稍后否认曾进行过这一活动，不管这种行为是有意的还是无意的，一旦出现再要解决双方的争执就不太容易了。

（9）病毒：由于 Intemet 的开放性，病毒在网络上的传播比以前快了许多，而且 Intemet 的出现又促进了病毒制造者间的交流，使新病毒层出不穷，杀伤力也大有提高。

37. 简述使用 Diffie—Hellman 密钥交换协议交换密钥的步骤。2-50

答：该协议建议用模一个素数的指数运算来进行直接密钥交换。

（1）设 p 为一素数，口是模 p 的本原元。用户 A 产生一个随机数戈，并计算 U =ax modp 送给用户 B。

（2）同样用户 B 产生一个随机数 y，计算　　y= ay mod D 送给用户 A。这样双方都能计算出相同的密钥

K= axy mod p=Vx mod p=Uy mod p

这种 Diffie-Hellman 密钥交换协议的安全性是基于求离散对数的困难性上的。

（3）若有有效的方法求离散对数，那么攻击者就可以求出石和，，，从而求出 K。由于攻击者不知道算和 y，因而他只能用 U 和 y 来求 K。

38. 简述使用 MD5 算法的基本过程。3-55

答：（1）附加填充比特：在消息的后面加上一个比特的 1 和适当数量比特的 0，使填充后

的消息长度比 512 的整数倍少 64。

（2）附加长度：将原消息长度的 64 比特表示附加到填充后的消息后面。这时，消息的总长度是 512 的倍数，能被 16 整除。

（3）初始化缓冲区：一个用于消息摘要的 128 比特缓冲区。这个缓冲区可以由 4 个 32 比特的寄存器 A、B、C、D 表示。初始值为：

A：01 23 45 67

B: 89 ab cd ef

C：fe dc ba 98

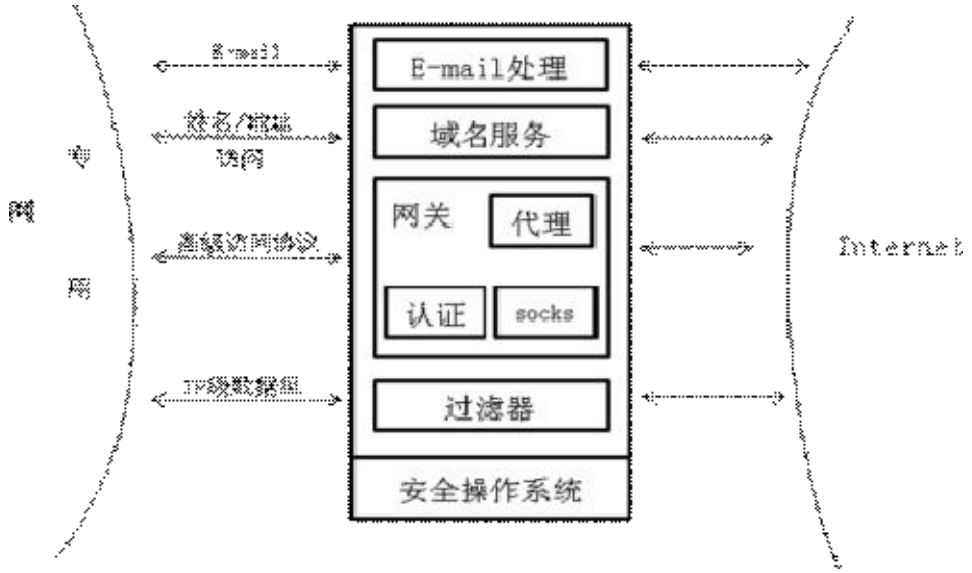
D：76 54 32 10

（4）按每块 16 个字（512 字节）对数据进行 4 轮规定算法处理。

（5）输出：由 A、B、C、D 四个寄存器按低位字节在前的格式排列得到 128 位的输出。

39. 简述防火墙的基本组成部分。5-81

答：防火墙主要包括安全操作系统、过滤器、网关、域名服务和 E - mail 处理。



40. 简述公钥证书包含的具体内容。8-112

答：公钥证书由以下两部分组成：

一、证书数据的组成

1、版本信息 Version：用来区分 X．509 证书格式的版本；

2、证书序列号 Serial　number：每一个由 CA 发行的证书必须有一个惟一的序列号，用于识别证书；

3、CA 所使用的签名算法 Algorithm Identifier: CA 的双钥加密体制算法；

4、发证者的识别码 Issuer Unique　Identifier：发此证书的 CA 识别码；

5、有效使用期限 Period of Validity：本证书的有效起始日期和结束日期；

6、证书主题名称；

7、公钥信息 Public key Information：此双钥加密体制的算法名称、公钥的位字符串表示（只适用于 RSA 加密体制）；

8、使用者 Subject：此公钥的所有者；

9、使用者识别码 Subject Unique Identifier:

10、额外的特别扩展信息。

二、发行证书的 CA 签名与签名算法

证书第二部分包括发行证书的 CA 签名和用来生成数字签名的签名算法。任何人收到证书后都能使用签名算法来验证证书是否是由 CA 的签名密钥签署的。

41. 简述电子钱包的功能。10-146

答：归纳电子钱包的功能有三类：

（1）电子证书的管理（电子证书的申请、存储及删除等）；

（2）进行交易（SET 交易时辨认商家身份并发送交易信息）；

（3）保存交易记录（保存交易记录以供查询）。

六、论述题（本大题 15 分）2-47

42. 试述 RSA 加密算法中密钥的计算方法；并根据该方法计算：（为计算方便）取 p=3，q=5，e=3 时的一组公钥—私钥对；如果明文为 7，计算密文。

答：一、RSA 密码体制描述如下：

1、独立选取两个大素数：p 和 q；

2、计算 n=pq；

3、然后计算小于 n 并且与 n 互质的整数的个数，即欧拉函数 φ(n)=（p-1）(q-l)；

4、随机选择加密密钥 e；要求 e 满足 1≤e≤ φ(n)，并且和 φ(n)互质。

5、最后，利用 Euclid 算法计算解密密钥 d，满足 ed=l（mod φ(n)）

其中 n 和 d 也要互质。数 e 和 n 是公钥，d 是私钥。

二、计算密钥对：

n=3×5＝15

φ(n)=2×4=8

e=3

由 ed=l（mod φ(n)）得 d=3

三、计算密文

当明文为 7 时，密文为（7×7×7）mod15=13