全国 2009 年 1 月自学考试电子商务安全导论试题

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.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(D　　)1-19

A.Cl、Bl、C2、B2　　B.Bl、B2、Cl、C2

C.A、B2、C2、D　　D.C1、C2、B1、B2

2.保证身份的精确性，分辨参与者所声称身份的真伪，防止伪装攻击，这样的业务称为(A　　)1-19

A.认证业务　B.保密业务

C.控制业务　D.完整业务

3.EES 采用的新加密算法是(B　　)2-51

A.RSA　B.Skipjack

C.DES　D.Diffie—Hellman

4.IDEA 加密算法首先将明文分为(C　　)2-26

A.16 位数据块　　B.32 位数据块

C.64 位数据块　　D.128 位数据块

5.在签名人合作下才能验证的签名为(A　　)3-67

A.无可争辩签名　B.双联签名

C.盲签名　　D.RSA 签名

6.消息用散列函数处理得到(B　　)3-53

A.公钥　B.消息摘要

C.私钥　D.数字签名

7.在计算机机房设计中，设备间应采用 UPS 不间断电源，UPS 功率大小应根据网络设备功率进行计算，并应具有的余量是(D　　)4-72

A.5%～10% B.10%～20%

C.15%～20%　　D.20%～30%

8.按 VPN 的服务分类，不属于业务类型的是(　A　)5-87

A.Storage VPN　B.Intranet VPN

C.Access VPN　D.Extranet VPN

9.下列不是防火墙控制技术的是(　C　)5-81

A.包过滤型　B.包检验型

C.VPN　D.应用层网关型

10.为数据库加密字段的存储、检索、索引、运算、删除、修改等功能的实现提供接口的技术是(　D　)6-97

A.数字签名　B.消息摘要

C.双密钥机制　　D.加密桥技术

11.下列不属于 Internet 的接入控制技术主要对付的入侵者是(　B　)6-93

A.伪装者　　B.病毒

C.违法者　　D.地下用户

12.下列不属于 Kerberos 存在的局限性的是(C　　)7-108

A.时间同步　B.重放攻击

C.密钥的分配　　D.口令猜测攻击

13.下列属于证书申请方式的是(　A　)8-125

A.E—mail 申请　B.电话申请

C.邮寄申请　D.短信申请

14.将公钥体制用于大规模电子商务安全的基本要素是(　D　)8-109

A.公钥对　　B.密钥

C.数字证书　D.公钥证书

15.通常 PKI 的最高管理是通过(　A　)9-129

A.政策管理机构来体现　　B.证书作废系统来体现

C.应用接口来体现　　D.证书中心 CA 来体现

16.SSL 协议主要用于交流购买信息，传送(　C　)10-152

A.电子现金　B.电子信用卡

C.电子商贸信息　D.客户信息

17.为了确保数据的完整性，SET 协议是通过(　　D　)10-145

A.单密钥加密来实现　B.双密钥加密来实现

C.密钥分配来实现　　D.数字化签名来实现

l8.下列不是 SHECA 证书管理器管理的证书是(　B　　)11-169

A.个人证书　B.服务器证书

C.他人证书　D.根证书

19.CFCA 是由(　B　　)11-153

A.招商银行牵头　B.中国人民银行牵头

C.中国移动牵头　D.中国电信牵头

20.Kerberos 的域内认证过程共分 3 个阶段，共 6 个步骤。在第 1 个阶段的第 1 个步骤，客户向 AS 发送的信息不包含(　C　)7-104

A.IDClient　B.IDTGS

C.IDServer　D.时间戳 a

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.计算机病毒的主要来源有(　ABCDE　　)4-76

A.非法拷贝引起的病毒　　B.通过互联网络传入的病毒

C.有人研制和改造的病毒　D.一些游戏软件染有的病毒

E.引进的计算机系统和软件中带有的病毒

22.接入控制的实现方法有(　　AC　　)6-94

A.DAC　B.DCA

C.MAC　D.MCA

E.CMA

23.Kerberos 的认证中心服务任务被分配到几个相对的服务器，这些服务器包括（　DE　　）7-104

A.ASS　B.Client

C. ServerD.TGS

E.AS

24.PKI 技术能够有效地解决电子商务应用中信息的(ABCDE　　)9-127

A.机密性　　B.真实性

C.完整性　　D.不可否认性

E.存取控制

25.SET 的技术范围包括(　ACD　　)10-142

A.认可信息和对象格式　　B.银行信息和对象格式

C.购买信息和对象格式　　D.证书信息和对象格式

E.控制信息和对象格式

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.在服务器面临的攻击威胁中，攻击者通过控制一台连接于入侵目标网的计算机，然后从网上断开，让网络服务器误以为___黑客____就是实际的客户端，这种威胁称为__ TCP 协议劫持入侵_____。1-15

27.根据近代密码学的观点，一个密码系统的安全性取决于对__密钥_____的保护，而不取决于对_

算法____的保密。2-49

28.在网络连接技术中，从表面上看它类似于一种专用连接，但实际上是在共享网络上实现的，这种连接技术称为__VPN_____，它往往使用一种被称作__隧道_____的技术。5-84

29.一个典型的 CA 系统包括安全服务器、注册机构 RA、_CA 服务器_____、__LDAP 目录服务器_____和数据库服务器等。8-124

30.SSL 就是客户和商家在通信之前，在 Internet 上建立一个“秘密传输信息的信道”，保障了传输信息的___机密性____、完整性和__认证性_____。10-138

四、名词解释题（本大题共 5 小题，每小题 3 分，共 15 分）

31. 主动攻击 1-13

答：

主动攻击是攻击者直接介入 Intemet 中的信息流动，攻击后，被攻击的通信双方可以发现攻击的存在。

32. 恶性病毒 4-76

答：

恶性病毒是指那些一旦发作后，就会破坏系统或数据，造成计算机系统瘫痪的一类计算机病毒。

33. 漏报率 7-100

答：

漏报率是指非法用户伪造身份成功的概率。

34. CA 证书 8-112

答：

CA 证书是证实 CA 身份和 CA 的签名密钥的证书。

35. 公证服务 9-131

答：

PKI 中支持的公证服务是指“数据认证”，也就是说，公证人要证明的是数据的有效性和正确性，这种公证取决于数据验证的方式。

五、简答题（本大题共 6 小题，每小题 5 分，共 30 分）

36. 简述电子商务发展的四个阶段。1-6

答：

（1）1995 年：网络基础设施大量兴建；

（2）1996 年：应用软件及服务成为热点；

（3）1997 年：网址及内容管理的建设发展，有关企业、业务的调整、重组及融合，所谓“人口门户”(Ponal)公司的出现；

（4） 1998 年：网上零售业及其他交易蓬勃发展。出现一批代做各种电子商务业务的所谓“主待”公司(Hosting)，或日“代庖”公司。

37. 简述 DES 加密算法的加密运算法则。2-26

答：

DES 的加密运算法则是，每次取明文中的连续 64 位（二进制位，以下同样）数据，利用 64 位密钥（其中 8 位是校验位，56 位是有效密钥信息），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 64 位的密文数据。

38. 数字签名可以解决哪些安全鉴别问题？3-67

答：

数字签名可以解决下述安全鉴别问题：

（1）接收方伪造：接收方伪造一份文件，并声称这是发送方发送的；

（2）发送者或接收者否认：发送者或接收者事后不承认自己曾经发送或接收过文件；

（3）第三方冒充：网上的第三方用户冒充发送或接收文件；

（4）接收方篡改：接收方对收到的文件进行改动。

39. 设置防火墙的目的及主要作用是什么？5-79

答：

一、设置防火墙目的是为了在内部网与外部网之间设立惟一的通道，允许网络管理员定义一个中心“扼制点”提供两个网络间的访问控制，使得只有被安全策略明确授权的信息流才被允许通过，对两个方向的信息流都能控制。

二、它的主要作用是：

1、防止发生网络安全事件引起的损害，使入侵更难实现，来防止非法用户，比如防止黑客、网络破坏者等进入内部网络。

2、禁止存在安全脆弱性的服务进出网络，并抗击来自各种路线的攻击。

3、Intemet 防火墙能够简化安全管理，网络的安全性在防火墙系统上得到加固，而不是分布在内部网络的所有主机上。

40. 简述有效证书应满足的条件。8-111

答：

证书要有效，必须满足下列条件：

（1）证书没有超过有效。

（2）密钥没有被修改。如果密钥被修改后，原证书就应当收回，不再使用。如果雇员离开了其公司，对应的证书就可收回，如果不收回，且密钥没被修改，则可继续使用该证书。

（3）证书不在 CA 发行的无效证书清单中。CA 负责回收证书，并发行元效证书清单。用户一旦发现密钥泄露就应及时将证书吊销。并由 CA 通知停用并存档备案。

41. 简述实现递送的不可否认性机制的方法。9-136

答：

可有下述一些方式实现递送的不可否认性：

（1）收信人签字认可。收方接收到消息后，由他（或其代理）向发方提供一个签字的收据，其中包括收到消息的杂凑值、收信时戳和身份等信息。可以由可信赖第三方提供一个证书来强化此类不可否认性。

（2）收信人利用持证认可。

（3）可信赖递送代理。可信赖第三方充当递送代理，发方将消息交给递送代理，递送代理每收到一个消息就转送给收方。收方签一个收据给递送代理，递送代理再签一个认可收据给发方。

（4）逐级递送报告。在现实的网络通信环境中，发方给收方的消息要经过多次传递才能送给收方。为了实现不可否认性，需要逐级建立不可否认业务。

六、论述题（本大题共 1 小题，共 15 分）

42. 试述混合加密系统的实施过程。3-69

答：

在一次信息传送过程中，可以综合利用消息加密、数字信封、散列函数和数字签名实现安全性、完整性、可鉴别和不可否认。具体过程如下：

一、发送方 A

1、求明文消息的消息散列值：hA =H’(M)；

2、发送方用自己的私钥 KSA 对散列值进行数字签名：h’=EKSA(hA)；

3、将明文 M 和数字签名 h’合并为 M’，M’=【Mh’】；

4、随机产生一个 DES 密钥 KDES；

5、用 DES 密钥 KDES 加密 M’，Ci =EKDES (M’)；

6、用接受方 B 的公钥加密 DES 密钥，C2 =EKPB (KDFS)。

A 将 C．和 C2 发送给接受方 B。

二、接受方 B

接受方 B 收到消息后：

1、B 用其私钥打开数字信封，得到发送方的 DES 密钥，KDES=DkSB(C2)；

2、再用此密钥去解密消息 C，，M’=DKDES(Cl)；

3、从 M’中分离出 M 和 h’；

4、求明文消息的消息散列值，hB =H (M)；

5、对 A 的数字签名 h’进行身份验证，hA =DKPA (h’)；

6、比较 hA 和 hB，如 h。=hB，则说明 M 确是 A 发送的消息，如 hA≠hB，则收到的 M 是不可信的。这就是数据完整性检验。