电子科技大学

2010 年攻读信息安全工学硕士学位研究生入学试题

考试科目：825 密码学基础与网络安全

注：所有的答案必须填写在答题纸上，写在试卷或草稿纸上均无效。

一、单项选择题（每题 1 分，共 30 题， 30 分）

请在 A、B、C 和 D 四个选项中，选择一个最佳答案填写到答题纸上。

1. 序列密码属于（ ）

A. 非对称密码体制　　B. 对称密码体制

C. 双钥密码体制　　D. 公钥密码体制

2. Kerberos 认证服务的安全性依赖于（ ）

A. 对称密钥加密体制　　B. 公钥加密体制

C. 数字签名　　D. Hash 函数

3. 数字证书是将用户信息和（ ）绑定在一起的数据文件。

A. 用户私钥　　B. 用户公钥

C. CA 私钥　　D. CA 公钥。

4. 两个密钥 3 重 DES 加密：$C = E_{K_1}[D_{K_2}[E_{K_1}[P]]]$，$K_1 \neq K_2$，其有效的密钥长度为（ ）

A. 56　　B. 112

C. 168　　D. 128

5. n 级 m 序列的周期为（ ）

A. m　　B. n

C. 2^{n-1}　　D. 2^{m-1}

6. 下列关于 Hash 函数 SHA-1 的说法正确的是（ ）

A. SHA-1 的输入长度是任意长的　　B. SHA-1 的分组长度是 512 比特

C. SHA-1 的输出长度是 128 比特　　D. SHA-1 函数中每一轮由 16 步迭代组成

7. 下列不属于数字签名应满足的基本要求是（ ）

A. 从签名可恢复消息　　B. 能与所签消息绑定

C. 签名者不能否认自己的签名　　D. 签名不可伪造

8. 在 Hash 函数中，已知 x，找到 $y(y\neq x)$满足 $h(y)=h(x)$在计算上是不可行的，这一性质称为（　　）

A. 抗强碰撞性　　B. 抗弱碰撞性

C. 单向性　　D. 杂凑性

9. 下列算法能提供不可否认性的是（　　）

A．AES　　B．DSA

C．MD5　　D．DES

10. 假定用户 A 和 B 使用 Diffie-Hellman 密钥交换协议商定一个共同的密钥 K，假定他们所使用的素数模为 p=11，Z_p 的生成元为 g=2。如果用户 A 的秘密随机选择的信息是 6,用户 B 的秘密随机选择的信息是 2，试问 K 是（　　）

A．12　　B. 8

C．6　　D. 4

11. 以下关于序列密码的说法正确的是（　　）

A. 序列密码输出的密钥流是周期序列

B. 序列密码是非对称密钥密码算法

C. 序列密码可提供认证

D. 序列密码加密算法中，明文的不同会影响密钥流的输出

12. 假如 Alice 的 RSA 公钥为 n=323，e=5，Alice 不小心泄露了私钥 d=173。Alice 将 e 换成 7，下列哪一个整数可作为相应的私钥 d（　　）

A. 41　　B. 173

C. 247　　D. 117

13. 公钥密码体制的概念是在解决单钥密码体制中最难解决的两个问题时提出的，这两个问题是密钥分配和（　　）

A．杂凑算法　　B．加密速度

C．数字签名　　D．安全性

14. MD5 杂凑函数的输出是（　　）

A．128 比特　　B．256 比特

C．160 比特　　D．512 比特

15. 下列关于 ElGamal 公钥加密算法正确的是（　　）

A．ElGamal 公钥加密算法的安全性是基于大数分解困难问题

B．ElGamal 公钥加密算法中明文和密文长度相同

C．ElGamal 公钥加密算法中的随机数 k 可以重复使用

D．ElGamal 公钥加密算法中的随机数解密时不再使用

16. 计算机病毒根据传染方式可分为引导型病毒、文件型病毒和（　　）

A．混合型病毒　　B．源码型病毒

C．入侵型病毒　　D．外壳型病毒

17. 下列属于被动攻击的手段是（　　）

A．删除信息　　B．修改信息

C．窃听　　D．伪造信息

18. 通过监视与分析主机的审计记录检测入侵，这样的入侵检测系统称为（　　）

A．分布式入侵检测系统　　B．基于网络的入侵检测系统

C．基于主机的入侵检测系统　　D．脱机检测系统

19. （　　）能有效控制内部网络和外部网络之间的访问及数据传输，从而到达保护内部网络的信息不受外部非授权用户的访问和对不良信息的过滤。

A．入侵检测　　B．反病毒软件

C．防火墙　　D．计算机取证

20. 在 PKI 中，不属于 CA 的任务是（　　）

A、证书的颁发　　B、证书的审批　　C、证书的备份　　D、证书的加密

21. 以下关于 TCP/IP 协议族的说法正确的是（　　）

A. TCP/IP 协议的开放性是其不安全的根本原因

B. TCP/IP 协议族中的 TCP 协议在设计之初考虑到了安全问题

C. TCP 协议的三次握手机制是为解决 TCP 协议的安全问题而提出的

D. TCP/IP 协议的上不能实现消息认证和数据加密等安全机制，需要新的协议，例如 IPv6

22. 以下关于网络互连设备的说法不正确的是（　　）

A. 集线器（Hub）可以作为网络隔离设备　　B. 路由器可以作为网络隔离设备

C. 交换机可以作为网络隔离设备　　D. 防火墙可以作为网络隔离设备

23. 以下关于包过滤（也叫分组过滤）防火墙的说法不正确的是（　　）

A. 数据包中的源 IP 地址可以作为包过滤防火墙的过滤条件

B. 数据包中的目的 IP 地址可以作为包过滤防火墙的过滤条件

C. 数据包中的传输层协议类型字段可以作为包过滤防火墙的过滤条件

D. 应用层协议中的内容可以作为包过滤防火墙的过滤条件

24. P^2DR 模型是一个动态的计算机系统安全理论模型，它的特点是（　　）

A. 不需要技术人员干预的模型　　B. 是主动防御安全理论模型

C. 具有动态性和基于时间的特性　　D. 具有自组织、自学习的特性

25. 根据 IDS 系统的数据来源，可以将其分为（　　）等两大类

A. 分布式 IDS 和集中式 IDS　　B. NIDS 和 HIDS

C.　IDS 和 IPS　　D. 异常检测 ADS 和入侵检测 IDS

26. Dorothy Denning（1987）年提出了通用的入侵检测模型，他的三个主要部件是（　　）

A. 事件产生器，活动记录器和规则集　　B. 时钟发生器，活动记录器和规则集

C. 事件产生器，活动记录器和数据库　　D. 事件产生器，监听器和规则集

27. 蠕虫病毒和木马病毒的主要区别在于（　　）

A. 木马程序和蠕虫病毒没有任何区别，都属于计算机病毒

B. 木马是一个完整、独立的程序，而蠕虫病毒只是一部分代码片段

C. 木马程序不具有传染性，而蠕虫病毒具有传染性

D. 木马具有隐蔽性和非授权性，而蠕虫则通过自我复制消耗网络资源

28. 计算机病毒的检测方法不包括（　　）

A. 搜索法　　B. 中断屏蔽法

C. 特征字识别分析法　　D. 比较法

29. 以下关于引用监视器（Reference Monitor）的说法正确的是（　　）

A. 引用监视器自身不一定正确和安全

B. 引用监视器是一种认证机制

C. 引用监视器是一种访问控制

D. 引用监视器必须能够识别系统中的程序，但是不能控制其他程序的运行

30. 自主访问控制模型（DAC Model）是根据自主访问控制策略建立的一种模型，一般采用（　　）方式存放不同主体的访问控制权限，实现对主体访问权限的限制。

A. 用户权限矩阵和中断监控等

B. 访问控制矩阵或访问控制列表

C. 用户密码表和用户权力表

D. 角色控制表和访问权限表

二、填空题（每空 1 分，共 30 空， 30 分）

1. Shannon 在其理论密码学奠基性的论文中，给出了一个好的密码系统抵抗统计分析需要满足的两个性质：_____和_____。

2. DES 算法中，S 盒的输入长度为_____比特，输出长度为_____比特。

3. AES 算法-Rijndael 的分组长度是可变的，可以指定为____位、____位和_____位。

4. 密码学的两个分支是_____和_____。其中前者是对信息进行编码以保护信息的一门学问，后者是研究分析破译密码的学问。

5. 离散对数问题指的是:给定一个素数p,令α,β是模p的非零整数,求解x,使得_____。

6. 网络安全的可信性随网络的扩展而下降，ISO 定义了四种连接方式来度量，它们是不可信结点连在不可信网络上、_____、_____和_____。

7. 两类基本的密钥建立的方法是_____和_____。

8. IPSec 的工作模式分为传送模式和_____。

9. Anderson 将入侵者分为假冒用户、_____和_____。

10. SSL 协议建立在传输层和应用层之间，包括两个主要的子协议：SSL 记录协议和 SSL 握手协议。SSL 记录协议为 SSL 连接提供了两种服务：_____和_____。

11. 恶意代码（软件）包括计算机病毒（如 CIH、爱虫、新欢乐时光、求职信）、_____（如红色代码、SQL 蠕虫王、冲击波、震荡波）、_____（如冰河、灰鸽子）、后门、恶

意网页和逻辑炸弹等。

12. 计算机病毒按照链接方式划分可分为_____、_____、_____和_____。

13. PDRR 安全模型包含_____、_____、_____、_____四部分。

三、简答题（45 分）

1. 根据密码分析者可能取得的分析资料不同，可将密码分析（或攻击）分为哪几类？给出这几类攻击的定义。（5 分）

2. 什么是入侵检测，什么是入侵检测系统？入侵检测系统的分类方法有哪些？（10 分）

3. 防火墙对流入和流出内部网络的数据进行过滤，在内部网络和外部网络之间有一堡垒主机。设配置如下：内部网络地址为 192.168.0.0/24，堡垒主机内网卡 eth1 地址为 192.168.0.1，外网卡 eth0 地址为 10.11.12.13，DNS 地址为 10.11.15.4。分析以下过滤规则是如何保护内部网络的。（10 分）

Set internal=192.168.0.0/24

Deny ip from $ internal to any in via eth0

Deny ip from not $ internal to any in via eth1

Allow udp from $ internal to any dns

Allow udp from any dns to $ internal

Allow tcp from any to any established

Allow tcp from $ internal to any www in via eth1

Allow tcp from $ internal to any ftp in via eth1

Allow tcp from any ftp data to $ internal in via eth0

Deny ip from any to any

4. 在访问控制中，设主体 S_1 的密级为绝密（Top Secret），S_2 的密级为机密（Secret），S_3 的密级为公开（Unclassified），客体 O_1 的密级为绝密，O_2 的密级为机密，O_3 的密级为公

开。

①如果按照不上读/不下写的访问控制方法，S_2 可以对哪些客体进行读和写操作？这样的访问控制方法确保了什么安全属性？（5 分）

②如果按照不下读/不上写的访问控制方法，S_2 可以对哪些客体进行读和写操作？这样的访问控制方法确保了什么安全属性？（5 分）

5. 请画出 OSI 的 7 层模型示意图和 TCP/IP 的 4 层模型示意图，并简要说明其中传输层、网络层和数据链路层的功能。（10 分）

四、计算题（15 分）

1. 求 Hill 加密算法 $C=\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 11 & 9 & 8\end{pmatrix} M \bmod 26$ 的解密函数，其中 C 表示密文，M 表示明文。（5 分）

2. 在 RSA 公钥加密体制中，n 为体制使用的模数，若敌手知道 $\phi(n)$，是否能求出 p，q？请说明理由。（5 分）

3. 给定一个信息位串 K(x)=10111010 和生成多项式 G(x)=11101，请问冗余码应该是几位？计算出冗余码 R(x)。（5 分）

五、 假定房间里有 4 个人，其中一个是国外特务，其余 3 人拥有 Shamir 秘密分享方案的数对，任何两个人都能确定秘密。国外特务随机选择了一个数对，人员和数对如下。所有的数对都是模 11 的。

A:（1，4） B:（3，7） C:（5，1） D:（7，2）

确定哪一个是特务，秘密是什么？（15 分）

六、下表是一台计算机上网访问纽约时报网站时，用 Wireshark 捕获的一个上网过程，共有8个步骤，请解释每一步骤的含义：（15分）

No.	Time	Source	Destination	Protocol	Information
1	0.000	128.100.11.13	128.100.100.128	DNS	Standard query A www.nytimes.com
2	0.129	128.100.100.128	128.100.11.13	DNS	Standard query response A 64.15.347. 200A 64.15.347.245 A 64.94.185.200
3	0.131	128.100.11.13	64.15.347.200	TCP	1127 > 80 [SYN] Seq=3638689752 Ack=0 Win=16384 Len=0
4	0.168	64.15.347.200	128.100.11.13	TCP	80 > 1127 [SYN, Ack] Seq=1396200325 Ack=3638689753 Win=1460 Len=0
5	0.169	128.100.11.13	64.15.347.200	TCP	1127 > 80 [Ack] Seq=3638689753 Ack=1396200326 Win=17316 Len=0
6	0.188	128.100.11.13	64.15.347.200	HTTP	GET / HTTP / 1.1
7	0.205	64.15.347.200	128.100.11.13	TCP	80 > 1127 [Ack] Seq=1396200326 Ack=36386890402 Win=32767 Len=0
8	0.236	64.15.347.200	128.100.11.13	HTTP	HTTP / 1.1 200 OK