电子科技大学

2011 年攻读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：所有答案必须写在答题纸上，做在试卷或草稿纸上无效。

一、单向选择题（每题 1 分，30 题， 共 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. 以下关于 TCP/IP 协议族的说法不正确的是（ ）
   A. TCP/IP 协议在设计之初几乎没有考虑到安全问题
   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不是为解决 TCP 协议的安全问题而提出的
   D. TCP 协议是一个面向连接的协议
2. 关于选择密文攻击说法正确的是（ ）
   A. 攻击者可以获得加密机　　B. 攻击者可以获得解密机
   C. 攻击者不能获得加密机和解密机　　D. 攻击者可以同时获得加密机和解密机
3. 根据欧拉定理，7^{803} 的后两位数字是（ ）
   A. 40　　B. 41
   C. 42　　D. 43
4. 以下关于第二次世界大战中德国所使用的轮转机密码（Enigma）说法正确的是（ ）
   A. Enigma 是非对称加密算法　　B. Enigma 是对称加密算法
   C. Enigma 是流密码算法　　D. Enigma 是经过证明的安全加密算法
5. 下列关于密码学中扩散（Diffusion）说法正确的是（ ）
   A. 扩散的含义是密钥与密文不相关
   B. 扩散的含义是密钥与密文相关
   C. 扩散的含义是改变明文的一个字符，相应密文中的多个字符会发生改变
   D. 扩散的含义是改变密文的一个字符，相应明文中的多个字符不会发生改变
6. 以下关于蜜罐（Honeypot）说法不正确的是（ ）
   A. 蜜罐技术可以用来收集攻击信息　　B. 蜜罐技术可以用来收集计算机病毒代码
   C. 蜜罐技术可以用来诱骗攻击者　　D. 蜜罐技术可以用来阻止网络攻击的发生
7. 无连接完整性可以用哪种安全机制来实现？（ ）
   A. 访问控制　　B. 认证交换
   C. 加密　　D. 业务流填充
8. 整数 79 的欧拉数是（ ）
   A.76　　B. 77
   C. 78　　D. 79
9. 关于 ACK 泛洪攻击（ACK Flooding）说法正确的是（ ）

A. ACK Flooding 利用了 UDP 协议的缺陷　　B. ACK Flooding 利用了 TCP 协议的缺陷
C. ACK Flooding 利用了 IP 协议的缺陷　　D. ACK Flooding 利用了 ICMP 协议的缺陷

10. 关于蠕虫的说法正确的是（　　）
A. 蠕虫需要依附于驻留文件且通过网络传播
B. 蠕虫需要依附于驻留文件来进行复制，但不需要通过网络传播
C. 蠕虫不需要依附于驻留文件，但需要通过网络传播
D. 蠕虫既不需要依附于驻留文件，也不需要通过网络传播播

11. 关于 SYN 泛洪攻击（SYN Flooding）说法不正确的是（　　）
A. SYN Flooding 利用了 TCP 三次握手的缺陷
B. SYN Flooding 消耗了被攻击者的存储资源
C. SYN Flooding 的根源不是消耗了被攻击者的计算资源
D. SYN Flooding 需要借助于 IP 欺骗才能进行

12. 关于入侵检测系统中误用检测（Misuse Detection）说法不正确的是（　　）
A. 误用检测根据掌握的关于入侵的知识来检测入侵行为
B. 误用检测必须建立攻击特征库
C. 误用检测不一定需要建立攻击特征库
D. 误用检测不需要掌握正常行为的知识

13. 下面关于 UDP 协议的说法中，不正确的是（　　）
A. UDP 是传输层的协议　　B. UDP 协议是面向连接的协议
C. UDP 是非面向连接的协议　　D. UDP 数据包中不包含源 IP 地址

14. 以下关于访问控制的说法不正确的有（　　）
A. Windows 操作系统实现了强制访问控制
B. UNIX 操作系统实现了强制访问控制
C. 所有的操作系统必须实现强制访问控制
D. 并非所有的操作系统都需要实现自主访问控制

15. 以下不属于 ISO 7498-2 和 ITU-T X.800 规定的安全服务的有（　　）
A. 认证（Authentication）　　B. 访问控制（Access Control）
C. 加密（Encryption）　　D. 数据机密性（Data Confidentiality）

16. 以下关于链路加密的说法不正确的是（　　）
A. 链路加密是在通信链路两端加上加密设备对数据进行加密
B. 链路加密可以采用硬件实现
C. 链路加密中每个用户可以选择自己的加密密钥
D. 链路加密中所有用户使用相同的加密密钥

17. 以下关于 IPSec 说法正确的是（　　）
A. IPSec 属于网络层的安全解决方案　　B. IPSec 属于传输层的安全解决方案
C. IPSec 属于应用层的安全解决方案　　D. IPSec 属于物理层的安全解决方案

18. 以下关于防火墙说法正确的是（　　）
A、所有防火墙都能够检测网络攻击　　B. 所有的防火墙都能够检测计算机病毒

C. 防火墙主要防御内部攻击　　D. 防火墙主要防御外部攻击

19. 以下关于入侵检测系统（IDS）的说法正确的是（　　）
A. 入侵检测系统可分为主机入侵检测系统和网络入侵检测系统
B. 入侵检测系统只能够检测已知攻击
C. 入侵检测系统不能够提供日志功能
D. 网络入侵检测系统（NIDS）不能够保护一个局域网

20. 以下关于虚拟专网（VPN）说法不正确的是（　　）
A. VPN 可以用专门的 VPN 设备来实现
B. VPN 可以用加密技术来实现
C. VPN 不能在防火墙上实现
D. VPN 可以在防火墙上实现

21. 以下关于安全扫描技术说法不正确的是（　　）
A. 扫描技术可以被攻击者利用
B. 扫描技术可以用 UDP 协议来实现
C. 扫描技术可以用 TCP 协议来实现
D. 扫描技术不能用来进行渗透性测测试

22. 以下关于 Windows NT 系列操作系统的安全组件说法不正确的是（　　）
A. Windows NT 系列操作系统包括 lsasrv.dll 安全组件
B. Windows NT 系列操作系统包括 samsrv.dll 安全组件
C. Windows NT 系列操作系统没有包括 SSL.dll 安全组件
D. Windows NT 系列操作系统没有包括 kerberos.dll 安全组件

23. 一般来说，关于系统安全相关的信息存放在 Windows 注册表的哪个子树？（　　）
A. HKEY_LOCAL_SECURITY
B. HKEY_LOCAL_WINDOWS
C. HKEY_LOCAL_WIN32
D. HKEY_LOCAL_MACHINE

24. 下列关于强制访问控制模型说法正确的是（　　）
A. 在该模型中，主体和客体均被赋予一定的安全级别，主体不能改变自身和客体的安全级别
B. 在该模型中，主体和客体均被赋予一定的安全级别，主体不能改变自身的安全级别，但是可以改变客体的安全级别
C. 在该模型中，主体和客体均被赋予一定的安全级别，主体能改变自身的安全级别，但是不能改变客体的安全级别
D. 在该模型中，主体和客体均被赋予一定的安全级别，主体既能改变自身的安全级别，也能改变客体的安全级别

25. 下列关于网络地址转换（NAT）正确的说法是（　　）
A. NAT 和防火墙能协同工作　　B. NAT 不能和防火墙协同工作
C. NAT 不能扩展 IP 地址空间　　D. NAT 不能用来解决 IP 地址紧张的问题

26. 下列关于数字签名说法正确的是（　　）
A. 数字签名是不可信的　　B. 数字签名容易被伪造
C. 数字签名容易抵赖　　D. 数字签名不可改变

27. 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

28. 以下关于分布式拒绝服务攻击（DDOS）的说法不正确的是（　　）
A. DDOS 一般需要通过分布在不同物理位置的攻击者同时发动攻击
B. DDOS 可能消耗被攻击者的计算资源、存储资源或带宽资源
C. DDOS 可能消耗被攻击者的计算资源和存储资源
D. DDOS 防御系统只能在被攻击者主机上部署

29.《中华人民共和国电子签名法》开始实施的时间是（　　）
A. 2005 年 3 月 1 日　　B. 2005 年 4 月 1 日
C. 2005 年 5 月 1 日　　D. 2005 年 6 月 1 日

30. 目前，得到许多国家认可的信息安全管理标准是（　　）
A. BS7799　　B. BS7498
C. ISO 9000　　D. CC

二、多项选择题（每题 2 分，10 题，　共 20 分）

每题有一个或多个正确答案。请将 A、B、C 和 D 四个选中所有正确答案的选项填写到答题纸上。（注意：多选、少选、错选均不得分）

1. 以下关于跨站点脚本攻击（Cross-Site Scripting Attack）的说法正确的是（　　）
A. 如果 Web 应用不支持用户输入，则跨站点脚本攻击无法实现
B. 如果用户输入不能用来生成动态内容，则跨站点脚本攻击无法实现
C. 如果用户输入不能用来生成静态内容，则跨站点脚本攻击无法实现
D. 如果 Web 应用对用户输入进行足够的有效性检验，则跨站点脚本攻击无法实现

2 以下关于网络钓鱼（Phishing）说法正确的有（　　）
A. 网络钓鱼融合了伪装、欺骗等多种攻击方式
B. 网络钓鱼与 WEB 服务没有关系
C. 典型的网络钓鱼攻击将被攻击者引诱到一个通过精心设计的钓鱼网站上
D. 网络钓鱼是“社会工程攻击”的一种形式

3. 下列哪些方法可以用来防止重放攻击？（　　）
A. 挑战—应答机制　　B. 时戳机制
C. 加密机制　　D. 压缩机制

4. RFC 1321 中以下关于 MD5 的说法正确的有（　　）
A. MD5 是一个加密算法标准
B. 消息填充对于 MD5 是必须的
C. 消息填充对 MD5 是可选的
D. MD5 的输出是 128 位

5. 以下关于分组密码操作模式说法正确的是（　　）
A. 在电子密码本（ECB）中，相同明文将得到相同密文
B. 密码分组连接模式（CBC）中，需要一个初始向量（IV）
C. 密码反馈模式（CFB）中，相同明文可能得到不相同密文
D. 所有分组密码操作模式都满足并行计算的需求

6. IPSec 协议中的 AH 协议能提供的服务有(　　)

A. 访问控制　　B. 无连接完整性

C. 数据源认证　　D.保密性（或秘密性）

7. 以下哪些操作过程是安全套接层协议（SSL）中的记录协议（SSL Record Protocol）可能包括的（　　）

A. 压缩　　B. 添加消息认证码 MAC

C. 加密　　D. 添加 SSL 记录头

8. 下列关于 Kerberos 协议说法正确的有（　　）

A. Kerberos 采用对称加密算法

B. Kerberos 可以实现双向认证

C. Kerberos 无法提供跨域认证功能

D. Kerberos 使用时戳机制抵抗重放攻击

9. 以下关于防火墙中状态检测技术说法正确的是（　　）

A. 状态检测技术可能对应用层数据进行解析

B. 状态检测技术可能对传输层数据进行解析

C. 状态检测技术可能对网络层数据进行解析

D. 与简单的包过滤技术相比，状态检测技术计算开销更大

10. 以下哪些设备可以用来进行网络隔离（　　）

A. 路由器　　B. 交换机

C. 集线器　　D. 防火墙

三、计算选择题（每题 5 分， 3 题，共 15 分）

请在 A、B、C 和 D 四个选项中，选择一个正确答案填写到答题纸上。

1. DES 算法中，已知 DES 算法中的第 1 个 S 盒如下：

S_1 行＼列	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

如果该 S 盒的输入为 101011，则其输出为（　　）

A. 0111　　B. 1000

C. 1001　　D. 1010

2. 居住某地区的女孩子有 25%是大学生，在女大学生中有 75%身高在 160 厘米以上，而女孩子中身高 160 厘米以上的占总数的一半。假如得知“身高 160 厘米以上的某女孩是大学生”的消息，问通过该消息获得多少信息量？（　　）

A. $-\log^{0.375}$　　B. $-\log^{0.275}$

C. $-\log^{0.175}$　　D. $-\log^{0.075}$

3. 已知矩阵 $M=\begin{bmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 11 & 9 & 8\end{bmatrix}(\text{mod } 26)$，则 M 的逆矩阵 M^{-1} 是（　　）

A. $M^{-1}=\begin{bmatrix}23 & 5 & 1\\ 6 & 17 & 24\\ 15 & 13 & 1\end{bmatrix}$　　B. $M^{-1}=\begin{bmatrix}22 & 6 & 1\\ 6 & 17 & 24\\ 15 & 13 & 1\end{bmatrix}$

C. $M^{-1}=\begin{bmatrix}22 & 5 & 2\\ 6 & 17 & 24\\ 15 & 13 & 1\end{bmatrix}$　　D. $M^{-1}=\begin{bmatrix}22 & 5 & 1\\ 6 & 17 & 24\\ 15 & 13 & 1\end{bmatrix}$

四、简答题（共 4 题，30 分）

1. （6 分）请列举防火墙主要技术和主要体系结构。

2. （6 分）什么是物理安全？简述物理安全的主要内容。

3. （8 分）什么是容错技术？冗余技术与容错技术的关系是什么？列举三种常见的冗余技术，并说明其含义。

4. （10 分）简述 X.509 证书（以版本 3 为例）所包含的主要内容。

五、（10 分）一次性口令机制（S/KEY）是一个允许用户 U 与服务器 S 共享一个口令 PWD，但是在每次认证过程中，用户不会重复使用口令 PWD 向服务器 S 证明自己的身份。S/KEY 的基本原理是，用户 U 和服务器 S 之间协商一个整数 n、一个用于认证需要的哈希函数 H，服务器在本地存储一个三元组（U、H^n（PWD），n），其中 H^n（PWD）表示利用哈希函数 H 对口令 PWD 进行 n 次哈希运算。试回答以下问题：

1、请描述 S/KEY 的协议过程。

2、该方案存在安全隐患是什么？请描述针对该安全隐患的攻击。

六、（10 分）缓冲区溢出是很多网络攻击的根源。请结合缓冲区溢出的原理，回答以下问题：

1、C 语言库函数 strcpy 的函数原型是什么？并据此说明 strcpy 存在缓冲区溢出安全隐患的原因。

2、用 C 语言编写一个简单的不存在缓冲区溢出安全隐患的程序，其 main 函数必须调用 function（*str）函数（*str 是 function 的指针参数），而 function 函数的功能是调用 strcpy 将一个字符串赋值给*str。

七、（15 分）DH 协议（Diffie-Hellman Key Agreement Protocol，简称 DH 协议）是密码学中经典的安全协议。结合安全协议的基本原理，回答以下问题：

1、两方的 DH 协是通信双方 A 和 B 可以协商一个共享密钥 k_{ab}，请说明两方 DH 协议存在的一种安全漏洞，并简述其攻击过程。（5 分）

2、请设计一个用于三方（A、B 和 C）的 DH 密钥协商协议，通过该协议，A、B 和 C 可以协商一个密钥 k_{abc}。（10 分）

八、（12 分）为了妥善保管一个电子保险箱的密码 k，管理员使用一个基于 Shamir 阈值方案（Shamir threshold Scheme）的(2，20)门限密码方案将该密码 k 分发给了 20 个密码管理员进

行管理。请回答以下问题：

1、如果所有密码管理员都是诚实的，那么打开保险箱至少需要多少人？说明原因。

2、如果 20 个密码管理员中至少有一个不诚实，不诚实的密码管理员会在密码重构过程中随机出示自己的信息，那么打开保险箱至少需要多少人？说明原因。

3、在有 1 个不诚实密码管理员的上述方案中，如果该保险箱只能试一次（即如果密码出错，该保险箱将被永远关闭），那么打开保险箱至少需要多少人？说明原因。

九、（8 分）证明素数的个数是无限的。