电子科技大学

2014 年攻读硕士学位研究生入学考试试题

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，写在试卷或草稿纸上均无效。

一、单向选择题（每题 1 分，20 题， 共 20 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. 2000 年颁布的《计算机病毒防治管理办法》中对计算机病毒的定义最准确的说法是（　　）
   A. 计算机病毒是恶意代码的一种
   B. 计算机病毒是导致系统功能变坏的恶意代码
   C. 计算机病毒是指可以通过互联网传播的、会导致计算机信息系统遭受破坏的一组计算机指令或程序代码
   D. 计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或程序代码
2. 以下关于公钥体制说法不正确的是（　　）
   A. 在一个公钥体制中，一般存在公钥和私钥两个密钥
   B. 公钥体制中仅根据密码算法和加密密钥来确定解密密钥在计算上是不可行的
   C. 公钥体制中仅根据密码算法和加密密钥来确定解密密钥在计算上是可行的
   D. 公钥体制中的私钥可以用来进行数字签名
3. 以下关于 Kerberos 说法正确的是（　　）
   A. Kerberos 是基于非对称密码算法的安全协议　　B. Kerberos 不能抵抗重放攻击
   C. Kerberos 可以实现双向身份认证　　D. Kerberos 主要用于密钥交换
4. 整数 31 的欧拉函数 $j(31)$ 等于（　　）
   A. 28　　B. 29
   C. 30　　D. 31
5. 下列关于强制访问控制模型说法正确的是（　　）
   A. 主体不能改变自身和客体的安全级别
   B. 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. 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. 主体既能改变自身的安全级别，也能改变客体的安全级别
6. 根据欧拉定理，7^{804} 的后三位数字是（　　）
   A. 400　　B. 401
   C. 402　　D. 403
7. 以下关于 UNIX 文件系统的安全保护机制说法不正确的是（　　）
   A. UNIX 文件系统提供了口令保护机制
   B. UNIX 文件系统提供了访问控制保护机制

C. UNIX 文件系统提供了基于组（group）的安全保护机制

D. UNIX 文件系统提供了基于进程和线程的安全保护机制

8. 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

9. 根据 2013 年 9 月最高人民法院和最高人民检察院关于网络谣言刑案的司法解释，以下说法不正确的是（　　）

A. 捏造损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的行为属于刑法所规定的“捏造事实诽谤他人”。

B. 将信息网络上涉及他人的原始信息内容篡改为损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的行为属于刑法所规定的“捏造事实诽谤他人”。

C. 同一诽谤信息实际被点击、浏览次数达到五千次以上，或者被转发次数达到五百次以上的行为属于刑法所规定的“捏造事实诽谤他人”且属于“严重危害社会秩序和国家利益”。

D. 利用信息网络诽谤他人，且引发公共秩序混乱的，应当认定为刑法规定的“严重危害社会秩序和国家利益”。

10. 以下哪项不属于物理安全威胁？（　　）

A. 自然灾害　　B. 物理攻击

C. 硬件故障　　D. 系统安全管理人员培训不够

11. 以下关于身份认证的说法不正确是（　　）

A. 身份认证是验证者获得对声称者所声称的事实的信任

B. 身份认证有单向和双向认证之分，但一般不能重复两次单向认证来实现双向认证

C. 密码技术和非密码技术都可以用来实现身份认证

D. 只有密码技术才能够用来实现身份认证

12. 关于域（field）的说法正确是（　　）

A. 域必须满足加法的分配率　　B. 域必须满足乘法的分配率

C. 在域中每个元素都有一个加法逆元　　D. 在域中每个元素都有一个乘法逆元

13. 以下关于地址解析协议（ARP）说法不正确的是（　　）

A. 地址解析协议用于 IP 地址和 MAC 地址的解析

B. 地址解析协议包括 ARP 请求和 ARP 应答两种类型的包

C. 由于 ARP 请求是定向传送，所以存在 ARP 欺骗攻击的安全威胁

D. 通过添加静态 ARP 表项到 ARP 地址解析表中可以在一定程度上防止 ARP 欺骗攻击

14. Windows 系统中本地安全管理员（LSA）的任务是 （　　）

A. 调用并监视安全警告序列(SAS，一般是 Ctrl+ALt+Del）

B. 创建用户的本地访问令牌

C. 提供安全服务相关的应用程序接口(API)

D. 管理用户的账户信息（如口令等）

15. Windows 中新技术文件系统（NTFS）的访问控制权限不包括（　　）

A. 读取权限（Read）　　B. 执行权限（Execute）

C. 改变拥有者权限（Change）　D. 拥有者权限（Owner）

16. 以下哪个不属于计算机证据（即电子证据）的范畴（　　）
A. 从计算机硬盘中恢复出来的电子记录
B. 从浏览器缓存中恢复出来的电子记录
C. 从即时通信服务器（如 QQ 服务器中）查找到的电子记录
D. 显示器上显示的信息
17. 以下关于网络扫描说法正确的是（　　）
A. TCP 协议中的 SYN 消息不能用来进行网络扫描
B. IP 协议不能用来进行网络扫描
C. UDP 协议可以用来进行网络扫描
D. FTP 协议不能用来进行网络扫描
18. 已知明文攻击是指（　　）
A. 攻击者拥有密文串　　B. 攻击者拥有明文串 x 和相应的密文串 y
C. 攻击者可获得对加密机的暂时访问　　D. 攻击者可暂时接近解密机
19. 关于电子密码本（ECB）密码操作模式说法正确的是（　　）
A. 对每一个明文数据块采用不同的密钥进行加密
B. 对每一个明文数据块采用不同的密钥进行解密
C. 错误传递仅有一块：出错密文块仅导致对应的明文块错误
D. 错误传递有多块：出错密文块将导致多个明文块错误
20. 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

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. 以下关于高级数据加密标准 AES 说法正确的有（　　）
A. AES 是对称加密算法　　B. AES 是非对称加密算法
C. AES 是分组密码算法　　D. AES 是流密码算法
2. 以下关于安全套接层协议 SSL 说法不正确的有（　　）
A. SSL 协议是解决 IP 协议安全性的一种方案　　B. SSL 协议能提供完整性
C. SSL 协议不能提供机密性保护　　D. SSL 协议不能提供认证功能
3. 选择字段的连接完整性可以由以下哪些安全机制来实现？（　　）
A. 加密　　B. 数字签名
C. 访问控制　　D. 数据完整性
4. IP 协议可能面临以下哪些安全威胁？（　　）
A. IP 地址假冒攻击　　B. 窃听
C. IP 碎片攻击　　D. 序列号猜测
5. 下列关于椭圆曲线加密算法（ECC）的说法中正确的有（　　）
A. ECC 属于数字签名算法　　B. ECC 属于非对称加密算法
C. ECC 不属于非对称加密算法　　D. ECC 算法的安全强度较 RSA 算法强

6. 以下关于美国国防部所提出的 PDRR 网络安全模型说法不正确的（　　）

A. 安全策略（Policy）是 PDRR 的重要内容

B. 依据 PDRRR 模型，增加系统的保护时间可能提高系统的安全性

C. 依据 PDRRR 模型，增加系统的检测时间可能提高系统的安全性

D. 依据 PDRRR 模型，应该尽量增加系统暴露时间来提高系统的安全性

7. 以下哪些技术可以用来对攻击源进行定位？（　　）

A. 日志技术　　B. ICMP 回溯技术

C. 数据包标记技术　　D. 蜜罐技术

8. X.509 数字证书的内容包括（　　）

A. 签名算法标示　　B. 证书的有效期

C. 证书序列号　　D. 主体的公钥

9. 以下关于数据备份说法正确的有（　　）

A. 按照备份后数据是否可以更改，数据备份可分为活备份和死备份

B. 差分备份只备份上次备份以来变化了的数据

C. 差分备份只备份上次全备份以来变化了的数据

D. 差分备份备份所有数据

10. 以下说法正确的有（　　）

A. 非对称加密算法较好地解决了密钥管理问题

B. TCP/IP 协议在设计之初并未考虑网络安全威胁

C. 网络隔离技术可以在一定程度上减少对信息系统的安全威胁

D. 安全协议需要使用某种密码算法且须提供一项或多项安全功能

三、计算选择题（每题 5 分， 共 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. 在标准 DES 算法中，已知 DES 算法的第 3 个 S 盒如下：

S_3	列 行	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

如果该 S 盒的输入为 100011，则其输出的四位二进制数为（　　）

A. 1000　　B. 1001

C. 1010　　D. 1011

2. 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？（　　）

A. 2 位　　B. 3 位

C. 4 位　　D. 5 位

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

A. $\boldsymbol{M}^{-1}=\begin{bmatrix}3 & 3 & 6\\ 8 & 4 & 10\\ 1 & 4 & 6\end{bmatrix}(\mathrm{mod}\ \ 11)$　　B. $\boldsymbol{M}^{-1}=\begin{bmatrix}3 & 3 & 7\\ 8 & 4 & 10\\ 1 & 4 & 6\end{bmatrix}(\mathrm{mod}\ \ 11)$

C. $\boldsymbol{M}^{-1}=\begin{bmatrix}3 & 3 & 8\\ 8 & 4 & 10\\ 1 & 4 & 6\end{bmatrix}(\mathrm{mod}\ \ 11)$　　D. $\boldsymbol{M}^{-1}=\begin{bmatrix}3 & 3 & 9\\ 8 & 4 & 10\\ 1 & 4 & 6\end{bmatrix}(\mathrm{mod}\ \ 11)$

四、简答题（共 6 题，40 分）

1. （5 分）什么是重放攻击？请列举 3 种抵抗重放攻击的方法。

2. （4 分）请从中国信息安全管理部门的角度，分析美国的“棱镜计划”。

3. （8 分）什么是计算机系统的安全漏洞（即系统脆弱性）？列举 3 中常用的安全漏洞检测方法。

4. （8 分）什么是 hash 函数？列举 Hash 函数的 3 个特点？列举 2 个目前正在使用的 hash 函数，列举两种 hash 函数在网络安全中的典型应用。

5. （7 分）简述 ACK 泛洪攻击（ACK Flooding）和 SYN 泛洪攻击（SYN Flooding）的相同点和不同点。

6. （8 分）列举 4 种 IPSec 协议可以提供的安全服务，并说明这 4 种安全服务是由认证头协议（AH）还是封装安全载荷协议（ESP）来实现的。

五、（9 分）DH 密钥协商协议（Diffie-Hellman Key Agreement Protocol，简称 DH 协议）是密码学中经典的安全协议。利用 DH 协议通信双方 A 和 B 可以协商一个共享密钥 k_{ab}。结合安全协议的基本原理，回答以下问题：

（1）请简述通信双方 A 和 B 利用 DH 协议如何协商共享密钥 k_{ab}；

（2）说明 DH 协议存在的一种安全漏洞，并简述其攻击过程。

六、（15 分）某企业计划部署安全防御系统，以便提高企业内部网络的安全。某信息安全产品集成商为该企业提供了一个可供选择的信息安全产品列表（如表 1 所示）。

表 1　安全产品简表

序号	产品名称	产品特殊说明	单价（万元）
1	路由器	不具备包过滤功能	32.0
2	交换机 A	不支持 VLAN 功能	1.0
3	交换机 B	支持 VLAN 功能	6.0
4	网络地址转换（NAT）设备	最多可以同时支持 200 个用户	3.0
5	网络入侵检测系统	支持 TCP/IP 协议	15.0
6	防火墙 A	不支持状态包过滤	5.0
7	防火墙 B	支持状态包过滤	15.0
8	VPN 设备	提供完整性保护和认证功能	10.0

根据该企业的组网及信息安全防御系统部署需求，路由器为必选产品。如果你作为该企业的信息安全主管，请结合信息安全相关知识，回答以下问题：

1、在交换机 A 和交换机 B 中，请从信息安全的角度，给出选择交换机 B 的理由。

2、在防火墙 A 和防火墙 B 中，请从信息安全的角度，给出选择防火墙 B 的理由。

3、从便于事后分析及防止企业内部信息泄露的需求来看，不在上述列表中的哪类信息安全产品可供你选择？

4、如果你最终选择了路由器一台、交换机 A 一台、交换机 B 一台、网络地址转换设备一台、网络入侵检测系统一套、防火墙 B 一台、VPN 设备一台，请回答以下问题：

（1）针对你同时选择了网络地址转换设备和 VPN 设备，有人反对，其理由是 VPN 提供完整性保护，但 NAT 却要修改 IP 包中的 IP 地址，因此二者无法协同工作。你如何回答这一反对意见？

（2）有人说由上述设备构成的网络是一个交换式网络，因此网络入侵检测系统无法捕获网络数据包，导致该产品无法发挥其正常功能，因此你的产品选择是错误的。你如何看待这一质疑？

（3）请画出由这些设备所构成的安全防御系统的拓扑结构示意图（要求所有选择的产品必须用完），简要说明该安全防御系统提供的 3 种安全保护功能，以及这些功能是由哪些安全设备提供的（提示：某项功能可能由多个设备协调工作来实现）。

七、（15 分）某公司使用一个有密码保护的保险箱来保存机密文件。为了妥善保管该保险箱的密码 p，管理员使用了一个基于 Shamir 阈值方案（Shamir threshold Scheme）的(t，20)门限密码方案（$t \geq 2$），并将计算结果分别发送给 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，且任意 5 个密码管理员都可以恢复密码 p，请问 t 的取值是多少？说明理由。

（2）如果 t=3，且 20 个密码管理员中有一个不诚实，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？说明理由。

（3）如果 t=3，且 20 个密码管理员中有一个不诚实，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。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？说明理由。

八、（9 分）针对 RSA 算法的安全性问题，有人说可以通过求解 RSA 算法的模数 n 的欧拉数来破解 RSA 算法，从而证明 RSA 基于大整数因子分解困难性的理论依据不成立。试证明对 RSA 算法的模数 $n=pq$（其中 p 和 q 是两个素数）进行因子分解和求解 n 的欧拉函数 $j(n)$ 是等价的（即对于 $n=pq$，如果可以对 n 进行因子分解，就可以计算 $j(n)$；同样，如果可以计算 $j(n)$，也可以对 n 进行因子分解）。

九、（7 分）设 a 是大于 1 的整数，试证明：

（1）a 的除 1 以外的最小正因素 q 是素数；

（2）当 a 为合数时 $q \leq \sqrt{a}$ 。