

7. 以下关于入侵防护系统（IPS）的说法不正确的是（ ）
- A、入侵防护系统（IPS）可以检测网络攻击行为
 - B、入侵防护系统（IPS）可以保护一个网络
 - C、入侵防护系统（IPS）可以阻断检测出的攻击行为
 - D、入侵防护系统（IPS）可以对计算机病毒进行检测
8. 在 PDRR 模型中，（ ）是静态防护转化为动态的关键，是动态响应的依据。
- A、防护
 - B、检测
 - C、响应
 - D、恢复
9. 目前公认的最安全的身份认证机制是（ ）
- A、一次口令机制
 - B、双因素法
 - C、基于智能卡的用户身份认证
 - D、身份认证的单因素
10. 以下对木马阐述不正确的是（ ）
- A、木马可以自我复制和传播
 - B、有些木马可以查看目标主机的屏幕
 - C、有些木马可以对目标主机上的文件进行任意操作
 - D、木马是一种恶意程序，它们在宿主机器上运行，在用户毫无察觉的情况下，让攻击者获得了远程访问和控制系统的权限。
11. 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
12. PKI 体系中提供目录浏览服务的是（ ）
- A、安全服务器
 - B、CA 服务器
 - C、注册机构 RA
 - D、LDAP 服务器
13. $G(2)$ 上 n 级 m -序列的一个周期内，长为 $n-1$ 的游程有（ ）个
- A、0
 - B、1
 - C、2
 - D、 2^{n-1}
14. 整数 30 的欧拉函数 $\varphi(30)$ 等于（ ）
- A、8
 - B、18
 - C、20
 - D、29
15. 7^{804} 的后三位数字是（ ）
- A、400
 - B、401
 - C、402
 - D、403
16. 与 RSA (Rivest, Shamir, Adleman) 算法相比，DSS (Digital Signature Standard) 不包括（ ）
- A. 数字签名
 - B. 鉴别机制
 - C. 加密机制
 - D. 数据完整性
17. 非对称密码技术有很多优点，其中不包括（ ）
- A. 可提供数字签名、零知识证明等额外服务
 - B. 加密/解密速度快，不需占用较多资源
 - C. 通信双方事先不需要通过保密信道交换密钥

- D. 密钥持有量大大减少
18. 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
19. 以下关于 IPSec 中密钥管理说法正确的是（ ）
- A、互联网络安全关联和密钥管理协议（IAKMP）是 IPSec 密钥管理的框架
- B、因特网密钥交换协议（IKE）是 IPSec 密钥管理的框架
- C、Diffie-Hellman 密钥交换协议是因特网密钥交换协议（IKE）使用的密钥交换协议
- D、Oakley 不是因特网密钥交换协议（IKE）使用的密钥交换协议
20. Windows 系统登录流程中没有使用的系统安全模块是（ ）
- A、安全帐号管理(Security Account Manager, 简称 SAM)模块
- B、Windows 系统的注册(WinLogon)模块
- C、本地安全认证(Local Security Authority, 简称 LSA)模块
- D、安全引用监控器模块

二、多项选择题（每题 2 分，共 10 题， 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. 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、超时—重传机制 D、序列号机制
2. 以下哪些是 TCP 协议面临的攻击？（ ）
- A、SYN Flooding 攻击 B、ACK Flooding 攻击
- C、LAND 攻击 D、ARP 欺骗攻击
3. 下列属于完全备份机制特点的是（ ）
- A、每次备份的数据量较大
- B、每次备份所需的时间也就较大
- C、不能进行得太频繁
- D、需要存储空间小
4. 身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述正确的是（ ）
- A、身份鉴别是授权控制的基础
- B、身份鉴别一般不用提供双向的认证
- C、目前一般采用基于对称密钥加密或公开密钥加密的方法
- D、数字签名机制是实现身份鉴别的重要机制
5. 以下关于 MD5 算法的正确说法有（ ）
- A、MD5 是一个消息摘要算法标准
- B、MD5 的输入可以为任意长，但其输出是 128 位
- C、MD5 的输入可以为任意长，但其输出是 160 位
- D、MD5 算法不论输入多长，都必须进行消息填充
6. 下列关于 NAT 地址转换的说法中正确的是（ ）
- A、地址转换技术可以有效隐藏局域网内的主机，是一种有效的网络安全保护技术

- B、地址转换可以按照用户的需要，在局域网内向外提供 FTP、WWW、Telnet 等服务
 C、有些应用层协议在数据中携带 IP 地址信息，对它们作 NAT 时还要修改上层数据中的 IP 地址信息
 D、NAT 与防火墙能协同工作，但与 VPN 不能协同工作

7. 以下关于安全审计和安全审计系统的描述正确的是（ ）
 A、对入侵和攻击行为只能起到威慑作用
 B、安全审计不能有助于提高系统的抗抵赖性
 C、安全审计是对系统记录和活动的独立审查和检验
 D、安全审计系统可提供侦破辅助和取证功能
8. 通常而言，以下哪些是域名解析系统（DNS）潜在的安全威胁（ ）
 A、DNS 劫持攻击
 B、DNS 缓存污染
 C、DNS 拒绝服务攻击
 D、DNS 欺骗
9. 使用 ESP 协议时，可以使用的加密运算是（ ）
 A、DES
 B、3DES
 C、AES
 D、RSA
10. 对于 DOS 网络攻击，可以采用以下哪些措施来缓解主机系统进程被攻击（ ）
 A、缩短 SYN Timeout 时间和设置 SYN Cookie
 B、增加网络带宽
 C、在系统之前增加负载均衡设备
 D、在防火墙上设置 ACL 或黑客路由

三、计算选择题（每题 5 分，共 4 题，20 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. 60 阶循环群共有（ ）个生成元
 A、59
 B、30
 C、16
 D、8
2. DES 算法中的第一个 S 盒如下，如果该 S 盒的输入为 011001，则其输出为（ ）

列号	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
行号	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	2	14	10	0	6	13

- A、1101
 B、1110
 C、1001
 D、1010
3. 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、117
 C、173
 D、247

4. UNIX 系统中, 某文件的拥有者拥有读、写和执行的权限, 组和其他用户只有读的权限, 则该文件的权限值为 ()

- A、742
C、722
- B、744
D、711

四、简答题（共 5 题，30 分）

1. (6 分) 简述 Hash 函数的性质并给出 Hash 函数的两个简单应用。

2. (6分) SSL (Secure Socket Layer) 协议是为网络通信提供安全及数据完整性的一种安全协议, 请论述 SSL 握手协议的工作过程

3. (6分) 客户在网上商店选中商品, 并决定使用电子钱包付款, 简述一个成功的 SET 交易的标准流程。

4. (6分) 在校园局域网中捕获到一个以太网帧, 此帧的全部数据如下图所示, 请对照相关协议的数据结构图, 说明该数据帧的用途和封装的上层协议是什么? 并简述两个该协议可能面临的攻击。

```

Line      Source          Destination      Protocol    Info
-----
1 00:16:75:0e:b8:76 IntelOemBtSrv6 Groupcast ARP Who has 192.168.1.1?
C
# Frame 31 (60 bytes on wire, 60 bytes captured)
# Ethernet II Src: IntelOemBtSrv6 (00:16:75:0e:b8:76), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
# Destination: broadcast (ff:ff:ff:ff:ff:ff)
# Source: IntelOemBtSrv6 (00:16:75:0e:b8:76)
# Type: ARP (0x0806)
# Trailer: 0000000000000000000000000000000000
# Hardware Resolution Protocol (request)
# Hardware type: Ethernet (0x0001)
# Protocol type: IP (0x0800)
# Hardware size: 6
# Protocol size: 4
# Opcode: request (0x0001)
# Sender MAC address: IntelOemBtSrv6 (00:16:75:0e:b8:76)
# Sender IP address: 10.0.26.11 (10.0.26.11)
# Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
# Target IP address: 10.0.26.1 (10.0.26.1)

0000 ff ff ff ff ff ff 00 16 75 0e b8 76 06 00 01 ..... V.V.V...
0010 0e 00 05 04 00 01 00 16 75 0e b8 76 00 00 1a 0c ..... V.V.V....
0020 00 00 00 00 00 00 00 04 00 16 75 0e b8 76 00 00 00 ..... V.V.V....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... V.V.V....

```

5. (6 分) 在 RSA 公钥加密算法中, n 为算法使用的模数, 若敌手知道 $\phi(n)$, 是否能求出 p, q ? 请说明理由。

五、论述与综合分析题 (30 分)

1. (10 分) 设 Alice, Bob 是一对通信伙伴, Alice 是发方, Bob 是收方, 它们共享会话密钥 K_s , f 是公开函数。Alice 认证 Bob 是否是他的通信伙伴的协议如下:

(1) Alice 产生随机数 RN , 用 Ks 对其进行加密: $C=E(RN, Ks)$, 并将密文 C 发给 Bob。同时, Alice 对 RN 进行 f 变换, 得到 $f(RN)$ 。

(2) Bob 收到 C 后, 对其解密得到 $RN=D(C, K_s)$ 。然后 Bob 也对 RN 进行 f 变换, 得到 $f(RN)$, 并将其加密为 $C'=E(f(RN), K_s)$, 将 C' 发给 Alice。

(3) A 将收到的 C' 解密得到 $f(RN)$, 并将其与自己在第(1)步得到的 $f(RN)$ 比较。若两者相等, 则 Alice 认为 Bob 是自己的通信伙伴。否则 Alice 认为 Bob 不是自己的通信伙伴。

在上述认证协议中，函数 f 起什么作用？若去掉 f ，该认证协议是否安全？请说明理由。

2. (10 分) 在 Kerberos 协议中，存在四类角色：用户 (C)、认证服务器 (AS)、票据许可服务器 (TGS) 和服务端 (S)，用户的目的是通过认证服务器 AS 和票据许可服务器 TGS，获得访问服务端 S 的权限。在 Kerberos 协议中，所有通信都保证了机密性。针对 Kerberos 协议，回答以下问题：

(1) 从密码算法角度来看，哪类加密算法适用于 Kerberos 协议？

(2) Kerberos 协议使用什么机制防止重放攻击？

(3) 用户 (C) 和票据准许服务器 (TGS) 之间没有共享密钥，它们之间是如何实现加密通信的？

(4) 用户 (C) 和服务端 (S) 之间没有共享密钥，它们之间是如何实现加密通信的？

3. (共 10 分) 设一个 3 级线性反馈移位寄存器 (LFSR) 的特征多项式为 $f(x) = 1 + x^2 + x^3$ 。

(1) 画出该 LFSR 的框图；

(2) 给出输出序列的递推关系式；

(3) 设初始状态 $(a_0, a_1, a_2) = (0, 0, 1)$ ，写出输出序列及序列周期。

(4) 列出序列的游程。

六、计算题 (共 2 题, 20 分)

1. (10 分) 在数字签名标准 DSS 中，设 $p = 83, q = 41, h = 2$ 。求：

(1) 参数 g 。

(2) 取私钥 $x = 57$ ，求公钥 y 。

(3) 对设消息 M ，若 $H(M) = 56$ ，取随机数 $k = 23$ ，求 M 的签名。

(4) DSA 签名算法中，如果签名人选择的随机数 k 被泄露，将会发生什么问题？

2. (共 10 分) $p = 11, U_1, U_2, \dots, U_7$ 是 7 个用户。 i 是 U_i 的身份标识。在 $(3, 7)$ -Shamir 门限秘密分享方案中， U_i 得到的子密钥记为 K_i 。已知 $K_1 = 4, K_2 = 0, K_3 = 6, K_4 = 1, K_5 = 4, K_6 = 7, K_7 = 9$ 。可是，由于秘密分配者的粗心导致这些子密钥的某一个不正确。针对上述场景，试求解下列问题：

(1) 用插值公式计算 K_1, K_2, K_3 所确定的 Z_p 上的二次多项式，以及 K_4, K_5, K_6 所确定的 Z_p 上的二次多项式。

(2) 找出错误的子密钥并纠正之。

七、证明题 (10 分)

设 G 是一个群，求证 G 是交换群的充要条件是，对于 G 中任意元素 a, b ，都有： $(ab)^2 = a^2b^2$ 。