2018 期末卷

1. 不属于网络层的功能是：A. 差错控制 B. 流量控制 C. 数据转发 D. 设备间通信

2. 关于 Alhoa，错误的是：A. 可用于无线网络的信道分配 B. 可用于有线局域网 C. 适用于网络负载重的情况 D. 适用于网络负载轻的情况

3. 以太网 MAC 协议的最小帧长的作用 A. 冲突检测 B. 冲突避让 C. 冲突增强 D. 安全传输

4. IEEE802.11MAC 协议使用 CTS 控制帧通知隐藏终端互相避让 A.信标 B. RTS C. CTS D. ACK

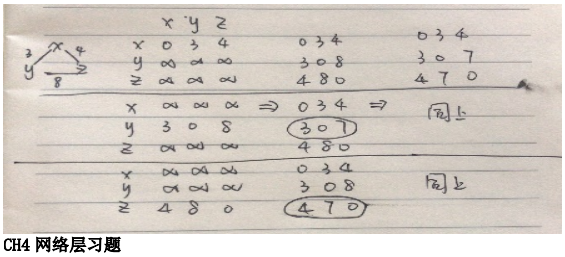
5. IPv4 首部分段偏移量的单位是__字节 A. 1 B. 2 C. 4 D. 8

6. 使用无分类地址的路由器为什么要用最长掩码匹配方式查找路由表?

答：这是由于采用 CIDR 后出现的问题：a-地址前缀的长度 prefix_len 无法从 IP 地址本身得到，且不同路由表项的 prefix_len 可能不同，只有查找路由表项才能得到。b-转发表中不同路由表项的地址前缀可能重叠，需选择前缀最长的匹配表项。

7. 使用 NAT 技术的依据：答：a 使用一个公用 IP 地址支持许多用户同时上网；b 仅为公共可访问的节点分配公用 IP 地址（减少需要的公用 IP 地址数）；c 网络内部节点对外是不可见的（安全考虑）。实现方法：将数据报中的（源 IP 地址，源端口号）替换为（NAT IP 地址，新端口号），记录每个（源 IP 地址，源端口号）与（NAT IP 地址，新端口号）的转换关系，取出数据报中的（目的 IP 地址，目的端口号）查找 NAT 转换表，然后用转换表中对应的（IP 地址，端口号）进行替换。端口号 16bits。

8. 使用距离矢量算法迭代计算每个路由器的向量表 8%



CH4 网络层习题

1. 一个子网 IP 地址为 10.115.0.0，子网掩码为 255.224.0.0 的网络，它的网络地址、广播地址、最小用户地址、最大用户地址分别是？答：网络地址：10.96.0.0； 广播地址：10.127.255.255;最小用户地址：10.96.0.1 ；最大用户地址：10.127.255.254

2. 假定路由器 R 的路由表如下。当目的地址为 201.4.20.126 的分组到达 R 时，R 将使用哪个接口转发该分组？答：s1 最长前缀匹配原则

掩码	网络地址	下一跳	接口
/26	180.70.65.192	-	s2
/22	201.4.20.0	-	s0
/24	201.4.22.0	-	s3
/25	201.4.20.0	-	s1

3. 一个 IPv4 分组的分片中，MF(或 M)位是 0【代表是最后一个分片】，HLEN 是 10，总长度是 200，分片偏移值是 300。试求**该分片**第一个字节和最后一个字节在原分组中的位置。

答：第一字节的位置是 2400(300*8)，最后一个字节的位置为 2559(2400+200-10*4-1)。（HLEN 单位是 4 个字节）

4. 基于目的地址转发“下一跳方法”的优缺点。答：

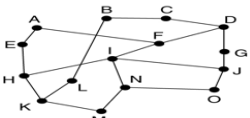
优点：每个路由表项只需保留“下一跳”的地址，无需给出完整的路由(路径)。

缺点：要求“下一跳”路由器知道剩余的路径信息或网络中的所有路由器信息保持一致。

5. RIP、OSPF 协议的缺点。答：RIP 缺点:(1)更新周期(30s)过短;(2)未进行区域划分

OSPF 缺点：用可靠广播方式在整个区域广播所有节点的链路状态，开销过大

6. 对于下图中的子网，若采用下列方法，从 K 开始广播需要产生多少个分组？(画出相应的树)



(1) 反向路径转发(Reverse path forwarding)？ 24 个分组

(2) 汇集树(sink tree)？ 最小生成树 14 个分组

7. 对于无控制洪泛、受控洪泛和生成树广播三种广播选路方式，下列说法是否正确：a) 一个节点可能收到同一个广播分组的多个拷贝；b) 一个节点可能在相同的出链路上多次转发同一个广播分组。答：无控制洪泛：a)对，b)对。受控洪泛：a)对，b)错。生成树广播：a)错，b)错。

8. 一个B类网络128.16.0.0/16被网络管理员划分为16个大小相同的子网，则子网掩码为__255.255.240.0__。如果按照IP地址从小到大对子网进行编号，写出第2个子网的地址范围，用a.b.c.d/x的形式表示__128.16.16.0/20__。

10. 一个路由器收到以下四条新的前缀：157.6.96.0/21、157.6.104.0/21、157.6.112.0/21和157.6.120.0/21，如果这些地址使用同一条输出线路，它们能被聚合吗？如果能，请给出聚合后的前缀；如果不能，请说明原因。答：能，聚合后的前缀是157.6.96.0/19 （取相同最长前缀）

11. 若路由器中有以下三条前缀表项：200.24.0.0/21、200.24.8.0/22、200.24.16.0/20。路由器收到目的地址为200.24.11.4的数据包，请问应使用哪个表项转发数据包?

答：使用200.24.8.0/22表项转发包

12. 按以下格式给出主机A和路由器R中的转发表，假设图中两个网络的子网掩码均为255.255.255.0，主机A的端口编号为1，路由器R的端口从左至右编号为1、2。

A的转发表

目的前缀	下一跳	输出端口
111.111.111.0/24	- （写直接交付也可以）	1
default 或者 222.222.222.0/24	111.111.111.110	1

R的转发表

目的前缀	下一跳	输出端口
111.111.111.0/24	- （写直接交付也可以）	1
222.222.222.0/24	- （写直接交付也可以）	2

CH4 网络层概念

1.网络层连接 vs 传输层连接:

传输层连接：进程-进程，连接状态仅保存在端系统中

网络层连接：主机-主机，连接状态保存在源主机、目的主机及所有中间路由器上

2. Internet（数据报网络）

计算机之间交换数据:弹性服务，没有严格的时序要求

终端（计算机）具有智能:可将复杂的工作（如差错控制）推到网络边缘，以保持网络简单

数据报网络只提供最小服务:可以运行在各种链路之上,增加新服务只涉及终端

ATM（虚电路网络）

由电信网发展而来:严格的时序和可靠性要求,要求保证服务

终端无智能或很少智能:复杂工作由网络完成，以保持终端简单

3.路由器三类交换结构：内存交换，总线交换，互联网络交换。当交换结构速率至少为端口速率的 n 倍（n 为输入端口数量）时，输入端口处不会出现排队。

4.TCP 头 20bytes，IP 头 20bytes，至少 40bytes。报头长度的单位是 4 字节。标志位：

MF（more fragments）：最后一个分片的 MF=0，其余分片的 MF=1

DF（don’t fragment）：DF=1 表示不允许对数据报分片

5.基于类的 IP 编址：A（0）类地址 1.0.0.0～126.255.255.255，地址个数 2^7-2 = 126，接口 2^{24}-2

B（10）类地址：128.0.0.0～191.255.255.255，地址个数 2^{14}-2 = 16382，接口数 2^{16}-2 = 65534

C（110）类地址的有效范围是：192.0.0.0～223.255.255.255，地址个数 2^{21}-2 = 2097152,接口 2^8-2

D（1110）类地址的范围是 224.0.0.0～239.255.255.255，用作多播地址。

网络号由 ICANN 统一分配，主机号由网络管理员统一分配。

6.试简单说明 IP、ARP、RARP、ICMP 的作用

IP 协议：实现网络互联。使参与互联的各个性能的网络从用户角度看好像是统一的网络。

ARP：完成 IP 地址到 MAC 地址的映射。RARP：使只知道自己硬件地址的主机知道其 IP 地址。

ICMP：允许主机或者路由器报告差错情况和提供有关异常情况的报告，共 15 种类型。从而提高 IP 数据成功交付率。但不纠正错误，差错报文发给源节点。

7. IP 使用逐跳路由：每个路由表项只记录去往目的地址的下一跳信息，而不是一条完整的路由.

8.分类编址的缺点：1-只能按照三种固定的大小分配地址空间，地址浪费严重。2-路由表必须记录每个已分配的网络，路由表规模爆炸式增长。CIDR：按照实际需要的地址数量分配地址空间，提高地址使用效率。允许将若干条路由聚合成一条路由，减小路由表规模。

9. DHCP 服务器使用 UDP 端口 67，客户使用 UDP 端口 68。主机广播 “DHCP discover” 报文寻找子网中的 DHCP 服务器。DHCP 服务器用 “DHCP offer” 报文进行响应给出推荐的 IP 地址及租期、其它配置信息

10.不产生 ICMP 差错报文的情况：对于携带 ICMP 差错报文的数据报，不再产生 ICMP 差错报文。对于分片的数据报，如果不是第一个分片，则不产生 ICMP 差错报文。对于具有组播(也称多播)地址的数据报，不产生 ICMP 差错报文。对于具有特殊地址(如 127.0.0.0 或 0.0.0.0)，不产生 ICMP 差错报文

11.ICMP 源节点抑制作用：通知源节点数据报已被丢弃。警告源节点，在路径中的某处出现了拥塞，源节点必须放慢(抑制)发送过程。

12.IPv6：ipv6 地址有 128bits，如 8000:0:0:0:0123:4567:89AB:CDEF，头有 40 字节。动机：IPv4 地址将很快耗尽，简化头部格式，加快数据报处理和转发，支持服务质量，支持多播，支持移动性，增强安全性。IPv6 与 IPv4 不兼容，但与其它所有因特网协议都兼容。

13.IPv4 到 IPv6 的过渡：双协议栈方案-支持 IPv6 的主机和路由器同时运行 IPv4 和 IPv6，源节点先查询 DNS：若 DNS 返回 IPv4 地址，发送 IPv4 分组；若返回 IPv6 地址，发送 IPv6 分组，双栈节点同时拥有 IPv4 和 IPv6 地址。对于数据包：采用报头转换，缺点是报头转换不完全，有信息丢失。或者建立隧道：将 IPv6 包封装到一个 IPv4 包中，送入 IPv4 网络，优点是保留原始数据报的全部信息。

14.选路算法分类：全局算法:所有路由器具有关于拓扑和链路代价的全部信息，集中式计算。分布式算法：路由器仅知道邻居节点以及到邻居节点的链路代价，通过与邻居交换信息，进行迭代计算。距离矢量算法 DV 是迭代的、异步的、分布式算法。

静态算法：路由随时间不变或缓慢变化（手工配置）。

动态算法：路由器根据拓扑及链路代价的变化而自动更新路由。

15.LS算法和DV算法的比较:

链路状态 LS:链路状态信息在全网传播，每个节点仅传播可靠的信息：亲自测量的本地链路代价（Dijkstra），节点计算的路由不传播，错误不扩散。

距离矢量 DV:距离矢量仅向邻居发送，节点传播的信息可能不正确.有些距离矢量是“道听途说”的，节点计算的路由要传播，会造成错误扩散。

16.RIP 与 OSPF 选路协议:RIP 在较低层 ISP 和企业网中使用，OSPF 较顶层 ISP 中使用。RIP 采用距离矢量法，选择跳数最少的路径，一条路径的最大代价限定为 15 跳，RIP 报文封装在 UDP 报文中发送，使用 UDP 端口 520（RIP 是一个应用层协议!）OSPF 采用链路状态法,选择代价最小的路径。链路代价：由管理员配置（由选路策略决定），OSPF 协议负责 OSPF 链路通告在网络中的广播及可靠传输，路由器根据收到的链路通告构造链路状态数据库。路由器利用链路状态数据库及 Dijkstra 算法，计算以路由器为根的最短路径树。

17.Intra-AS 和 Inter-AS 选路协议：Intra-AS 选路协议：也称内部网关协议 IGP,用于在 AS 内部交换选路信息，如 OSPF、RIP 使用某个路由测度（代价）选择到目的节点的最优路径.

Inter-AS 选路协议：用于在不同的 AS 之间交换选路信息，如 BGP 主要依据策略而不是路由测度去寻找可达路径（不追求最佳路径）.

18. 建立多播树的两种方法：1. 基于源的树：优点：多播分组总是使用最佳路径转发；缺点：路由器需要维护大量的多播树。2. 组共享树：优点：路由器对于每个组只维护一棵多播树;缺点：多播分组使用的转发路径可能不是最佳的。

CH5 链路层概念

1. 链路层服务：组帧（基本服务）将数据报封装到帧中，以及从帧中解封装数据报。链路接入（广播链路）在广播信道上协调各个节点的发送行为。可靠交付（部分协议提供）通过确认、重传等机制确保接收节点正确收到每一个帧（停-等、GBN、SR）低误码率链路（如光纤、某些双绞线）上很少使用，高误码率链路（如无线链路）应当使用。流量控制：调节发送速度，避免接收节点缓存溢出可以与可靠交付（如 GBN、SR）集成，也可以是单独的机制。差错检测。差错纠正（有些提供）：检测并纠正传输错误（不是通过重传）。半双工和全双工：半双工通信时，提供收/发转换。

2. 为什么在传输层与链路层上都需要可靠交付？传输层负责端到端，而链路层提供的是点到点的可靠交付，在一个节点向下一个节点发送数据帧时提供， 如果出现差错，可以在一段链路中进行重传， 而不是迫使传输层或应用层进行端到端的重传，然而。对于低比特差错的链路， 链路层可靠交付可能被认为是一种不必要的开销， 由于这个原因， 许多有线的链路层协议不提供可靠交付。链路层的一个重要特点是数据报在每一条链路上可能有不同的链路层协议所承载， 在第一段的可能是以太网协议， 第二段可能是 PPP 协议， 最后一段可能是 WAN 协议， 所以某段链路可能提供可靠的交付， 而某一段可能不提供， 所以，网络层在面对各段链路层提供的易购服务集合的情况下， 必须能够完成他端到端的任务。

3. 海明码与海明距离：检错能力：为检测出所有 d 比特错误，编码集的海明距离至少应为 d+1，纠错能力：为纠正所有 d 比特错误，编码集的海明距离至少应为 2d+1。

4. 多址接入 MAC 协议划分为哪三种类型？其中，哪一种（或几种）是无冲突的协议？哪一种（或几种）是有冲突的协议？答：多址接入 MAC 协议划分为信道划分、随机接入、轮流协议三种类型。信道划分为每个节点分配子信道，重负载高效，轮流协议是轮流发送，这两种是无冲突的；随机接入不划分信道，节点可自行决定何时发送，重负载低效，是有冲突的，且冲突后无法恢复。

5. 信道划分的类型：时分多址、频分多址、码分多址。

6. 若一无限用户 slotted ALOHA 信道处于负载不足与过载的临界点，则

(1)信道中空闲时槽的比例是多少？ 答：$p_0=e^{-G}$，G=1=p_0(空闲比例)=36.8%

(2)成功发送一个帧发送次数是多少？答：G/S=1/0.368≈2.72(注：$S=Ge^{-G}$)

7. 纯 aloha 最大效率 $Np(1-p)^{2(n-1)}$= 1/(2e) = 0.18

8. 时隙 aloha 协议优点：单个活跃节点可以信道速率连续发送。高度分散：节点自行决定什么时候发送。简单。缺点：发生冲突的时隙被浪费了。由于概率发送，有些时隙被闲置。需要时钟同步。

9. ARP 报文格式和解析流程：ARP 请求为 1，ARP 响应为 2，在以太网上，ARP 报文封装在以太帧中传输。解析流程：A 创建 IP 数据报，src IP=A，dest IP=B，A 查找转发表，得到下一跳地址 111.111.111.110，A 利用 ARP 获得下一跳 111.111.111.110 对应的 MAC 地址（R-1），A 创建链路层帧，封装 IP 数据包，src MAC =A，dest MAC = R-1，发送。R 接收帧，取出 IP 数据报，发现目的地址为 B，R 查找转发表，得知 B 在其端口 R-2 的直连网络上，R 利用 ARP 获得 B 的 MAC 地址，R 创建链路层帧，封装 IP 数据报，src MAC=R-2，dest MAC = B，发送。B 的网卡接收帧，取出 IP 数据报，交给网络层。

10. 为什么要有最小帧长？答：为确保发送节点在发送结束前检测到冲突，帧的发送时间必须足够长。若信号在以太网上相距最远的两个适配器之间的往返延迟为 2τ，那么帧的发送时间不应小于 2τ，即帧的最小长度≥链路速率×2τ。以太网标准规定最小帧长为 64 字节（不包括前导码），这个长度足以保证在 10Mbps 的最大直径以太网中，发送节点可在完成发送前检测到可能的冲突。

11. 交换机是如何提升网络性能的？答：划分冲突域，为每个端口提供专用的带宽。

12. 交换机和路由器：均为存储-转发设备：交换机工作于链路层，根据 MAC 地址存储转发帧；路由器工作于网络层，根据 IP 地址存储转发数据报。内部都有转发表：交换机：使用“逆向学习法”学习转发表，路由器：运行选路协议计算转发表。但交换机可以即插即用，转发速度快，成本低，不能连接 MAC 协议不同的网络；而路由器需要配置，转发速度慢，成本高，可以连接异构链路，可以阻断广播帧的传播。

13. VLan 划分方法：基于交换机端口、基于 MAC 地址、基于 IP 地址。

CH6 无线网概念

1. 隐藏/暴露节点：发送节点看不到，但影响接收方接收。发送节点能看到，以为冲突，但不影响接收。

2. IEEE 802.11 协议哪个(或几个)控制帧发现隐藏终端与暴露终端的？

答：(1) 隐藏终端：CTS；(2)暴露终端：RTS

3. 802.11 为什么不采用 csma/cd？答：发送过程中检测冲突很困难（接收信号的强度远小于发送信号的强度）不能检测出所有的冲突（隐藏节点），且冲突对无线网络损害很大，要尽可能避免。

4. 无线和移动网对上层协议的影响：性能上的影响很大，传输出错或切换都会导致丢包（丢包率高），链路层重传会产生很大延迟。TCP 将丢包（长延迟也当作丢包）解释为拥塞，不必要地减小拥塞窗口，导致应用吞吐率很低（无线链路的带宽本来就很低）。

CH5 链路层&局域网习题

2. IEEE 802.3 MAC 协议的全称？它是如何解决冲突的？

答：(1)1-坚持 CSMA/CD；(2)发前侦听，边发边听，冲突避让

3. 若某站点经历了 10 次（大于 10 次按 10 计算）连续冲突，则该次冲突导致站点在 IEEE 802.3、802.3u 网络中站点的平均等待时间分别为多少？

答：(1)1024/2=512； 802.3:512*51.2μs； (2)802.3u:512*5.12μs

5. IEEE 802.3 MAC 协议中最小帧长的功能与计算依据？

答：最小帧长的功能：检测冲突。 计算依据：传输速率*相距最远的两个站点间传播时延

6. 假定生成多项式 $G(x)=(x^4+x^2+1)(x+1)$，试计算帧 100110101100 的循环冗余码(CRC)。答：001101

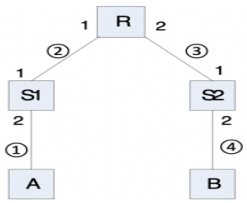
7. 假定生成多项式 $G(x)=(x^4+x^3+1)(x+1)$，试计算帧 100110101100 的循环冗余码(CRC)。答：11101

9. 为什么 ARP 请求封装在一个广播帧中发送，而 ARP 响应封装在一个单播帧中发送？

答：发送节点利用 ARP 请求查询目标主机的 MAC 地址，由于尚不知道目标主机的 MAC 地址，所以 ARP 请求封装在广播帧中发送。发送 ARP 响应的节点已经从 ARP 请求中获得了请求节点的 MAC 地址，所以 ARP 响应可以用单播帧发送。

10. 假设节点 A、B、C 连接到同一个广播局域网上，A 向 B 发送的单播帧（dest MAC = B），C 的适配器能收到吗？如果能收到，C 的适配器会处理这个帧吗？如果会处理，C 的适配器会把帧中的 IP 数据报交给自己的网络层吗？答：能收到；会处理；但不会将 IP 包交给自己的网络层。

11. 在如图所示的网络中，路由器 R 连接了两个链路层交换机 S1 和 S2。假设主机 A 向主机 B 发送了一个数据报（src IP = A，dest IP = B），请给出编号①～④的线路上传输的以太帧的源地址和目的地址，填入下表。MAC 地址用符号表示，比如 A 的 MAC 地址表示为 A，R 的端口 1 的 MAC 地址表示为 R-1，等等。



线路编号	Src MAC	Dest MAC
1	A	R-1
2	A	R-1
3	R-2	B
4	R-2	B

13. 16 个(编号 1 ~ 16)站点正在竞争一条采用自适应遍历树(adaptive tree walk)协议的共享信道. 若地址编号大于或等于 13 的站点全部处于发送就绪状态，则需要多少时槽才能解决竞争？答：11 个

14. ADSL 通道数(子频带)？其中数据通道数？若每个通道均使用 QAM-128 调制，数据通道总容量？256,248,248*7*4k

15. 首先计算 frame 100110101111 及 $G(x)=(x^4+x^3+1)(x+1)$ 的 CRC，然后描述 $G(x)$ 的检错能力.(1)G(x)=x^5+x^3+x+1(101011)，CRC=00000 (2)检错能力：①可检测所有单个错误(G(x)多于一项)②奇数个错误(含 1+x 项)③2 个错误(说明：该项回答不出不扣分)④长度不大于 5 的突发错误⑤$(1-2^{-4})$长为 6 的突发错误⑥$(1-2^{-5})$更长和突发错误

16. 若使用一个 256-kbps 的无差错卫星信道(往返传播时延为 512-msec)一个方向上发送 512-byte 数据帧，而在另一个方向上返回很短的确认帧。则对于窗口大小为 1, 15, 127 的最大吞吐量是多少?512*8/256k=16ms

(1)k=1,16/(16+512)*256=7.75 (2)k=15,7.75*15=116.36 (3)k=127,256

17. HDLC 与 PPP 协议的主要区别？

(1)HDLC 使用序列号(滑动窗口协议)，PPP 在控制域为缺省值时不使用序列号(停等协议)且为不可靠传输(2)HDLC 面向 bit 填充(同步传输)，PPP 除支持面向比特填充(同步传输，直接使用 HDLC 协议)，还可使用面向 byte 填充(异步传输，使用类 HDLC 协议 RFC1662)(3)PPP 基于 HDLC，主要用于在点到点链路上传输 IP 流量，并可支持多种网络协议

18. 假设数据帧为 D bits，链路带宽为 b bps，链路出错概率为 p，采用前向纠错策略需要 x bits 的冗余码，采用检错加重传策略需要 y bits 的冗余码。试比较分析两种策略的带宽利用率与时延性能。

(1)前向纠错策略：传输数据量 D+x，传输次数 1，故带宽需求量为(D+x)、传输时延为(D+x)/b

(2)检错加重传策略：一次传输数据量 D+y，传输次数 1/(1-p)，故带宽需求量为(D+y)/(1-p)、传输时延为(D+y)/(b*(1-p))

CH8 网络安全

0. 数字签名是一种可提供发送方身份鉴别、报文完整性和防发送方抵赖的安全机制。(20 分)

（1）请给出数字签名最常见的构造方法。

（2）根据数字签名的构造方法，说明数字签名为什么可以提供以上安全服务。

答：(1) 当实体 A 需要为报文 M 生成数字签名时，A 首先用一个散列函数计算 M 的报文摘要，然后用 A 的私钥加密该报文摘要，生成数字签名。

(2) A 的私钥是只有 A 知道的秘密，任何其它实体无法得到，因而一个有效的数字签名可提供发送方身份鉴别。报文摘要可用于检测报文的完整性，对报文内容的任何修改将产生不同的报文摘要。用 A 的私钥加密后的报文摘要是不可伪造的，从而数字签名就将 A 与报文 M 紧密关联在一起，既能提供报文完整性服务，也能防止发送方抵赖。

1. 在下面的空格中填入“谁的什么密钥”：

A 向 B 发送一个一次性会话密钥，A 用___B 的加密密钥(公钥)_加密该会话密钥。

Certifier.com 用____CA 的私钥_____为 foo.com 签发公钥证书。

A 向 B 发送一个签名的报文，A 用_____A 的私钥_____生成这个数字签名。

A 向 B 发送一个可供鉴别的报文，A 用_____与 B 共享的密钥_____生成报文鉴别码（写出一种方法即可）。

2. 在下面的空格中填入可实现相应安全服务的安全机制：

机密性：加密 完整性：报文鉴别 防抵赖：数字签名 防假冒：鉴别

3. 在下面的空格中填入需要用到的算法或函数的序号：①对称密钥算法，②公开密钥算法，③散列函数，④密码散列函数。（报文鉴别码写出一种方法即可）

生成数字签名__3__ 数据加密__1__ 生成报文鉴别码 __4__ 加密会话密钥__2__

4. RSA 算法，p=3，q=11（1） 求 n，z （2） 选择 e=3，d=7 可以吗？原因。 （3）用(e,n)加密 M=9，得到 C；用(d,n)解密 C，给出过程。

1）n=pq=33，z=(p-1)(q-1)=20

2)可以。选择一个小于 n 的数 e，且 e 与 z 没有公因数即可。且 ed-1 可以被 z 整除。

3)C=M^e mod n =9^3 mod 20 = 9； M=c^d mod n = 9^7 mod 20 = 9

5. Diffie-Hellman 密钥交换过程：

q 是一个素数，q=97；a < q ，a 是 q 的一个素根 a=5，公开 a，q。

A 选择一个私有的 X_A，X_A< q，X_A=36，计算公开的 Y_A，Y_A= a^{X_A} mod q=50。

B 选择一个私有的 X_B，X_B< q，X_B=58，计算公开的 Y_B，Y_B= a^{X_B} mod q=44。

A 计算会话密钥 K=$(Y_B)^{X_A}$ mod q= 75，B 计算会话密钥 K=$(Y_A)^{X_B}$ mod q=75。