# 参考答案

### 第一周：

**参考答案：**

**1) 由于A先发报文所以，A的报文在路由器的队列中排在B的报文前面，所以A交付2Mbits报文需要时间为：2/10+2/20+2/10=0.5s=500ms；（3分）**

**B将1Mbits的文件交付给D需要时间为：1/10+2/20(排队时间)+1/20+1/10=0.35s=350ms。（3分）**

**2) 从t=0时刻到t=0.1s，A发送了1000个分组，用时：1000×1000/10000000=0.1s，**

**从t=0.1s时刻起与B共享连接路由器的链路，平均各共享到带宽10Mbps，A大约再用时：1/10+2×1000/10000000=0.1002s交付剩余的1000个分组，故A向C交付2Mbits文件大约需要(0.1+0.1002)s≈0.2s；（3分）**

**B向D交付1Mbits文件需要时间大约为：1/10+2×1000/10000000=0.1002s≈0.1s。（3分）**

**3) 分组交换比报文交换更公平。（2分）**

### 第二周：

考虑两台主机A和主机B由一条带宽为R bps、长度为M米的链路互连，信号传播速率为V m/s。假设主机A从t=0时刻开始向主机B发送分组，分组长度为L比特。试求：

1) 传播延迟（时延）dp；

2) 传输延迟dt；

3) 若忽略结点处理延迟和排队延迟，则端到端延迟de是多少？

4) 若dp>dt，则t=dt时刻，分组的第一个比特在哪里？

5) 若V=250000km/s，L=512比特，R=100 Mbps，则使带宽时延积刚好为一个分组长度（即512比特）的链路长度M是多少？

**(注：1k=10^3,1M=10^6)**

**1.参考答案：**

**1) 传播延迟（时延）dp=M/V；（2分）**

**2) 传输延迟dt=L/R；（2分）**

**3) 端到端延迟de= L/R+M/V；（2分）**

**4) 若dp>dt，则t=dt时刻，分组的第一个比特所在位置是：距离主机A的Vdt米的链路上；（2分）**

**5) 带宽时延积=Rdp=RM/V=512，因此， M=512V/R=512×250000000/100000000 =1280米。（2分）**

**2.参考答案：**

**1) 传送该文件的吞吐量：TH=500kbps；（3分）**

**2) 传送该文件到主机B大约需要时间：T=4×8×10^6/(500×10^3)=64s。（3分）**

### 第三周：

**1.参考答案：**

**1）浏览器解析到URL对应的IP地址的最短时间是：RTTd；（2分）最长时间是：4RTTd。（2分）**

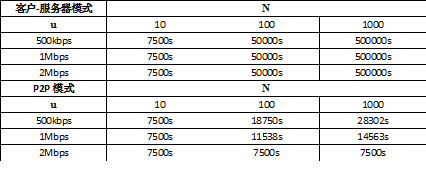
**2）若浏览器没有配置并行TCP连接，则基于HTTP1.0获取URL链接Web页完整内容需要的时间：18RTTh。（2分）**

**3) 若浏览器配置5个并行TCP连接，则基于HTTP1.0获取URL链接Web页完整内容需要的时间：6RTTh。（2分）**

**4) 若浏览器没有配置并行TCP连接，则基于非流水模式的HTTP1.1获取URL链接Web页完整内容需要的时间：10RTTh；（2分）基于流水模式的HTTP1.1获取URL链接Web页完整内容需要的时间：3RTTh。（2分）**

### 第四周：

**参考答案：**

****

#### 第六周：

#### 第八周：

**1.参考答案及评分标准：**

**(1)DHCP服务器可为主机2~主机N动态分配IP地址的最大范围是：111.123.15.5～111.123.15.254；（2分）主机2发送的封装DHCP Discover报文的IP分组的源IP地址和目的IP地址分别是0.0.0.0和255.255.255.255。（2分）**

**(2)主机2在通过DHCP服务器获取IP地址的同时还可以获取:子网掩码（255.255.255.0）、默认网关（111.123.15.1）和域名服务器IP地址。（3分）**

**(3)主机1能访问WWW服务器，但不能访问Internet。（2分）由于主机1的子网掩码配置正确而默认网关IP地址被错误地配置为111.123.15.2（正确IP地址是111.123.15.1），所以主机1可以访问在同一个子网内的WWW服务器，但当主机1访问Internet时，主机1发出的IP分组会被路由到错误的默认网关（111.123.15.2），从而无法到达目的主机。（1分）**

#### 第九周：

**1．参考答案及评分标准：**

**（1）R1的路由表：**

**目的网络            接口**

**192.168.1.0/24          S1（2分）**

**192.168.1.192/26        E0（2分）**

**192.168.2.0/23          S0（2分）**

**（2）R1更新后的路由表：**

**目的网络            接口**

**192.168.1.0/25          S1（2分）**

**192.168.1.128/26        S0（2分）**

**192.168.1.192/26        E0（2分）**

**192.168.2.0/23          S0（2分）**

**R1的距离向量：**

**192.168.1.0/25          2（2分）**

**192.168.1.128/26        3（2分）**

**192.168.1.192/26        1（2分）**

**192.168.2.0/23          2（2分）**

#### 第十三周：

1.参考答案：

1）明文“This is an easy problem”加密后的密文是：“uasi si my cmiw lokngch”；

2）密文“rmij'u uamu xyj”解密后的明文是“wasn't that fun”。

2.参考答案：

1）能破解；（1分）因为在单码替代密码系统中，字母之间的替代关系是固定的，而选择明文中已包含了所有字母，所以选择明文攻击可以完全确定字母替代关系，所以可以破解。（2分）

2）不能直接破解；（1分）因为在多码替代密码系统中，字母之间的替代关系是不固定的，因此，尽管选择明文中已包含了所有字母，但并不能直接完全确定字母替代关系，所以不能直接破解。（2分）

3.参考答案：

1）n = p\*q = 55, z = (p-1)(q-1) = 40；

2）因为e = 3时满足，e<n，且与z没有公因子；

3）d=27；

4）m = 8, m^e = 512, 密文c= m^e mod n = 17.

4.参考答案：

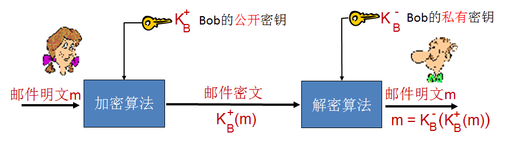


注：H(.)为散列函数。

5.参考答案：

1)不能；（2分）由于Alice没有公钥-密钥对，且Alice和Bob之间没有共享密钥，因此Bob无法核实邮件消息是由Alice创建的。（2分）

2)可以；（2分）原理框图如下：



（2分）

6.参考答案：

不会；(2分)因为伪造的TCP无法通过数据完整性校验（攻击者没有共享的MAC密钥）。(2分)

7.参考答案：

1).由于IV = 11, 所以密钥流为：111110100000 ……….

对于给定的消息 m = 10100000，ICV = 1010 XOR 0000 = 1010

于是，WEP分组的3个字段分别为：

IV: 11（2分）

加密的消息: 10100000 XOR 11111010 = 01011010（2分）

加密的ICV: 1010 XOR 0000 = 1010（2分）

2).接收端提取IV(11)，生成密钥流：111110100000 ……….

解密恢复消息 m = 01011010 XOR 11111010 = 10100000；（2分）

解密恢复 ICV = 1010 XOR 0000 = 1010。（2分）

利用恢复得到的消息m的前4比特与后4比特进行异或，得到：

1010 XOR 0000 = 1010 = ICV（恢复的），通过完整性校验。（2分）

3).由于ICV是消息的前4比特与后4比特的异或结果，因此，Trudy只需再翻转消息的第一个比特或者第五个比特即可使得接收到的分组通过ICV检查。（2分