Please DO NOT upload questions and answers onto the Internet.

1.1	D	1.2	C	1.3	E	1.4	B	1.5	A
1.6	A	1.7	D	1.8	D	1.9	A		

2. (a)

IP address: 203.211.152.66 Port number: 53

(b) TTL

(c) 58.26.128.0

3. (a)

$$\begin{aligned} C &= B * log_2(1+SNR) \\ &= 3 * 10^3 * log_2(1+511) \\ &= 27,000 \text{ bps} \end{aligned}$$

(b)

$$\frac{1.8 * 10^6}{60 * 3} = 10,000$$

(c) 00111010

4.

# of pkt = $\left\lceil \frac{400 * 10^3}{1000-80} \right\rceil = 435$

Total # of bits sent = 435*80 + 400,000 = 434,800

Length of first 434 packets: 1000
Length of last packet: 800

End-to-end delay = $\frac{1000}{10^3} + 40 + \frac{434{,}800}{10^3} + 40 = 515.8$ ms

5.

1. Alice encrypts m with her private key to create digital signature $K_A^-(m)$.
2. Alice concatenates message with digital signature $m \oplus K_A^-(m)$, and encrypt the extended message with Bob's public key: $K_B^+(m \oplus K_A^-(m))$.
3. Alice sends $K_B^+(m \oplus K_A^-(m))$ to Bob.
4. Bob decrypts the received message using his private key: $K_B^-(K_B^+(m \oplus K_A^-(m))) = m \oplus K_A^-(m)$.
5. Bob then uses Alice's public key to derive message from digital signature: $K_A^+(K_A^-(m)) = m'$
6. If $m = m'$, message authenticity (and integrity) are preserved.
7. Because message is encrypted during transmission, message confidentiality is preserved.

(Another solution is for Alice to send $K_B^+(m) \oplus K_A^-(K_B^+(m))$)

6.

(a) Fill in the initial distance vectors of routers A to C.

	cost to A	cost to B	cost to C	cost to D	cost to E	cost to F
from A	**0**	**2**	**5**	**-**	**-**	**-**
from B	**2**	**0**	**-**	**1**	**2**	**-**
from C	**5**	**-**	**0**	**1**	**-**	**-**

(b) Fill in the final distance vectors of routers A to C.

	cost to A	cost to B	cost to C	cost to D	cost to E	cost to F
from A	**0**	**2**	**4**	**3**	**4**	**5**
from B	**2**	**0**	**2**	**1**	**2**	**3**
from C	**4**	**2**	**0**	**1**	**4**	**3**

(c) Fill in the following forwarding table of router A.

To destination Net	Next hop
137.132.58.128/28	B
137.132.89.0/26	**B**
137.132.80.128/25	**B**
137.132.82.0/24	**B**

(d)

All traffic between (A, D), (A, E) and (A, F) is sent via B. The link between A and C is under-utilized while the link between A and B may be overloaded.

7.

(a)	**(b)**
1000	**53000**

(c)

Y buffers out-of-order packets. The packet with sequence number 53000 is an out-of-order packet. If it were discarded by receiver, X will not retransmit D before this packet is retransmitted (and acknowledged). This is because TCP sender only maintains one timer and resends the oldest unacknowledged packet upon timeout.

(d)

Assumption: packets may be lost or corrupted but will not be reordered by the network.

The previous packet C is received at 110 ms. Once corresponding ACK reaches X, X will start a timer for packet D. When timer expires, D will be resent and received by Y at 190 ms.

Assume propagation delay is d ms. ACK of packet C take d to reach X. Timeout period is (slightly greater than) $2d$. Retransmission takes another d. Therefore $4d = 190 - 110$. Timeout value chosen by X is slightly greater than $2d$ which is 40 ms.

(Other reasonable answers will also be accepted.)