University of Barishal
Department of Computer Science and Engineering
Course Title: Computer Networks
Course Code: CSE-3105
3rd Year 1st Semester Final Examination
Admission Session: 2017-2018

Marks: 60

Time: 03 Hours

N.B.: Answer any **FIVE** questions out of the followings. All parts of each question must be answered consecutively. Right side of the question shows the maximum marks.

1.a) What is DHCP? How does DHCP work? Write down the advantages and disadvantages of DHCP? **4**

b) Depict the format of global unicast address in IPv6 addresses. Does there any specific relationship between hostid (at the IP level) and link-layer address? Explain. **4**

c) Define the following Concepts: Computer Network, Network Architecture, Protocol, and Multilayer Protocol. **4**

2.a) Consider sending 4000-byte IP datagram (including the 20 bytes IP header) into a link that has an MTU of 1400 bytes. Determine the values of the length field and the offset field in each fragment. **5**

b) Explain the connection establishment and connection termination process of TCP protocol. **4**

c) What do you mean by loopback interface? An organization is assigned the block 2000:1456:2474/48. What is the IPv6 address of an interface in the third subnet if the IEEE physical address of the computer is $(F5\text{-}A9\text{-}23\text{-}14\text{-}7A\text{-}D2)_{16}$? **3**

3.a) An ISP is granted a block of addresses with 190.100.0.0/16 (65,536 addresses). The ISP needs to distribute these addresses to three groups of customers as follows: **6**

   i) The first group has 64 customers; each need 256 addresses

   ii) The second group has 128 customers; each need 128 addresses

   iii) The third group has 128 customers; each need 64 addresses

Design the subblocks and find out how many addresses are still available after this allocation.

b) Find errors, if any, in the following IPv4 address. **2**

   i) 111.56.045.78   ii) 110101.23.14.69

   iii) 75.35.325.12   iv) EF6.23.00011.6

c) A block of addresses is granted to a small organization and we know one of the addresses is 205.16.37.39/25. Find the first address, last address and number of addresses in the block. **4**

4.a) What is RSA algorithm? Alice wants to send message a to Bob. Then Bob needs to select keys. Suppose, Bob chosen p = 5 and q = 7 in the RSA algorithm. Now, find the value of d. Also, encrypt the message "BU" using Bob's public key so that he can only decrypt. For simplicity, do the encryption and decryption character by character. **5**

b) What is Digital Signature? How it can be implemented to provide authentication? **4**

c) Alice has found a way to write secretly to Bob. Each time, she takes a new text, such as an article from the newspaper, but inserts one or two spaces between the words. A single space means a binary digit 0; a double space means a binary digit 1. Bob extracts the binary digits and interprets them using ASCII code. Is this an example of cryptography or steganography? Explain. **3**

5.a) In an IPv4 datagram, the value of total-length field is $(00A0)_{16}$ and the value of the header-length (HLEN) is $(5)_{16}$. How many bytes of payload are being carried by the datagram? What is the efficiency (ratio of the payload length to the total length) of this datagram? **3**

b) List three forwarding techniques and give a brief description of each. 3

c) Derive the routing table for the following Fig. 1. Can router R1 receive a packet with destination address 140.24.7.194? What will happen to the packet if this occurs? 6
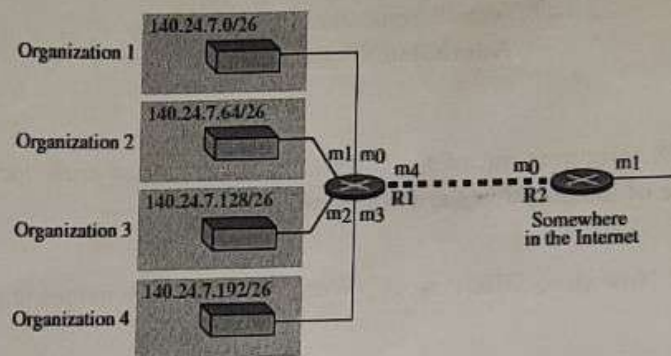

Fig. 1

6.a) Define Routing Protocol. Use Dijkstra's algorithm to find the shortest path tree and the forwarding table for node A in the Fig. 2. 5
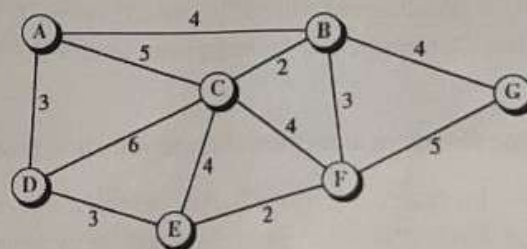

Fig. 2

b) What are the policies of congestion control in TCP? Explain any of them with necessary diagram. 5

c) What is IP address? Compare between IPv4 and IPv6 address. 2

7.a) What is Cryptography? Distinguish between passive and active attacks. 3

b) What are the differences between message confidentiality and message integrity? Can you have one without another? Use the additive cipher with k = 2 to encrypt the plaintext "CSE". Then decrypt the message to get the original plaintext. 5

c) Is it possible for an attacker to launch a man-in –the-middle attack on the DH scheme? If so, explain why and how? 4

8.a) How message authentication code (MAC) works? Does it provide Confidentiality? Justify your answer. 4

b) Assume we have a very simple message digest. Our unrealistic message digest is just one number between 0 and 25. The digest is initially set to 0. The cryptographic hash function adds the current value of the digest to the value of the current character (between 0 and 25). Addition is in modulo 26. What is the value of the digest if the message is "CSE"? Why is this digest not secure? 4

c) What is the purpose of the Integrated Services Digital Network (ISDN)? Explain different ISDN components. 4

"Nothing can stop you until you choose to be stopped."