ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)

ORGANISATION OF ISLAMIC COOPERATION (OIC)

Department of Computer Science and Engineering (CSE)

35

SEMESTER FINAL EXAMINATION — WINTER SEMESTER, 2022-2023

DURATION: 3 HOURS — FULL MARKS: 150

CSE 4585: Computer Networks

Programmable calculators are not allowed. Do not write anything on the question paper.

Answer **all 6 (six)** questions. Figures in the right margin indicate full marks of questions whereas corresponding CO and PO are written within parentheses.

---

1. a) Explain how the slot time in CSMA/CD is related to the maximum network length. Suppose that you would like to increase the link speed of your Ethernet cable, how would this upgrade affect the minimum required packet size? If you upgrade your cable to a higher speed and realize that you cannot change the packet size, what else can you do to maintain the correct operation? — 5 + 5 (CO1) (PO1)

   b) Suppose an Ethernet destination address is 05:01:02:03:04:05. Mention the type of the address? How does the address appear on the line in binary? — 5 (CO1) (PO1)

   c) Briefly explain the learning procedure of a transparent bridge with a suitable example. Demonstrate the major problem of a transparent bridge. — 5 + 5 (CO1) (PO1)

2. a) "The RTS-CTS hand-shaking can be a solution to the hidden station problem but it cannot help in solving the exposed station problem"- Explain with the aid of necessary diagrams. — 8 (CO1) (PO1)

   b) Briefly explain the access method (baseband layer) of Bluetooth. Mention the effective length of a one-slot frame and a three-slot frame of Bluetooth. In a Bluetooth frame, why does the 54-bit header portion contain three identical 18-bit sections? — 8 (CO1) (PO1)

   c) Distinguish between the Distributed Coordination Function (DCF) and the Point Coordination Function (PCF) as a MAC sublayer for IEEE 802.11. What is a repetition interval and why this is necessary? — 9 (CO1) (PO1)

3. a) TCP uses a sliding window technique for flow control. The sender has sent bytes up to 202 and the receiver has sent an acknowledgement number of 200 with an *rwnd* of 12 bytes (assume the *cwnd* is 20). Depict the current window. After some time the sender has received an acknowledgment value of 204 and an *rwnd* of 6. Draw the new window. Is there any problem with the current window? If yes, explain the problem with the possible solution. — 8 (CO2) (PO1)

   b) Suppose you have a TCP source, which starts transmission from segment number 15 with an initial value of slow start threshold 65000. Draw the timing diagram (time axes toward the bottom of the page for both the source and destination) for the successful transmission of segments of at least 10. The diagram should include slow start phase, congestion avoidance phase, and congestion detection phase with one packet loss identified by triple duplicate acknowledgement and one by time out. Assume a suitable segment size. — 9 (CO2) (PO1)

   c) With the aid of necessary equations explain how the value of Retransmission Time-Out (RTO) is calculated for the Retransmission timer. Your answer should include a scenario incorporating the Karn's algorithm. — 8 (CO2) (PO1)

4. a) What is IP address space depletion? Briefly explain different measures to handle IP address depletion. 8 (CO2) (PO1)

b) What is the subnet address and broadcast address of the host 192.168.10.244/29? A router receives a packet on an interface with a destination address of 192.168.10.174/28. What will the router do with the packet? 5 (CO2) (PO1)

c) Neatly sketch different components of an ARP package. Explain how ARP is used to create a subnetting effect. 4 + 4 (CO2) (PO1)

d) What is the purpose of including the IP header and the first 8 bytes of datagram data in the error reporting ICMPv4 messages? 4 (CO2) (PO1)

5. a) SCTP is a message-oriented, reliable protocol that combines the good features of UDP and TCP. SCTP provides additional services not provided by UDP or TCP, such as multiple-stream and multihoming services. Explain the features that help SCTP to provide the additional services. How does a SCTP packet differ from a TCP segment? 6 + 4 (CO2) (PO1)

b) SCTP uses a four-way handshaking for an association establishment whereas TCP uses a three-way handshaking for a connection establishment. What are the improvements of SCTP association establishment with the cost of an extra message passing? An SCTP client opens an association using an initial tag of 100, an initial TSN of 66, and a window size of 20000. The server responds with an initial tag of 1971, an initial TSN of 1998, and a window size of 15000. Show the time-line diagram of the association establishment. 5 + 5 (CO2) (PO1)

c) TCP uses two timers namely persistence and keepalive to handle deadlock and long idle sessions. How does SCTP handle these events? 5 (CO2) (PO1)

6. a) Give the taxonomy of attacks in relation to security goals. Can you have integrity without confidentiality? Justify your answer. 2 + 3 (CO4) (PO1)

b) A small private club has only 100 members. Answer the following questions:

i. How many secret keys are needed if all members need to send secret messages to each other? If a member needs to send a message to another member, he/she first sends it to the president; the president then sends the message to the other member. How many secret keys are needed if everyone trusts the president of the club? 3 (CO4) (PO2)

ii. If the president decides that two members who need to communicate should contact him first. The president then creates a temporary key to be used between the two. The temporary key is encrypted and sent to both members. How many secret keys are needed? 2 (CO4) (PO2)

iii. Design an authentication protocol for the above club where the president can play the role of a Trusted Third Party (TTP). Your scheme should provide mutual authentication and should avoid the reflection attack as well as the playback attack. 5 (CO4) (PO2)

c) Asymmetric-key/Public-key cryptography uses two separate keys: one private and one public. Asymmetric-key cryptography means that Bob and Alice cannot use the same set of keys for two-way communication. Bob needs only one private key to receive all correspondence from anyone in the community, but Alice needs n public keys to communicate with n entities in the community. 4 + 6 (CO4) (PO2)

i. Does the advent of asymmetric-key cryptography eliminate the need for symmetric-key cryptography? Justify your answer.

ii. What are the differences in the function of asymmetric-key cryptography between a digital signature and a cryptosystem (encryption)? Use the necessary diagrams to support your answer.