**Chapter6 - Congestion Control:**

1. What are the issues in resource allocation?
2. Know the categories of Resource allocation – Router centric, Reservation based, Window based.
3. How resource allocation performance is measured or explain the power of a Network. How Load and throughput contribute to performance?
4. Explain fairness in resource allocation. In practical communication all paths are not same, know how to apply fairness, Study Raj Jain’s fairness index.
5. FIFO queue, Fair queue – what are issues in these schemes and how to solve those issues in FIFO or Fair queue? What is weighted Fair queue?
6. TCP congestion control protocols – Slow start, Additive increase/Multiplicative decrease, fast retransmit and fast recovery. Know how to solve a given problem applying these protocols. You may be asked to draw the in-transit packet flow between sender and receiver.
7. How does TCP congestion control differ from Flow control?

**Chapter8 – Network Security (Slides in 11/21/2022 week):**

1. What are the known security attacks? What problem do they cause?
   1. Eavesdrop: intercept message
   2. Inserting messages into connections
   3. Impersonation: can fake source address (spoof) in packet
   4. Hijacking: take over connection (sender or receiver)
   5. DoS (denial of service)
2. What are Symmetric and Public Key encryptions?
   1. **Symmetric Key**:
   2. **Public Key**:
   3. **Secret key > secret decryption algorithm**
3. Digital certificate and public key encryption – What are the relation between them?
4. Describe a scenario where symmetric key and public key encryption are both needed to ensure Confidentiality, integrity, and Authenticity.
   1. **Confidentiality**: only sender and intended receiver can understand contents. Sender encrypts / receiver decrypts
   2. **Authentication**: sender and receiver confirm identities
   3. **Message Integrity**: sender/receiver want to ensure message not altered without detection (during transit and after)
   4. **Access and Availability**: services available and accessible to users
   5. **Scenarios**:
5. Why Symmetric key encryption may not be enough to ensure all sorts of network security issues?
6. Why Public key encryption is not used to encrypt the total data transfer or network communication despite being strongly secured?
7. What are DES and AES? Both encryption algorithms
   1. DES:
   2. AES:
8. **Be able to compute the cipher text if the key, algorithm, and plain text is given.**

**Chapter9 - Applications:**

1. Know about the different application protocols for Email messages, Web protocols Such as SMTP, HTTP. Know the issues and solutions of the older versions of SMTP and HTTP
2. What are some differences between URL and URI?
3. Why caching is used in HTTP? What problems does it solve?
4. How DNS works? What is the benefit of Hierarchical structure of DNS?
5. Be able to draw the steps of finding an end IP address from a network graph via DNS query.
6. What are some possible risks/attacks for DNS?