**Exam. Code: 0918**
**Sub. Code: 33455**

**2055**
**B.E. (Computer Science and Engineering)**
**Sixth Semester**
**CS-601: Computer Networks and Security**

**Time allowed: 3 Hours** **Max. Marks: 50**

***NOTE:*** ***Attempt five questions in all, including Question No. 1 (Section-A) which is compulsory and selecting two questions each from Section B-C.***

*x-x-x*

## Section – A

I. Attempt the following:

a) Differentiate between Local Area Network (LAN) and Wide Area Network (WAN) with suitable examples.
b) Difference between Distance Vector Routing and Link State Routing with an example.
c) Explain the difference between UDP and TCP protocols.
d) Explain open loop and closed loop congestion control techniques.
e) What is piggybacking? Explain its advantages and disadvantages. (5x2)

## Section – B

II. a) With reference to Classful addressing, you are given a subnet mask as 255.255.254.0. Describe the following:
   i) Total number of hosts that can be configured in the network.
   ii) Total number of subnets if the network is Class A.
   iii) Identify and explain the purpose of any six key fields in the IPv4 header.
   b) Explain the terms slow start, additive increase and multiplicative decrease with the help of diagram in the context of TCP congestion control. (2x5)

III. a) Consider a network A using the IP protocol with a Maximum Transmission Unit (MTU) of 520 bytes. Assume that the IP header is 20 bytes. Consider a network B with a Maximum Transmission Unit (MTU) of 200 bytes and an IP header of 20 bytes.
   i) What is the maximum data that the datagram at network layer can carry in network B?
   ii) Suppose a datagram in network A has to be sent to network B. In network A, how many fragments will a datagram has to be fragmented and why?
   iii) Discuss the potential impact of fragmentation on network performance and efficiency.
   b) What is Domain Name System (DNS)? What are the resources associated with it? Why is DNS over HTTPS preferred over traditional DNS? Justify with security vulnerabilities. (2x5)

IV. a) Write the difference between Symmetric Key and Public Key authentication with suitable examples. Also explain the respective advantages and disadvantages.
   b) A company wants to ensure confidentiality, integrity, and authenticity for the security of web-based transactions process. Define a hybrid cryptographic solution using SSL/TLS and digital certificates. Justify the approach with diagram illustrating the SSL/TLS handshake with digital certificates. (2x5)

P.T.O.

## Section - C

V. a) Discuss the application layer protocols FTP, Telnet, SNMP and SMTP.

b) Explain the IP Security (IPSec) architecture and its role in securing network communications.

(2x5)

VI. a) Explain in detail the concept of switching in computer networks. Provide a scenario where virtual circuit switching would be preferable over packet switching and justify your choice.

b) Compare and contrast the TCP/IP and OSI Reference Model with the key factors of TCP/IP Protocol suite. (2x5)

VII. a) Explain how Diffie-Hellman Key Exchange prevents eavesdropping. Derive its mathematical formulation and discuss its vulnerabilities.

b) Suppose you want to send a 10-bit message (1101010110) using a CRC technique, where the CRC generator is 1011.

i). Calculate the CRC code that needs to be appended to the message before transmission. Show the step-by-step calculations.

ii). Mention and explain any two error control techniques other than CRC with the help of an example.

(2x5)