Reg. No. : E N G G T R E E . C O M

Question Paper Code : 20928

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2023.

Fourth Semester

Electronics and Communication Engineering

EC 3401 – NETWORKS AND SECURITY

(Regulations 2021)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Compare between point-to-point and multipoint connections in network.

2. If the data link layer can detect errors between hops, why do you think we need another checking mechanism at the transport layer?

3. Find the error, if any, in the following IPv4 addresses.

   (a) 111.56.045.78

   (b) 75.45.301.14

4. Compare between Intradomain and Interdomain routing protocols.

5. Differentiate between Connectionless and Connection-Oriented Service.

6. Why do we need a DNS system when we can directly use an IP address?

7. List the security services in network.

8. Why is the Caesar cipher substitution technique vulnerable to a brute-force cryptanalysis?

9. Who are the potential adversaries to implant a hardware Trojan?

10. How potential vulnerabilities can be introduced by design flaws?

PART B — (5 × 13 = 65 marks)

11. (a) With neat diagram, illustrate in detail about the seven layers of the OSI - architecture model.

Or

(b) (i) Exemplify in detail about TCP/IP protocol suite. (7)

(ii) Find the minimum Hamming distance for the following cases :

- Detection of two errors.
- Correction of two errors.
- Detection of 3 errors or correction of 2 errors.
- Detection of 6 errors or correction of 2 errors. (6)

12. (a) (i) Compare and contrast between IPv4 addresses and IPv6 addresses. (6)

(ii) Illustrate IPv6 datagram packet format with neat diagram. (7)

Or

(b) (i) Enumerate three transition strategies to move from IPv4 to IPv6. Illustrate the difference between tunneling and dual stack strategies during the transition period. When is each strategy used? (7)

(ii) Exemplify in detail about Internet Control Message Protocol (ICMP) error reporting messages. (6)

13. (a) Discuss in detail about User Datagram Protocol (UDP) with neat diagrams.

Or

(b) (i) Explain in detail about the congestion control and avoidance techniques. (7)

(ii) Describe about HTTP architecture and its functionality. (6)

14. (a) (i) Explain in detail about OSI Security Architecture model with diagram. (6)

(ii) Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES.

- XOR of subkey material with the input to the f function
- XOR of the f function output with the left half of the block
- Swapping of halves of the block. (7)

Or

(b) (i) Write down the RSA algorithm and illustrate with an example. (7)

(ii) Illustrate the working nature of Secure Hash Algorithm (SHA). (6)

15. (a) (i) The RSA-T 100 Trojan is triggered when a 32-bit specific plaintext is applied. Calculate the probability of triggering this Trojan if one uses random patterns as plaintext. (7)

(ii) Exemplify the main idea of side channel analysis. Compare between invasive and noninvasive attacks. (6)

Or

(b) (i) Illustrate the basic steps to perform a front-side electrical probing attack. (6)

(ii) Discuss in detail about block chain technology and its features. (7)

PART C — (1 × 15 = 15 marks)

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

- The first group has 64 customers; each need 256 addresses.
- The second group has 128 customers; each need 128 addresses.
- The third group has 128 customers; each need 64 addresses.

Design the subblocks and find out how many addresses are still available after these allocations

Or

(b) A client uses TCP to send data to a server. The data are 16 bytes. (i) Calculate the efficiency of this transmission at the TCP level (ratio of useful bytes to total bytes). (ii) Calculate the efficiency of transmission at the IP level. [Note : Assume no options for the P header]. (iii) Calculate the efficiency of transmission at the data link layer. [Note : Assume no options for the IF header and use Ethernet at the data link layer].