(b) Explain the working of email security using PGP. Explain how confidentiality, integrity and non-repudiation is implemented using PGP. (CO4)

(c) Explain how security is implemented in Wireless networking. Write about WAP end to end security. (CO4)

5. (a) What do you mean by IDS and IPS ? Explain how it works, also state its advantages. (CO5)

(b) Explain the following terms : (CO5)

(i) SPAN (Switched Port Analyser)

(ii) Packet Filter Firewall

(iii) Distributed Denial of Service Attack

(iv) Rootkit

(c) What do you mean by Malware ? Write about *five* types of Malwares attacks. Also state how to solve the problem of malware. (CO5)

H Roll No. .....

TCS–619

B. TECH. (CSE) (SIXTH SEMESTER)
END SEMESTER
EXAMINATION, June, 2023

NETWORK AND SYSTEM SECURITY

Time : Three Hours

Maximum Marks : 100

Note : (i) All questions are compulsory.

(ii) Answer any *two* sub-questions among (a), (b) and (c) in each main question.

(iii) Total marks in each main question are **twenty**.

(iv) Each sub-question carries 10 marks.

1. (a) Explain the following terms : (CO1)

(i) Access Control

(ii) Masquerade attack

(iii) Routing Control

(iv) Traffic Padding

P. T. O.

(b) What do you mean by Network Security Model ? Explain it with a neat diagram. (CO1)

(c) Differentiate between the following : (CO1)

(i) Authentication and Access Control

(ii) Block Cipher and Stream Cipher

(iii) Security Mechanism and Security Services

(iv) Snooping and Spoofing

2. (a) Explain with the help of suitable block diagram how Confidentiality and Authentication is achieved in Message Authentication using Message Encryption Technique. (CO2)

(b) Calculate the value of Private and public key pair using RSA algorithm, given that $p = 19$; $q = 11$. Also show the Encryption and decryption steps using the plain text value of M = 4. Write all the steps involved. (CO2)

(c) Explain about Digital Signature Standard with the help of a neat diagram. (CO2)

3. (a) What do you mean by Public Key Infrastructure (PKI) ? Explain how PKI plays a role in reliable distribution and verification of Digital Signature and Public key. (CO3)

(b) Users A and B want to establish a secret key using Diffie-Helimen key exchange protocol using a common prime $q = 353$, a primitive root $\alpha = 3$, A's secret key $X_A = 97$ and B's secret key $X_B = 233$. Compute (i) A's public key, Y_A (ii) B's public key, Y_B (iii) A's and B's common secret key, K. (CO3)

(c) What are the various technologies to implement web security ? Explain about SSL/TLS and SSH. (CO3)

4. (a) Explain the working of "ipsec" in detail. Write about the two major phases and their importance. Write about the protocols which are used in "ipses". Write about the two modes in which "ipsec" is implemented. (CO4)