4. (a) Explain about the complete implementation of ipsec security with diagrams. Give details of each phase and also write about the protocols used in each phase. (CO4)

(b) Explain how e-mail security works. State the differences between PGP and S/MIME. (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 Firewall ? Explain how it works. Also state its advantages and disadvantages. (CO5)

(b) Explain the following : (CO5)

(i) Intrusion Detection System

(ii) Gateway

(iii) Distributed Denial of Service Attack

(iv) Rule Based Firewall

(c) What do you mean by Malware ? Write about *five* types of Malwares attacks which has caused wide spread damages in year 2021 onwards. (CO5)

530

H **Roll No.** ....

TCS–619

B. TECH. (CSE) (SIXTH SEMESTER)

END SEMESTER EXAMINATION, 2022

NETWORK 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) What do you mean by confusion and diffusion in cryptography ? State the differences between diffusion and confusion with examples. (CO1)

P. T. O.

(b) State about the various security attacks in X.800 security architecture. Also write about the security services and mechanisms used to implement security in any organization. (CO1)

(c) What do you mean by Access Control ? Write an explain how access control is different from authentication. (CO1)

2. (a) With the help of a diagram, briefly discuss the functions performed in a single round in DES. Also draw the block diagram of double and triple DES. (CO2)

(b) Calculate the value of private and public key pair using RSA algorithm, given that $p = 7$; $q = 11$. Also show the encryption and decryption steps using the plaintext value of M = 5. Write all the steps involved. (CO2)

(c) Explain about digital signature standard with the help of a neat diagram. Also state how it is different than RSA approach. (CO2)

3. (a) What do you mean by Authentication ? How is it different from integrity ? Explain X.509 authentication service with relevant diagrams. (CO3)

(b) Users A and B want to establish a secret key using Diffie-Hellman 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 : (CO3)

(i) A's public key, Y_A

(ii) B's public key, Y_B

(iii) A's and B's common secret key, K

(c) Explain about the various technologies which are implemented in network, transport and application layer of OSI network model to impart web security. (CO3)