5. (a) What do you mean by firewall ? Write about the different types of firewalls available. State how a firewall is different from intrusion detection system. (CO5)

(b) Explain the following term : (CO5)

(i) Intrusion detection system

(ii) Packet filter firewall

(iii) Distributed denial of service attack (DDoS)

(iv) Intellectual property.

(c) What do you mean by malware ? Write about *five* types of malwares attacks along with their solutions and precautions. (CO5)

110 O

H Roll No. ....

TCS–392

B. TECH. (CSE) (THIRD SEMESTER) END SEMESTER EXAMINATION, Dec., 2023

INTRODUCTION TO CRYPTOGRAPHY

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 network security model ? Explain the key components with suitable block diagram. (CO1)

(b) Write about the security services and mechanisms used in implement security in any organization. State the relationship between them. (CO1)

(c) What do you mean by authentication and authorization ? Write and explain how authentication and authorization is important in network and web security. (CO1)

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

(b) State how a stream cipher is different from a block cipher. Explain the importance of pseudorandom generator. (CO2)

(c) State how modern block ciphers convert a plain text into cipher text. State how cryptographic strength is increased in a modern block cipher. (CO2)

3. (a) Calculate the values of the following (show the steps) : (CO3)

(i) 2^{51} mod 17

(ii) 2^{245} mod 11

(b) Explain with suitable diagram the various key distribution techniques available in symmetric key distribution. (CO3)

(c) State the various ways public key is distributed in an asymmetric encryption. (CO3)

4. (a) Explain with the help of suitable block diagram how confidentiality, Authentication and integrity is achieved in message authentication using message authentication code. (CO4)

(b) Explain about digital signature with the help of a block diagram. Also state how message authentication and public key cryptography is used in a digital signature. (CO4)

(c) Calculate the value of private and public key pair using RSA algorithm, given that p = 1; q = 13. Also show the encryption and decryption steps using the plain text value of M = 5. Write all the steps involved. (CO4)

P. T. O.