(c) Calculate the value of Private and Public key pair using RSA algorithm, given that p = 11; q = 13. Also show the Encryption and Decryption steps using the plain text value of M = 5. Write all the steps involved. (CO4)

5. (a) Explain how confidentiality, integrity and authentication is offered by PGP (pretty good privacy) State what extra services are offered (apart from the 3 services stated above) by GP in email security. (CO5)

(b) Explain the following terms : (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 5 types of Malware attacks which has caused widespread damages in recent times. (CO5)

H Roll No. .....

TCS–491

B. TECH. (CSE)
(FOURTH SEMESTER)
END SEMESTER EXAMINATION,
June/July, 2022
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 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 stated in x.800 security architecture. Also write about the security services and mechanisms used to implement security in an organization. (CO1)

(c) What do you mean by Access Control ? Write and 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) Explain what do you mean by Stream Cipher ? State the importance of pseudo randon number generators in a Stream Cipher. (CO2)

(c) State how Modern Block ciphers converts a plain Text into Cipher Text. State how cryptographic strength is increased in a modern block cipher. (CO2)

3. (a) Explain the role of Modular arithmetic in cryptography. What do you mean by Euclid's Theorem and Fermet's Theorem ? Explain them with a suitable example. (CO3)

(b) Explain with suitable diagram the various Key distribution techniques available in symmetri 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)

P. T. O.