

B.Tech IV Year I Semester (R20) Regular Examinations December/January 2024

CRYPTOGRAPHY & NETWORK SECURITY

(Common to CSE (DS) and CSE)

Time: 3 hours

Max. Marks: 70

PART – A
(Compulsory Question)

- 1 Answer the following: (10 X 02 = 20 Marks)
- | | |
|--|----|
| (a) Define Steganography. | 2M |
| (b) What is privacy? | 2M |
| (c) Explain Euler's theorem. | 2M |
| (d) Define Elliptic Curve Cryptography. | 2M |
| (e) How digital signature is important in Cryptography? | 2M |
| (f) List some applications of cryptographic hash function. | 2M |
| (g) Define Kerberos. | 2M |
| (h) How to encapsulate security payload? | 2M |
| (i) Write a note on firewall. | 2M |
| (j) Define SSH Protocol. | 2M |

PART – B

(Answer all the questions: 05 X 10 = 50 Marks)

- 2 With a neat sketch Explain the OSI Security Architecture. 10M
- OR**
- 3 (a) What is AES and how does it works? Why the AES algorithm is necessary? 5M
(b) Explain the data encryption standard. 5M
- 4 What is Diffie - Hellman key exchange and how does it works? Consider Diffie - Hellman key exchange between two parties A and B. Let A sends $J = Nx1 \pmod p$ and B sends $K = Nx2 \pmod p$ respectively. Let $N = 5$, $x_1 = 3$, $x_2 = 6$ and $p = 23$. How to calculate and find the shared key between two parties. 10M
- OR**
- 5 (a) Demonstrate the working process of RSA Algorithm. 6M
(b) Explain Chinese remainder theorem. 4M
- 6 (a) When to use the Secure hash algorithm in cryptography? 5M
(b) Write a brief note on X.509 certificate. 5M
- OR**
- 7 (a) Distinguish HMAC and CMAC. 5M
(b) Explain message authentication function. 5M
- 8 How does the electronic mails will be secure? How to choose the type of electronic mail security with an example? 10M
- OR**
- 9 (a) What is Internet key exchange? 5M
(b) List the principles of remote user authentication. 5M
- 10 What is firewall? Explain the types of firewalls with an example. How the firewall will works? 10M
- OR**
- 11 Brief note on: 10M
(i) HTTPS,
(ii) TLS.
