

**20P340**

(Pages: 2)

Name.....

Reg. No.....

**THIRD SEMESTER M.Sc. DEGREE EXAMINATION, NOVEMBER 2021**

(CBCSS-PG)

(Regular/Supplementary/Improvement)

**CC19P CSS3 E02c - CRYPTOGRAPHY AND NETWORK SECURITY**

(Computer Science)

(2019 Admission onwards)

Time: Three Hours

Maximum: 30 Weightage

**PART A**

Answer any *four* questions. Each question carries 2 weightage.

1. What is Brute force attack?
2. Explain DES.
3. What is MAC?
4. What is SSH?
5. How are digital signatures used for securing the network system?
6. Write the significant features of WORMS.
7. What is intrusion detection?

**(4 × 2 = 8 Weightage)**

**PART B**

Answer any *four* questions. Each question carries 3 weightage.

8. Explain Fiestal Cipher Round Structure.
9. Explain the HMAC algorithm and structure.
10. Explain key distribution using asymmetric encryption.
11. Give a brief overview of cipher block modes of operation.
12. Write a note on HTTPS.
13. Explain Diffie Hellman Key Exchange.

**(4 × 3 = 12 Weightage)**

**PART C**

Answer any *two* questions. Each question carries 5 weightage.

14. Explain in detail AES structure and associated algorithms.
15. Give a detailed account of Kerberos.
16. Discuss the aspects of transport Layer security.
17. Explain security attacks, services and mechanisms.

**(2 × 5 = 10 Weightage)**

\*\*\*\*\*