QP-6320

Seat No.

Total No. of Pages : 2

MAR_APR 2025 SUMMER EXAMINATION

1156 Master of Technology

Sub. Name: Cryptography & Network Security

Sub. Code: 72685

Day and Date: JUNE ,06-06-2025 **Total Marks: 70**

Time: 10:30 AM To 01:30 PM

Instructions: **1. All questions are compulsory**
2. Assume suitable data wherever necessary and mention it boldly
3. Figures to the right indicate full marks

Q1) Solve any TWO **[14]**

a. With help of diagram explain a model for network security **[7]**

b. Explain RSA algorithm **[7]**

c. Write short note on “Polyalphabetic Ciphers”. **[7]**

Q2) Solve any TWO **[14]**

a. Discus three critical aspects of block cipher design **[7]**

b. Explain the overall scheme for DES Encryption **[7]**

c. Write short note on “Caesar Cipher”. **[7]**

Q3) Solve any TWO **[14]**

a. Explain the nature of Brute-Force attacks for hash functions and MAC’s. **[7]**

b. With the help of diagram explain the concept of public key cryptography **[7]**

c. Write note on Types of Viruses **[7]**

Q4) Solve any TWO **[14]**

a. Give the difference between Kerberos: version 4 and 5. **[7]**

b. Describe IPsec Authentication Header with help of its format **[7]**

c. Write note on Requirements for a Hash function **[7]**

Q5) Solve any TWO **[14]**

a. Explain three classes of Authentication functions **[7]**

32328

b. Write note on Combinations of SAs in IPsec **[7]**

c. Give the overview of IP security **[7]**

End Of Question Paper

Important Note for Chief Exam Officer / SRPD Coordinator / Sr Supervisor/ Student -
This Question Paper may be distributed for following Subjects as common code.
सदरची प्रश्नपत्रिका खालील विषयांकरिता वितरित करता येईल.

1] (1156) Master of Technology (CBCS) (72685) Cryptography & Network Security Part 1 SEM 2

322328