

M.Tech. Computer Science & Engineering (CBCS Pattern) Semester-II  
**PCSS243 - Network Security & Cryptography**

P. Pages : 1

Time : Three Hours



**GUG/S/25/10998**

Max. Marks : 70

- 
- Notes :
1. Solve **any five** questions.
  2. All questions carry equal marks.
  3. Due credit will be given to neatness and adequate dimensions.
  4. Assume suitable data wherever necessary.

- |    |    |  |   |
|----|----|--|---|
| 1. | a) | What is the difference between passive and active security threat?       | 7 |
|    | b) | What is OSI security architecture?                                       | 7 |
| 2. | a) | What is steganography? Where it can be used?                             | 7 |
|    | b) | Discuss in detail the architecture and authentication about IP security. | 7 |
| 3. | a) | List important design considerations of a stream cipher key              | 7 |
|    | b) | Explain Diffie- Hellman key exchange algorithm.                          | 7 |
| 4. | a) | Explain HMAC algorithm in detail.  | 7 |
|    | b) | Explain Miller - Rabin algorithm.  | 7 |
| 5. | a) | Explain digital signature standard.                                      | 7 |
|    | b) | Explain public - key cryptosystem.                                       | 7 |
| 6. | a) | Discuss about the concept of electronic mail security.                   | 7 |
|    | b) | Discuss in detail C-MAC Algorithm.                                       | 7 |
| 7. | a) | Discuss the architecture and authentication in IP security.              | 7 |
|    | b) | Explain multipurpose internet mail extension.                            | 7 |
| 8. | a) | What is the purpose of S-boxes in DES?                                   | 7 |
|    | b) | Explain about viruses in detail.   | 7 |

\*\*\*\*\*