

M. Tech. Computer Science & Engineering (CBCS Pattern) Semester - II
PCSS243 / 24(C) - Network Security & Cryptography

P. Pages : 1

Time : Three Hours



GUG/S/23/10998

Max. Marks : 70

- Notes :
1. Solve **any five**.
 2. All questions carry equal marks.
 3. Due credit will be given to neatness and adequate dimensions.
 4. Assume suitable data wherever necessary.
 5. Diagrams and Chemical equation should be given wherever necessary.
 6. Illustrate your answers wherever necessary with the help of neat sketches.

1. a) Explain Specific Security Mechanism and Pervasive security mechanism. **8**
b) Explain key objectives that are at the heart of computer security. **6**
2. a) Give reasons why computer and network security is complex. **8**
b) Explain model for network security using neat labelled diagram. **6**
3. a) Explain five ingredients of Symmetric encryption scheme. Also explain symmetric cryptosystem with neat labelled diagram. **8**
b) List and explain conventional encryption scheme for attack. Also give three independent dimensions of cryptosystem. **6**
4. a) Explain Authentication with two specific authentication services. **6**
b) Explain: **8**
 - i) Steganography
 - ii) Types of attacks on messages and known to cryptanalyst.
5. a) Explain general scheme for DES Encryption with General Depiction of DES Algorithm. **8**
b) Explain Stream Cipher and Block Cipher. **6**
6. a) Explain Secure Hash Algorithm. **8**
b) Explain Block Cipher design principles. **6**
7. a) Explain public key Cryptography with neat labelled diagram. **8**
b) Explain five possible approaches for attacking RSA algorithm. **6**
8. a) Explain RSA processing of Multiple blocks with neat labelled diagram. **8**
b) Explain Diffie-Hellman key exchange algorithm with diagram. **6**
