



- Notes :
1. All questions are compulsory.
  2. Due credit will be given to neatness and adequate dimensions.
  3. Assume suitable data wherever necessary.

1. Explain following transposition technique with suitable example. **16**

- i) Rail-fence technique
- ii) Simple columnar technique

**OR**

2. a) Explain in brief all types of network security services. **8**

b) Write note on:- **8**

- i) Denial of service attack
- ii) Man-in-middle attack

3. What is an AES algorithm? Explain with diagram. **16**

**OR**

4. a) Write note on:- **8**

- i) CFB
- ii) OFB

b) Explain working of international data encryption algorithm (IDEA) in detail. **8**

5. a) Explain in detail MDS algorithm. **8**

b) Explain digital signature in detail. **8**

**OR**

6. a) Discuss in detail, the concept of Kerberos. **8**

b) Explain Public Key cryptography algorithm in detail. **8**

7. Write note on: **16**

- i) SET
- ii) PGP

**OR**

8. a) Discuss Email privacy in detail. **8**
- b) Discuss pretty good privacy in detail. **8**
9. a) Write a note on following malicious programs. **8**
- i) Logic Bomb
- ii) Trojan Horse
- b) What are the firewall design principles. Explain in detail. **8**

**OR**

10. a) Define virus. Explain different types of viruses differentiate between virus & worms. **8**
- b) What is intruder? Classify their classes and discuss intrusion detection techniques. **8**

\*\*\*\*\*