N. B:

1) All questions are compulsory.
2) Make suitable assumptions wherever necessary and state the assumptions made.
3) Answers to the same question must be written together.
4) Numbers to the right indicate marks.
5) Draw neatly labeled diagrams wherever necessary.
6) Use of Non-programmable calculators is allowed.

**1. Attempt *any two* of the following.**

- **a.** Describe the various security services.
- **b.** What are poly-alphabetic ciphers? Explaining one technique with suitable example
- **c.** What is cryptanalysis? Explain different cryptanalysis attacks
- **d.** What is DDOS attack? What are the ways in which DDOS attack can be classified?

**2. Attempt *any two* of the following.**

- **a.** Explain the working of AES round in detail.
- **b.** Explain the encryption operation used inRC5 algorithm
- **c.** Explain the working of IDEA algorithm
- **d.** Write a note on Blowfish.

**3. Attempt *any two* of the following.**

- **a.** What is message digest? Explain.
- **b.** Explain the working of the SHA algorithm
- **c.** What is a digital signature? Explain the different categories of verification.
- **d.** Explain the ElGamal cryptosystems

**4. Attempt *any two* of the following.**

- **a.** Explain the Diffie Hellman's Key agreement algorithm and its vulnerability
- **b.** What is Key pre-distribution? Explain
- **c.** Write a note on station-to-station protocol.
- **d.** What is KDC? Explain its different implementations and significance.

**5. Attempt *any two* of the following.**

- **a.** What are firewalls? What are its characteristics and limitations?
- **b.** Write a note on IPSec Architecture
- **c.** What is SSL Record protocol? Explain its operations
- **d.** Explain the Handshake protocol action

**6. Attempt *any two* of the following.**

- **a.** Explain the password based authentication system. What are the problems associated with passwords?
- **b.** Write a note on Kerberos
- **c.** Explain Biometric authentication technique.
- **d.** What is certificate based authentication and explain its working.

7. **Attempt *any three* of the following.**

**a.** What are the different goals of security? Explain the different attacks these security goals are vulnerable to

**b.** Explain the working of DES function in details

**c.** What is Asymmetric encryption? Explain the RSA algorithm used for asymmetric encryption

**d.** Explain the concept of Digital Certificate and how it is created?

**e.** What are the approaches used to detect intrusion? Give a brief description of each

**f.** Write a note on Authentication token.