**Q.P. Code: 24747**

**(3 Hours)** **[Total Marks:80**

**N.B** (1) Question No1 is compulsory.

(2) Attempt any three out of remaining questions.

(3) Figures to the right in parenthesis indicate full marks.

**1.** (a) Explain overview of DES with one round in detail? **[10]**

(b) Explain and differentiate between the various architectures of a firewall and its implementation? **[10]**

**2.** (a) What do you mean by Intrusion Detection System? Discuss the various types of intrusion detection system **[10]**

(b) Discuss Authentication? Explain how authentication can be done using tokens? **[10]**

**3.** (a) What are Digital certificates? Explain the stepwise process of certificate generation? How is Digital Certificate issue and by whom? **[10]**

(b) What is the need for database security? Explain database access control and inference control? **[10]**

**4.** (a) Define Message Digest. Explain MD5 and compare with SHA? **[10]**

(b) Define WEP authentication. Explain authentication and key agreement in 802.11i? **[10]**

**5.** (a) Discuss email security with respect to PGP and S/MIME. **[10]**

(b) Analyze RSA and its security. Why is RSA a secure algorithm? Give an example? **[10]**

**6.** Write a short note on (Any four) **[20]**

(i) Digital Signatures

(ii) Web Services Security

(iii) Defense Against Denial-of-Service Attacks

(iv) SET Participants

(v) TKIP