Q.P. Code : 360900

(3 Hours) **Total Marks : 100**

Note : 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 **neat labeled diagrams** wherever **necessary.**
6) Use of **Non-programmable** calculators is **allowed.**

1. Attempt **any two** of the following: **10**
   a) Write a note on Security mechanism
   b) What is Kerberos? Explain.
   c) Explain the SSL architecture and explain the SSL protocol stack.
   d) What is DDOS attack? What are the ways in which DDOS attack can be classified?

2. Attempt **any three** of the following: **15**
   a. Give the difference between Symmetric and asymmetric encryption.
   b. Give the general structure of DES algorithm. Explain the various mode of operation.
   c. Explain the RSA cryptosystem.
   d. Explain Vigenere Cipher. Encrypt the following text using vigenere cipher with keyword MUMBAI
      "TOMORROW IS A NEW DAY"
   e. Define entropy. Explain the properties of entropy.
   f. What is cryptanalysis? Explain the cryptanalysis of DES

3. Attempt **any three** of the following: **15**
   a. Explain the MD4 algorithm for message digest generation.
   b. Explain the digital signature standard.
   c. Explain the Diffie-Hellman key exchange algorithm
   d. What are the different cryptographic hash function criteria?
   e. What is key predistribution? Explain the concept.
   f. Write a note on Fail-stop signatures.

[TURN OVER]

4. Attempt **any three** of the following: **15**
   a. Describe the various security services.
   b. What is the various security attacks identified under the OSI security architecture? Explain.
   c. Explain the security mechanism defined by X.800.
   d. What is nonrepundiation? Explain with the help of an example.
   e. Explain the model for Network Security.
   f. Explain the challenges involved in establishing computer security.

5. Attempt **any three** of the following: **15**
   a. How is the certificate processing carried out by S/MIME?
   b. What is PGP protocol used for? Explain its features.
   c. When is the user certificate revoked in X.509? Explain each scenario.
   d. Write a note on Compression in PGP.
   e. What are the three enhanced security services proposed for S/MIME?
   f. Explain the authentication procedures used by X.509.

6. Attempt **any three** of the following: **15**
   a. What is ESP used for? Explain the ESP format in detail.
   b. Explain the basic combination of security association. What is the advantage of combining the security associations?
   c. What is SSL Record protocol? Explain its operations.
   d. State the areas where SET protocol can be used. Summarize the participants in SET system.
   e. Write a note on ISAKMP.
   f. Write a note on TLS.

7. Attempt **any three** of the following: **15**
   a. Explain the various ways in which a password file can be protected.
   b. Explain the architecture of Distributed intrusion detection.
   c. What are malicious programs? Give its classification.
   d. Write a note on Trojan horse.
   e. What are firewalls? What are its characteristics?
   f. What the various firewall configurations possible? Explain any one in detail.
