Total No. of Questions : 12]

SEAT No. : □

P1467

[Total No. of Pages :2

## [4759] - 224

B.E. (Computer Engineering)

INFORMATION SECURITY

(2008 Course) (Elective - IV) (Semester - II)

Time : 3 Hours] ***[Max. Marks : 100***

Instructions to the candidates:

1) ***Answer three questions from Section I and three questions from Section II.***
2) ***Answers to the two sections should be written in separate books.***
3) ***Neat diagrams must be drawn wherever necessary.***
4) ***Assume suitable data, if necessary.***

SECTION - I

Q1) a) What are different attributes of security? Explain each in detail. **[10]**

b) Discuss different standards related to Information security. **[8]**

OR

Q2) a) Explain OSI security architecture in detail. **[10]**

b) What are different issues of IS? Explain each in detail. **[8]**

Q3) a) What is cryptography? Explain polyalphabetic ciphering with suitable example. **[8]**

b) Explain round function of DES algorithm in detail. **[8]**

OR

Q4) a) Enlist block ciphering modes of operation. Explain CBC mode in detail.**[8]**

b) Differentiate AES and DES algorithms. **[8]**

Q5) a) What is RSA? If RSA prime No. p = 3, q = 11, e = 3 and m = 00111011 (m-message), then calculate private key d and cipher text. **[8]**

b) Enlist problem of key managements using private key cryptography. Why Diffie-Hellman algorithm is used in network security. **[8]**

OR

P.T.O.

Q6) a) What are practical issues of RSA algorithm? Discuss each issue in detail. **[8]**

b) Explain Elliptical curve cryptography with suitable algorithmic steps. **[8]**

SECTION - II

Q7) a) What is kerberos? Explain all steps of kerberos with suitable diagram. **[10]**

b) What is X.509? Explain roles of X.509 in detail. **[8]**

OR

Q8) a) What is Message Digest? Explain MDS algorithm in detail. **[10]**

b) Define MAC. Discuss HMAC in detail. **[8]**

Q9) a) Define Ip sec. Discuss Ip sec protocols in detail. **[8]**

b) What is intrusion Detection system? Enlist and explain different types of IDS. **[8]**

OR

Q10) a) Explain steps of SSL Handshaking protocols. **[8]**

b) Enlist and explain firewall design principles in short. **[8]**

Q11) a) What is PGP? Explain operations of PGP. **[8]**

b) Explain working principles of SET with suitable diagram. **[8]**

OR

Q12) Write a short note on followings. **[16]**

a) Security services

b) Smart cards

c) S/MIME

d) Electronic commerce security.

☼ ☼ ☼