

Total No. of Questions : 12]

SEAT No. :

P3181

[Total No. of Pages :2

[4859]-222

B.E.(Computer Engineering)
INFORMATION SECURITY (IS)
(2008 Pattern) (Elective-IV)

*Time : 3 Hours]**[Maximum Marks : 100**Instructions to the candidates:*

- 1) *Answer three questions from section-I and three questions from section-II*
- 2) *Answer to the two sections should be written in separate answer books.*
- 3) *Neat diagrams must be drawn wherever necessary.*
- 4) *Figures to the right side indicate full marks.*
- 5) *Assume suitable data if necessary.*

SECTION - I

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

b) Explain lifecycle of information security with diagram. [8]

OR

Q2) a) Explain security architecture in detail with suitable diagram. [10]

b) What is mechanism in security? Discuss any one mechanism in detail.[8]

Q3) a) What secret key and cryptography? Discuss both with suitable example. [8]

b) Explain Triple DES algorithm with advantages over DES algorithm. [8]

OR

Q4) a) Explain RC4 algorithm in detail [8]

b) What is ciphering? Explain any two ciphering technique with suitable example. [8]

Q5) a) Differentiate public key and private key cryptography with suitable example. [8]

b) What key management in security? Explain any one algorithm for key management. [8]

OR

P.T.O.

- Q6)** a) Encrypt message using ECC algorithm. Take any message as a sample. [8]
 b) What is man-in-middle attack? Discuss with suitable example. [8]

SECTION - II

- Q7)** a) What is Kerberos? Explain working principles of it in detail. [10]
 b) Discuss PKI in detail. [8]

OR

- Q8)** a) What is MD5? Explain MD5 in detail with its applications. [10]
 b) What hash function? Differentiate hash function and MAC with formulae. [8]

- Q9)** a) Explain design principle of Firewall. [8]
 b) Differentiate TLS and SSL. [8]

OR

- Q10)** a) Discuss working principles of Intrusion Prevention System. [8]
 b) Differentiate IDS and Intrusion Prevention System. [8]

- Q11)** a) What Electronic commerce security? Explain SET in short. [8]
 b) What is PGP? Describe it in detail. [8]

OR

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

- a) PGP
- b) Smart Cards
- c) PEM
- d) S/MIME

