Total No. of Questions : 12]

SEAT No. :

P2809

[Total No. of Pages : 2

[5154]-190-A
B.E. (Computer)
INFORMATION SECURITY
(2008 Course) (Semester -II) (410451 D)

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 SEPRATE answer books.***
3) ***Neat diagrams must be drawn wherever necessary.***
4) ***Figures to the right indicate full marks.***

SECTION -I

Q1) a) Enlist and explain different types of cryptographies in detail. **[10]**

b) Describe different standard or information security in detail. **[8]**

OR

Q2) a) What is transposition scheme of cryptography & Explain any one method of it with suitable example. **[10]**

b) Apply any one algorithm to secure your confidential document. **[8]**

Q3) a) Describe DES algorithm with example. **[8]**

b) What is ciphering? Explain any one with suitable example. **[8]**

OR

Q4) a) Write and explain RC5 algorithm in detail. **[8]**

b) Enlist and explain any one cipher mode of operation. **[8]**

Q5) a) What is ECC? Explain with suitable example to encrypt a message. **[8]**

b) What is RSA? Discuss it in short. **[8]**

OR

Q6) a) Explain number theory with its applications. **[8]**

b) Write and explain DH algorithm in detail. **[8]**

P.T.O.

SECTION -II

Q7) a) What is MAc? Explain it's principles of working. **[10]**

b) What is PKI? Discuss it with suitable example. **[8]**

OR

Q8) a) Discuss applications of DSA in detail with suitable example. **[10]**

b) What is HMAC? Differentiate HMAC & MAC. **[8]**

Q9) a) What is SSL? Explain SSL in detail. **[8]**

b) What is intrusion presentation system? Differential IDS and IPS. **[8]**

OR

Q10) a) Discuss different modules of IDS. **[8]**

b) Explain firewall's. Design principles. **[8]**

Q11)a) Explain format of S/MIME in detail. **[8]**

b) What is PEM? Discuss it in detail. **[8]**

OR

Q12)Write a short note on following: **[16]**

a) X. 50g

b) Electronic Commerce Security

c) Security Mechanisms.

d) PGP.

⊗⊗⊗