Total No. of Questions : 12]

SEAT No. :

P2810

[Total No. of Pages : 2

[5154]-191

B.E. (Information Technology)

INFORMATION ASSURANCE & SECURITY

(2008 Pattern) (Semester-I)

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

Instructions to the candidates:

1) ***Answer of question1 or 2, 3 or 4,and 5 or 6 from section-I and question 7or 8,9 or 10 and 11 or12 from section-II.***
2) ***Answers 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) ***Use of Calculator is allowed.***
6) ***Assume Suitable data if necessary.***

SECTION-I

Q1) a) What is attack? Explain different types of attacks? **[10]**

b) Illustrate how to share and split the secret and its significance in some application. **[8]**

OR

Q2) a) What is Chinese remainder theorem? Explain with examples. **[10]**

b) What are security goals? Explain various types of Authentication **[8]**

Q3) Describe the different modes of operation (ECB, CBC, CFB, OFB & CTR mode) with the help of block diagram. **[16]**

OR

Q4) a) Write working of AES algorithm in detail. **[8]**

b) Describe the advantages and disadvantages of symmetric and asymmetric key cryptography. **[8]**

Q5) a) List and state the channels of key distribution in symmetric and asymmetric key systems. **[8]**

b) Illustrate the Diffiee Hellman Key exchange protocol. **[8]**

OR

Q6) a) What is PKI? Explain the different PKI architectures. **[8]**

b) What problem was Kerberos designed to address. Describe Kerberos realm. **[8]**

P.T.O.

SECTION-II

Q7) a) What is IPSEC? How does AH and ESP differ while working under Tunnel mode and Transport mode. **[10]**

b) What do you mean by internet key exchange protocol? Explain its different phases? **[8]**

OR

Q8) a) What is SSL? Explain the SSL architecture in detail? **[10]**

b) Explain different IDS methods with one example each. **[8]**

Q9) a) Write a short note on smart card and chip card transaction. **[8]**

b) Explain domains of ISO 27001 security standard and state its purpose. **[8]**

OR

Q10) a) Explain and draw model for ISMS(Information Security Management system) of PDCA Cycle (Plan, Do, Check, Act phase). **[8]**

b) Illustrate idea of Electronic Cash. **[8]**

Q11) Write a short note on following (any four) **[16]**

Q a) Electronic evidence.

b) Internet fraud

c) Identity theft

d) Computer Forensic

e) Cyber tourism

OR

Q12) a) Illustrate Industrial Espionage in IT industry. **[8]**

b) List some of the cyber crime and respective penalties. **[8]**