Total No. of Questions : 12]

SEAT No. :

P1780

[Total No. of Pages :3

[4859]-181

B.E. (Information Technology)

INFORMATION ASSURANCE & SECURITY

(2008 Pattern) (Semester-I)

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

Instructions to the candidates:

1) ***Answer of question 1 or 2,3 or 4, and 5 or 6 from section-I and question 7 or 8, 9 or 10 and 11 or 12 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) Enlist security goals and mechanism in detail. **[10]**

b) Differentiate between following: **[8]**

i) Active and passive attacks

ii) Authentication and Authorization

OR

Q2) a) Write the Extended Euclidean algorithm to compute the inverse. (Illustrate with proper variables and comments). **[10]**

b) Illustrate the use of polynomials for secret sharing. **[8]**

Q3) a) Draw block diagram of AES and state the general steps in process. **[8]**

b) Calculate cipher text using RSA algorithm.Given data as follows: Prime numbers P,Q as 7,17 respectively and plain text is to be send is 10. **[8]**

OR

P.T.O.

Q4) a) Describe different modes of operation (ECB, CBC, CFB, OFB,CTR mode) with the help of block diagram. **[10]**

b) Explain working of MD5 in detail. **[6]**

Q5) a) Explain role of key distribution center in symmetric system. **[8]**

b) Illustrate Diffie-Hellman key exchange algorithm with diagram. **[8]**

OR

Q6) a) Explain public key infrastructure X.509 with the help of architectural block diagram. **[8]**

b) Draw sequence diagram of Needham Schroeder protocol and explain. **[8]**

SECTION - II

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

b) State and explain various categories of intrusion detection system. **[8]**

OR

Q8) a) What are different requirements of Kerberos? Explain the architecture of Kerberos. What do you mean by Kerberos Realms? **[10]**

b) Explain SSL architecture in detail. **[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]**

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) Write short note on Indian IT laws 2000, 2008 amendments. **[8]**