

Total No. of Questions : 12]

SEAT No. :

P792

[Total No. of Pages : 2

[4659]-204

B.E. (Information Technology) (Semester - I)
INFORMATION ASSURANCE AND SECURITY
(2008 Pattern)

Time : 3 Hours]

[Max. Marks : 100

Instructions to the candidates :

- 1) *Answer Question 1 or 2, 3 or 4, 5 or 6 from Section I and Question 7 or 8, 9 or 10, 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 indicate full marks.*
- 5) *Assume suitable data, if necessary.*

SECTION - I

- Q1)** a) State the Chinese Remainder Theorem with example. [8]
b) What is mean by Modular arithmetic & Exponentiation? [8]

OR

- Q2)** a) Explain the seven principles of security. [8]
b) How AES encryption does not solve an integrity problem? What is the solution? [8]

- Q3)** a) Describe the modes of operation (ECB, CBC, CFB, OFB) with the help of block diagram. [8]
b) Draw block diagram of SHA-1 and state the general step in the process. [8]

OR

- Q4)** a) Discuss and compare Linear Cryptanalysis and Differential Cryptanalysis. [8]
b) Describe the advantages and disadvantages of symmetric and asymmetric key cryptography. [8]

- Q5)** a) Discuss key management with respect to the following issues : [12]
i) Key generation.
ii) Key distribution.
iii) Key updation.
b) What is PKI? Explain the different PKI Architecture. [6]

OR

P.T.O.

- Q6)** a) Draw sequence diagram of Neeham Schroeder protocol and explain. [9]
b) How the Digital Certificate creation takes place? Enlist the contents of digital certificate. [9]

SECTION - II

- Q7)** a) What is IPSEC? How does AH and ESP differs while working under Tunnel mode and Transport mode? [12]
b) Explain Internet Key Exchange protocol? [6]

OR

- Q8)** a) Illustrate application programming level security solution for Peer to Peer chat application which should support authentication, integrity and secrecy. [12]
b) State various categories of Intrusion Detection System. [6]

- Q9)** a) Explain any four domains of ISO 27001 standard. [8]
b) Describe the types of Smart Cards? Explain the advantages and disadvantages of Smart Card. [8]

OR

- Q10)** a) Explain Electronic payment system. List the characteristics of e-payments. Explain list of requirements to evaluate e-payments system. [8]
b) Explain and draw a model for ISMS (Information security management system) of PDCA cycle (Plan, DO, Check, Act Phase). [8]

- Q11)** Write short notes on (Any Three) : [16]
a) Industrial Espionage.
b) Security by obscurity.
c) Internet Fraud.
d) Electronic Evidence.

OR

- Q12)** Write short notes on (Any Three) : [16]
a) Indian IT Act.
b) Cyber Terrorism.
c) Identify Theft.
d) Computer Forensics.

