Total No. of Questions : 12]

SEAT No. :

P3407

[Total No. of Pages : 3

[4959]-181

B.E. (Information Technology)

INFORMATION ASSURANCE AND SECURITY

(2008 Course) (Semester - I) (414441)

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

Instructions to the candidates:

1) ***Answer 3 questions from Section - I and 3 questions 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) Explain the following threats: **[8]**

i) Modification or alteration.

ii) Masquerading.

iii) Repudiation of origin.

iv) Denial of service (DOS).

b) State & Prove Fermat's Theorem. **[8]**

OR

Q2) a) Explain the following terms with example. **[8]**

i) Confusion & Diffusion.

ii) Secret Splitting & Secret Sharing.

b) Explain Cipher Techniques: Substitution & Transposition with example. **[8]**

P.T.O.

Q3) a) In a public key cryptosystem using RSA, given N = 209 and the encryption key (E) as 23, Find out the corresponding private key (D). **[6]**

b) Explain Data Encryption Standard (DES) symmetric cryptographic algorithm along with different modes of operations. **[10]**

OR

Q4) a) What are the key requirements of message digest & why SHA is more secure than MD5. **[8]**

b) Draw AES block diagram and explain the steps in detail. **[8]**

Q5) a) What is man in the middle attack? Explain with example the Diffie-Hellman Key exchange algorithm. **[9]**

b) Explain the key distribution scenario using private key algorithm. **[9]**

OR

Q6) a) Explain X.509 standard for digital certificate. **[9]**

b) What is digital signature. Explain the steps to create a digital signature using Digital Signature Algorithm (DSA). **[9]**

SECTION - II

Q7) a) List the benefits of IPSec. Distinguish between tunnel and transport mode in IPSec. Describe briefly how IPSec works. **[8]**

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

OR

Q8) a) Discuss SSL with respect to 4 phases. **[8]**

i) Establish security capabilities.

ii) Server authentication and key exchange.

iii) Client authentication and key exchange.

iv) Finish.

b) State various categories of Intrusion Detection System. **[8]**

Q9) a) Which are the key participants in SET? How does SET protect payment information from the merchant? Explain the SET model. **[8]**

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

OR

Q10)a) What is dual signature? Why dual signatures are needed? Explain mathematically and by schematic diagram how it is generated. **[8]**

b) Explain electronic payment system. List the characteristics of e-payments. Explain list of requirements to evaluate e-payments system. **[8]**

Q11)Write short notes on: **[18]**

a) Computer Forensics.

b) Cyber Terrorism.

c) Online investigative Tools.

OR

Q12)a) Describe the term "Industrial Espionage" in detail with example. **[9]**

b) Write short note on Indian IT Law 2000, 2008 amendments. **[9]**