Total No. of Questions : 12]

SEAT No. :

P2046

[Total No. of Pages : 3

B.E. (I.T.) (Semester - I)

INFORMATION ASSURANCE & SECURITY

(2008 Pattern)

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

Instructions to the candidates:

1) ***Answers to the two sections should be written in separate answer books.***
2) ***Neat diagrams must be drawn wherever necessary.***
3) ***Figures to the right side indicate full marks.***
4) ***Use of calculator is allowed.***
5) ***Assume suitable data if necessary.***

SECTION - I

Q1) a) Differentiate: **[8]**

i) Active and Passive attacks.

ii) Authentication and Authorization.

b) State the Chinese remainder theorem with example. **[8]**

OR

Q2) a) Differentiate: **[8]**

i) Confusion & Diffusion.

ii) Secret Splitting & Secret Sharing.

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

Q3) a) In a public key cryptosystem using RSA you intercept the cipher text C = 284 sent to user whose public key is e = 223 and n = 713. What is the plain text M? **[9]**

b) Explain Data Encryption Standard (DES) symmetric cryptographic algorithm along with different modes of operations. **[9]**

OR

P.T.O.

Q4) a) What are the key requirements of message digest & why SHA is more secure than MD5. **[9]**

b) Draw AES block diagram and explain the steps in detail. **[9]**

Q5) a) What is man in the middle attack? Explain with example the Diffie - Hellman Key exchange algorithm. **[8]**

b) Explain the key distribution scenario using private key algorithm. **[8]**

OR

Q6) a) Explain X.509 standard for digital certificate. **[8]**

b) What is digital signature? Explain the steps to create a digital signature. **[8]**

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) Explain the concept of mobile payment system. **[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) Identity Theft.

b) Security by Obscurity.

c) Computer Forensics.

OR

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

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