Total No. of Questions : 12]

SEAT No. :

P2010

[Total No. of Pages : 3

[5254]-181

B.E. (Information Technology)

INFORMATION ASSURANCE & SECURITY

(2008 Pattern)

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

Instructions to the candidates:

1) ***Answers 3 questions from Section - I and 3 questions from Section - II.***
2) ***Answer to the two section should be written in separate answer books.***
3) ***Neat diagrams must be drawn wherever necessary.***
4) ***Figures to right indicate full marks.***
5) ***Assume Suitable data, if necessary.***

SECTION - I

Q1) a) Explain the following terms with example. **[8]**

i) Authentication and Authorization

ii) Confusion & Diffusion

b) What is mean by modular arithmetic and exponentiation? **[8]**

OR

Q2) a) State & prove Fermat's theorem. **[8]**

b) List and briefly define types of cryptanalytic attacks based on what is known to attacker? **[8]**

Q3) a) What are the key requirements of message digest and why SHA is more secure than MDS? **[8]**

b) Describe the advantages and dis-advantages of symmetric and asymmetric key photography. **[8]**

OR

Q4) a) Draw AES block diagram and explain the steps in detail. **[8]**

b) 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]**

c) What is message disest and give it's importance? **[2]**

P.T.O.

Q5) a) Explain X.509 standard for digital certificate. **[9]**

b) What is PKI? Explain the different PKI architectures. **[9]**

OR

Q6) a) What is key distribution center? What is certificate authority. Give any two names of CAS. **[9]**

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

SECTION - II

Q7) a) What problem was Kerberos designed to address? Describe Kerberos Realm. **[8]**

b) What is IPSEC? How does AH & ESP differs while working under tunnel mode & transport mode? **[8]**

OR

Q8) a) What is IDS? Explain working of honey pots an intrusion detection system. **[8]**

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

i) Establish Security Capabilities.

ii) Server authentication & key exchange.

iii) Client authentication & key exchange.

iv) Finish

Q9) a) Explain ISO 27001 security standard & state its purpose. **[8]**

b) What is dual signature? Why dual signatures are needed? Explain mathematically & by schematic diagram how it is generated? **[8]**

OR

Q10) a) Explain & draw a model for ISMS (Information Security Management System) of PDCA Cycle (Plan, Do, Check, Act Phase) **[8]**

b) Explain the concept of mobile payment system. **[8]**

Q11) Write a short notes on: (any three) **[18]**

a) Electronic evidence

b) Computer forensics

c) Cyber terrorism

d) Identity theft

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]**

⊖ ⊖ ⊖