Total No. of Questions : 8]

SEAT No. :

P4520

[Total No. of Pages : 2

[4860] - 335

M.E. (Computer) (Computer Engineering)

INFORMATION AND NETWORK SECURITY

(2008 Course) (510105) (Elective-II) (Semester-I)

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

Instructions to the candidates:

1) ***Answer any THREE questions from each section.***
2) ***Answer to the two sections should be written in separate books.***
3) ***Neat diagrams must be drawn wherever necessary.***
4) ***Figures to the right side indicate full marks.***
5) ***Use of logarithmic tables, slide rule, mollier charts, electronic pocket calculator and steam table is allowed.***
6) ***Assume Suitable data if necessary.***

SECTION-I

Q1) a) Enlist and explain steps necessary for creating information security policy. **[7]**

b) Explain different threat scenarios with suitable examples. **[7]**

c) What is service interruption-based attack? Explain with suitable example. **[4]**

Q2) a) What requirements must a public key cryptosystems fulfil to be a secure algorithm. **[8]**

b) Explain Data Encryption Standard (DES) encryption structure, structure of encryption round and DES function. **[8]**

Q3) a) What are the basic protections provided by secure socket layer? How can it found whether the user has entered into a secure site? **[8]**

b) What is meant by bastion host? Describe the screened-subnet firewall system with a Demilitarized Zone (DMZ). **[8]**

P.T.O.

Q4) Write Short Notes on (Any Three). **[16]**

a) ARP hazard.

b) Issues in multi-level secure systems.

c) Privacy and data protection.

d) Physical and logical access control.

SECTION-II

Q5) a) What is discrete logarithm problem? Explain different approaches for solving discrete logarithm problem. **[10]**

b) Explain what is Blind-key cryptosystem with suitable example. **[8]**

Q6) a) Explain different type of attacks, that are possible on packet-filtering firewalls? **[8]**

b) Explain how firewall differs from intrusion detection system? List the issues to be addressed when installing firewall. **[8]**

Q7) a) Explain how wireless security is different from wired data security, and how WEP addresses security in wireless LANs. **[8]**

b) Explain security of the Diffie-Hellman algorithm. Discuss advantages and limitations of the Diffie-Hellman algorithm. **[8]**

Q8) Write Short Notes on (Any Three) **[16]**

a) Source masking and hidden channels.

b) One time password.

c) Secure RSVP.

d) Time stamping and reliable ordering of events.

ζ ζ ζ