Total No. of Questions : 12] [Total No. of Pages : 3

P1499

[3764]-431

B.E. (Information Technology)

INFORMATION SYSTEM SECURITY

(414441) (2003 Course)

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) ***Your answers will be valued as a whole.***
6) ***Use of logarithmic tables slide rule, Mollier charts, electronic pocket calculator and steam tables is allowed.***
7) ***Assume suitable data, if necessary.***

SECTION - I

Q1) a) Explain in brief: **[10]**

i) Interception

ii) Fabrication

iii) Modification

iv) Interruption.

b) What are the two basic ways of transforming plaintext into ciphertext. Explain with example. **[8]**

OR

Q2) a) Compare and contrast, with suitable example Active and Passive attacks. **[10]**

b) Discuss the concept of Caesar cipher. How is monoalphoetic cipher different from Caesar cipher. **[8]**

Q3) a) Explain in detail Clark-Wilson model. **[8]**

b) Discuss the role of trust in security policy. **[4]**

c) Discuss availability issues in security policies. **[4]**

OR

P.T.O.

Q4) a) Explain in detail Biba Integrity model. [8]

b) Explain [8]

i) Mandatory

ii) Discretionary

iii) Role based access controls.

Q5) a) Distinguish between differential and linear cryptanalysis. [8]

b) Explain any one symmetric key algorithm in detail with an example. [8]

OR

Q6) a) Distinguish between stream and block ciphers. [5]

b) Discuss idea behind algorithm modes. [5]

c) Explain vulnerabilities of DES. [6]

SECTION - II

Q7) a) What is the difference between MAC and message digest. [8]

b) With a neat example explain RSA. [8]

OR

Q8) a) Describe the advantages and disadvantages of symmetric and asymmetric key cryptography. [8]

b) With a neat example explain Diffie-Hellman algorithm. [8]

Q9) a) What is the role of a CA and RA in the creation of digital certificate. [8]

b) With a neat diagram explain Kerberos realm. [8]

OR

*Q10)*a) Compare and contrast Tunnel and Transport mode of IPsec. [8]

b) Explain digital signature algorithm. [8]

*Q11)*a) Explain SSL with respect to: [8]

i) Its position in the TCP/IP stack.

ii) Services it provides.

iii) What protocols it is comprised of.

b) Discuss firewall design principles. Explain what firewall can do and what firewall cannot. [10]

OR

*Q12)*a) Explain Intrusion detection system. [10]

b) Write notes on <u>any two</u>: [8]

i) Traffic Confidentiality.

ii) Blowfish

iii) Cookies

iv) PGP.

□□□□