Total No. of Questions : 12]

[Total No. of Pages : 3

P1289

[3864]-409

B.E.

NETWORK AND INFORMATION SECURITY

Time : 3 Hours]

[Max. Marks : 100

Instructions to the candidates:

1) *Attempt any three questions from Section - I and three questions from Section - II.*
2) *Figures to the right indicate full marks.*
3) *Draw neat diagrams wherever necessary.*
4) *Make suitable assumptions wherever necessary.*

SECTION - I

Q1) a) Explain the basic security concepts. How the individual components of the system are identified for analysis. [8]

b) Explain the ISO Security Architecture. [8]

OR

Q2) a) What are typical phases of operation of viruses or worms? How do the worms propagate? [8]

b) Explain Man-in-Middle attacks and Reply attacks with suitable example. What are different security measures to control these attacks? [8]

Q3) a) Enlist and explain the principles of Public Key Cryptosystem. [8]

b) Enlist and explain three threats associated with user authentication over a network or internet. [8]

OR

Q4) a) Explain basic arithmetic and logical functions used in MD5 and SHA-1 operation. [8]

b) Enlist HMAC design objectives and explain HMAC algorithm with structure. [8]

Q5) a) What is triple encryption? Explain meet-in-middle attack in DES with suitable example. [9]

b) Explain different type of attacks addressed by message authentication.[9]

OR

Q6) Write short notes on : [18]

a) Digital Signatures.

b) Kerberos.

c) Trusted systems.

d) Elliptical curve cryptography.

SECTION - II

Q7) a) What is the purpose of the X.509 standard? How is an X.509 certificate revoked? [8]

b) What are key components of VPN? Discuss various security issues concern to VPN. [8]

OR

Q8) a) What services are provided by IPSec? Explain various application of IPSec with examples. [8]

b) What are key components of VPN? Discuss various security issues concern to VPN. [8]

Q9) a) What protocols comprise SSL? What is the difference between SSL connection and SSL sessions? [8]

b) What are different types of Intruders in the system? Explain with examples. [8]

OR

*Q10)*a) List and define the principle categories of SET participants. **[8]**

b) List and explain the techniques used to avoid guessable password. **[8]**

*Q11)*a) What is OS hardening? Explain the concepts of Honey pot with suitable illustration. **[10]**

b) Explain the difference between Packet filtering router and Stateful inspection firewall. **[8]**

OR

*Q12)*Write short notes on any three : **[18]**

a) Email Security.

b) Smart Card Security.

c) WiFi and WiMax Security.

d) Advanced Encryption Standard.

❖ ❖ ❖ ❖