P1446   **[3764]-419**

B.E. (Computer Engg.)
NETWORK AND INFORMATION SECURITY
(2003 Course)

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

Instructions to the candidate:

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 must be drawn wherever necessary.*
4) *Make suitable assumptions wherever necessary.*

SECTION - I

Q1) a) What do you mean by packet sniffing and snooping? What are the different means to carry out these attacks?   **[8]**

b) What are different security threats? Explain various types of passive and active security attack.   **[8]**

OR

Q2) a) What do you mean by Code Injection? Differentiate between worms, viruses and Trojan Horses.   **[8]**

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

Q3) a) "Public key cryptography complements private key cryptography rather than replaces it". Justify with example.   **[6]**

b) What are different requirements of kerberos? Explain the architecture of kerberos. What do you mean by kerberos Realms?   **[10]**

OR

Q4) a) Differentiate between MD5 and SHA-1 hash algorithms.   **[6]**

b) Explain X.509 Authentication service in details.   **[10]**

Q5) a) What are different variations of DES algorithm and how it works?**[8]**

b) What is elliptical curve cryptography (ECC)? What are various implementation choices for ECC?   **[10]**

OR

Q6) Write short notes on (any Three): [18]

    a)   Security services and mechanisms.

    b)   Firewall and packet filters.

    c)   Advanced Encryption standard.

    d)   Electronic mail security.

SECTION - II

Q7) a)   What are key components of virtual private Networks? Why VPN users require strong authentication? [8]

    b)   What is tunneling? What are different tunneling protocols used in VPN? [8]

OR

Q8) a)   Explain various services, benefits and applications of IPSec protocol. Elaborate the concept of Security Association. [8]

    b)   List and explain Encryption and Authentication algorithms used in AH and ESP. [8]

Q9) a)   Explain the architecture of SSL. Differentiate between SSL and TLS. [10]

    b)   Explain the security facilities in the TCP/IP Protocol stack. [6]

OR

Q10) a)   Enlist and explain different components of Secure Electronic Transaction (SET). [8]

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

Q11) a)   Explain various security measures in VLAN and wireless LAN. [8]

    b)   What is OS hardening? Explain the concept of Honeypot with suitable diagram. [10]

OR

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

    a)   Router Security.

    b)   Smart Card Security.

    c)   Wifi and کا Max Security issues.

    d)   Internet standards and the Internet Society.

□□□□