Code No.: CY514PE/IT511PE   R20   H.T.No. [ ][ ][8][R][ ][ ][ ][ ]

[Time: 3 Hours]   [Max. Marks: 70]

Note: This question paper contains two parts A and B.
    Part A is compulsory which carries 20 marks. Answer all questions in Part A.
    Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks.

PART-A   (20 Marks)

1. a) What are the security mechanisms?   [2M]
   b) Discuss about the Masquerade in brief.   [2M]
   c) Use Caesar cipher algorithm to encrypt the message "Hello" where key=15. [2M]
   d) Write about cipher block chaining mode of operation.   [2M]
   e) What problem was Kerberos designed to address? Explain.   [2M]
   f) What are the properties of hashing functions?   [2M]
   g) What are the functions of HTTP protocol?   [2M]
   h) What are the benefits of Digital Signature?   [2M]
   i) What is transport mode and tunnel mode in IP sec?   [2M]
   j) Give a brief note on Virtual Elections.   [2M]

PART-B   (50 Marks)

2. a) Determine the security services involved in various types of Active and Passive attacks.   [5M]
   b) Describe the model for network security with neat sketch.   [5M]

OR

3. a) What is symmetric key cryptography? Discuss its advantages and limitations.   [5M]
   b) Explain various substitution techniques with suitable examples.   [5M]

4. a) Summarize the public key cryptographic principles. Explain RSA algorithm for given example Where p = 3 and q = 11.   [5M]
   b) Enumerate Diffie-Hellman Key exchange for encryption and decryption with suitable Examples.   [5M]

OR

5. a) Explain DES algorithm with suitable examples. Discuss its advantages and limitations.   [5M]
   b) What is Elliptic Curve Cryptography (ECC)? Discuss ECC algorithm with neat diagram.   [5M]

6. List the main features of SHA-512 cryptographic hash function. What kind of compression function is used in SHA-512?   [10M]

OR

7. a) What is HMAC function? Summarize the design objectives of HMAC.   [5M]
   b) Explain about Elgamal Digital Signature Scheme.   [5M]

8. a) What is SSL? Explain about SSL record protocol format.   [5M]
   b) Enumerate the functionalities of Secure Shell.   [5M]

OR

9. Explain about the IEEE 802.11i Wireless LAN Security.   [10M]

10.a) Write a short note on Pretty Good Privacy. [5M]
   b) Describe IP Security architecture with neat diagram. [5M]

OR

11.a) Write a short note on S/MIME. [5M]
   b) Discuss encapsulating security payload in detail. [5M]

****