[5870]-1076
T.E. (E&TC)
NETWORK SECURITY
(2019 Pattern) (Semester - II) (304195(E)) (Elective - II)

Time : 2½ Hours]   *[Max. Marks : 70*

Instructions to the candidates:
  1) *Answer Q.1 or Q.2, Q.3 or Q.4, Q.5 or Q.6, Q.7 or Q.8.*
  2) *Neat diagrams must be drawn whenever necessary.*
  3) *Figures to the right indicate full marks.*
  4) *Assume suitable data, if necessary.*

Q1) a) Compare symmetric key encryption and Asymmetric key encryption.**[6]**

   b) Explain Diffie-Helman key exchange algorithm with example.   **[6]**

   c) What is Block cipher? Discuss Block cipher modes of operation.   **[6]**

OR

Q2) a) Discuss RC4 Stream Cipher with an example.   **[6]**

   b) Draw and Explain Feistal Cipher structure in detail.   **[6]**

   c) Using RSA algorithm encrypt plain text "03", with $p = 11$, $q = 3$, & $e = 13$.
                                                                          [6]

Q3) a) Explain Knapsack algorithm.   **[6]**

   b) Write a note on Digital Signature algorithm.   **[6]**

   c) What is authentication? Explain various methods of authentication. **[5]**

OR

Q4) a) Discuss x. 509 authentication service.   **[6]**

   b) Elaborate the characteristics needed in secure Hash function.   **[6]**

   c) What is message digest? Compare MAC with SHA1   **[5]**

Q5) a) Explain in detail, working of PGP algorithm. **[6]**

b) Describe IPsec security services. **[6]**

c) What is security association and what are the fields of SAD. Discuss in brief. **[6]**

OR

Q6) a) What is S/MIME? State its operation in detail. **[6]**

b) Discuss Authenticati Header and Encapsulation in email security. **[6]**

c) Draw the IPsec security architecture and explain in detail. **[6]**

Q7) a) What are the types of firewall? Explain any two in detail. **[6]**

b) Discuss nature of viruses and the types of viruses. **[6]**

c) List and briefly define three classes of intruders. **[5]**

OR

Q8) a) Explain SSL protocol in detail. **[6]**

b) Write a note on secure Electronic Transaction. **[6]**

c) Enlist four techniques used by firewalls to control access and enforce a security policy. **[5]**

❄ ❄ ❄