

[3 Hours ]

Total Marks:80 ]

- N.B. (1) Question No. 1 is compulsory  
(2) Attempt any three questions out of the remaining five questions  
(3) Figures to the right indicate full marks  
(4) Assume suitable data whenever required and justify them

1. a) Explain substitution technique and transposition technique in detail. 10  
b) Explain security attacks, services and mechanisms. 10
  2. a) Explain DES algorithm. What is the strength of DES? 10  
b) Explain ECB and CBC in detail. 10
  3. a) What is Chinese remainder theorem explain with example. 10  
b) Write short note on public key cryptography. 10
  4. a) Explain Secure hash algorithm. 10  
b) What is Firewall? Explain different type of firewall. 10
  5. a) Explain Kerberos authentication protocol 10  
b) Explain RSA algorithm with example. 10
  6. Write short note on following: 20
    - a) Digital signature.
    - b) Zero knowledge authentications.
    - c) Hash function.
    - d) Intrusion detection system.
-