

Time: 3 Hrs

Max. Marks: 80

Instructions to the candidates, if any:-

N.B. : (1) Question No. 1 is compulsory.

(2) Attempt any three questions out of remaining five questions.

- Q1 a) Explain the relationship between security services and Mechanisms. (05)
b) Explain the significance of an intrusion detection system for securing a network (05)
c) What is X.509 certificate? Describe the steps involved in its generations (05)
d) List and explain various types of attacks on encrypted message. (05)
- Q2 a) Explain Block cipher modes of operation. (10)
b) Explain Digital Signature Scheme with RSA. (10)
- Q3 a) How is security achieved in the transport and tunnel modes of ipsec? Describe the role of AH and ESP. (10)
b) What is DDOS attack? Explain how is it launched. (10)
- Q4 a) With a block diagram describe SHA512. (10)
b) With a neat diagram explain SSL Handshake Protocol. (10)
- Q5 a) Explain firewall and its types along with its advantages and disadvantages. (10)
b) Explain Kerberos. Why is it called as SSO? (10)
- Q6 Answer the following (20)
a) Compare symmetric and asymmetric encryption.
b) Write in brief about denial of service attacks.
c) Use Cases for NAC
d) Explain Principle element of NAC
