

Time (3 Hours)

[Total Marks 80]

N. B:

1. Question No. 1 is Compulsory.
2. Solve any THREE from Question No. 2 to 6.
3. Draw neat well labelled diagram wherever necessary

- Q. 1 a) A secure e-voting system is to be designed. Discuss the security goals that must met and enlist mechanisms for the same. (5)
- b) Explain principle elements of NAC (5)
- c) Enlist properties & applications of Hash function. (5)
- d) Describe different types of Denial of service attacks. (5)
- Q2. a) Explain the need of Network Access Control in Enterprise Networks. Explain the major NAC enforcement methods. (10)
- b) Explain in detail with diagram, How Kerberos can be used for authentication. (10)
- Q3. a) How is security achieved in the transport and tunnel modes of IPSEC? Describe the role of AH and ESP. (10)
- b) Define Malware. Explain its types in detail (10)
- Q4. a) Explain Firewall & its types along with advantages and disadvantages (10)
- b) Explain different modes of operation of Block ciphers (10)
- Q5. a) Explain classical encryption techniques with example (10)
- b) In an RSA system, given $N=91$ $e=5$ Calculate $\Phi(n)$, p , q and private key d . What is the cipher text when you encrypt message $m=25$ using the public key. Also perform decryption. (10)
- Q6. Write Short Notes on ANY 4: (20)
- a) SSL protocol stack
 - b) Compare and contrast AES and DES
 - c) IDS and its types
 - d) Use cases for NAC
 - e) Digital Signature
