

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 labeled diagram wherever necessary.

- Q. 1 a) A secure e-voting system is to be designed. Discuss the security goals that must be met and enlist mechanisms for the same. (5)
- b) What is the drawback of Double DES algorithm? How is it overcome by Triple DES? (5)
- c) Define ARP spoofing with an example. Compare with IP spoofing. (5)
- d) What is the significance of a digital signature on a certificate? Justify (5)
- Q. 2 a) Encrypt "This is the final exam" with Playfair cipher using key "Guidance". Explain the steps involved. (10)
- b) Compare and contrast DES and AES. (10)
- Q. 3 a) Two users wish to establish a secure communication channel and exchange a session key after mutual authentication. Show how this can be done with the help of a KDC. (10)
- b) Given modulus $n=221$ and public key, $e=7$, find the values of p , q , $\phi(n)$, and d using RSA. Encrypt $M=5$. (10)
- Q. 4 a) Define DOS attack. Show the different ways by which this attack can be mounted at various layers. (10)
- b) Show how Kerberos protocol can be used to achieve single sign-on in distributed systems (10)
- Q. 5 a) A user wishes to do online transactions with Amazon.com. Discuss a protocol which can be used to set up a secure communication channel and provide server side and client side authentication. Show the steps involved in the handshake process. (10)
- b) What is a firewall? Explain different types of firewalls and list their advantages. (10)
- Q. 6 a) Write short notes on (any two): i) Email security ii) Diffie Hellman algorithm iii) El-Gamal Algorithm (10)
- Q. 6 b) How does IPSec help to achieve authentication and confidentiality? Justify the need of AH and ESP. (10)
