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) Describe RC5 algorithm with an example. (5)
b) Explain the purpose of keylogger and rootkit. (5)
c) Explain Playfair Cipher with an example. (5)
d) Explain how VPN can be used to encrypt your personal data. (5)

Q2. a) Explain Public Key Cryptography and RSA algorithm. Given modulus n=91 and public key e=5, find the value of p, q, phi(n) and d using RSA. Encrypt M=25. (10)
b) List and explain all types of Malware in detail. Differentiate between Virus and Worms. (10)

Q3. a). Explain Kerberos protocol in detail. Show how a Kerberos protocol can be used to achieve single sign-on in distributed systems. (10)
b) Explain the OSI Security Architecture and Network Security Model. (10)

Q4. a) Explain Email security process. Explain how S/MIME can be used for Digital Signature and verification operations on email messages. (10)
b) Explain the implementation of Network Access Control with one use case. (10)

Q5. a) Explain how Network Management security is implemented using SNMP v3. (10)
b) What is an Intruder Detection System? Explain its types in detail. (10)

Q6. Write Short Notes on ANY 4: (20)
a) Firewall design principles
b) Block Cipher Modes of Operation
c) HMAC and CMAC
d) Steganography and its applications
e) SHA 256 and SHA 512
f) SSL Architecture

****