13/11/2024 IT SEM-V C SCHEME CNS QP CODE: 10064504

(Time: 3 hours) **(Total Marks: 80)**

INSTRUCTIONS
(1) Question 1 is compulsory.
(2) Attempt any three from the remaining questions.
(3) Draw neat diagrams wherever necessary.

Q1

a) Enlist security goals. Discuss their significance **(5)**

b) Compare and contrast DES and AES. **(5)**

c) Explain the purpose of keylogger and rootkit **(5)**

d) SHA provides better security than MD5 Justify **(5)**

Q2

a) Encrypt "This is the final exam" with Play fair cipher,the key is 'Guidance' **(10)**

b) What is the significance of a digital signature on a certificate ?Justify **(10)**

Q3

a) How does IPSec help to achieve authentication and confidentiality?Justify the need of AH and ESP **(10)**

b) What Is PKI. Explain PKI architecture in detail **(10)**

Q4

a) Show how a Kerberos protocol can be used to achieve single sign on in distributed systems **(10)**

b) What is network access control? Discuss the elements present in this context **(10)**

Q5

a) Explain different types of denial of service attacks **(10)**

b) Explain network management security with respect to SNMP protocol **(10)**

Q6

a) Explain different methods of IDS? State capabilities and challenges in IDS **(10)**

b) Explain transposition ciphers with illustrative examples **(10)**

****