T.E. Sem-VI (IKT) (Rev-19) (CMPH) winter 2025. 16/12/2025.

Duration: 3hrs

Max Marks: 80

N.B. : (1) Question No 1 is Compulsory.
(2) Attempt any three questions out of the remaining five.
(3) All questions carry equal marks.
(4) Assume suitable data, if required and state it clearly.

1 Attempt any FOUR [20]

a Give examples of replay attacks. List three general approaches for dealing with replay attacks.

b Compare and contrast keyed and keyless transposition ciphers.

c Write short note on packet sniffing attack.

d Explain transposition cipher with example.

e What are computer viruses and worms? Write any four key differences between them.

2 a Find the shared secret key in a Diffie-Hellman scheme with a common prime 71 and primitive root 7. Given the private keys of Alice and Bob are 5 and 12 respectively. [10]

b Explain AES. Compare and contrast AES vs DES. [10]

3 a What are different types of firewalls? How a firewall is different from an IDS. [10]

b Explain layer wise TCP/IP Vulnerability. [10]

4 a Why are digital certificates and signatures required? What is the role of digital signature in digital certificates? Explain any one digital signature algorithm. [10]

b How does PGP achieve confidentiality and authentication in emails? [10]

5 a Explain how you would use the MD5 hashing algorithm to verify the integrity of the received message. Show all the steps of the algorithm with the help of a diagram. [10]

b Explain Kerberos. Why is it called an SSO? [10]

6 a Enlist the various functions of the different protocols of SSL. Illustrate the connection establishment between client and server in SSL handshake protocol in detail. [10]

b What is Digital Signature? Explain RSA as a Digital Signature Scheme. [10]

****