Sr. No. 602305

December 2023
MCA- III SEMESTER
Network Security (MCA-20-209-2)

Time: 3 Hours   Max. Marks:75

Instructions: 1. It is compulsory to answer all the questions (1.5 marks each) of Part -A in short.
2. Answer any four questions from Part -B in detail.
3. Different sub-parts of a question are to be attempted adjacent to each other.

PART -A

Q1 (a) Differentiate between hash function and hash algorithms.   (1.5)

(b) How many rounds are there in AES?   (1.5)

(c) What are the different types of keys used in cryptography?   (1.5)

(d) What is kerberose 95?   (1.5)

(e) Explain the importance of authentication.   (1.5)

(f) What do we ensure with message non-repudiation?   (1.5)

(g) What is the key size in DES?   (1.5)

(h) Which layer does IPSEC VPN works?   (1.5)

(i) What is public key cryptography?   (1.5)

(j) What is the role of X.509 authentication service?   (1.5)

PART -B

Q2 (a) How does PGP ensure authentication and confidentiality in Emails? Explain (10)
with diagram.
(b) Differentiate between vulnerability, Threats, Attacks, and Control.   (5)

Q3 (a) What is the objective of a flooding attack? Categorize flooding attacks in (8)
MANET and explain them.
(b) What do you mean by MANET? Discuss any 5 major security issues in MANET.   (7)

Q4   What is the key role of IP Security? Explain the modes and security payloads of (15)
IP security.

Q5 (a) Explain Wireless Sensor Networks. Discuss some security aspects in Wireless (8)
sensor networks.
(b) Which security service is ensured with cryptography? How does DES differ   (7)
from AES?

Q6 (a) What do you mean by hash functions? Discuss their properties and   (10)
applications with a suitable diagram.
(b) What are the major points of difference between traditional document   (5)
fingerprint and message digest?

Q7   Write in brief about:
    a) Sinkhole attacks
    b) Sybil attacks
    c) Blackhole attack
    d) Sleep deprivation attack
    e) HELLO flood attacks

****