Ref No: EX/PG/DMC/T/128A/12/2024

M. Tech. Distributed & Mobile Computing Examination, 2024

1st year 2nd Semester

SUBJECT: - Security in Wireless and Mobile Systems

Time: 3 hours Full Marks: 100

Answer any ***five*** from the questions below.

1) a) What is access control in networking? Explain how VPN provide security?
   b) What is firewall? How does it provide security in networking?
   c) What is CIA triad in network security? Explain in details with examples.
   d) Distinguish between worm and Trojan horse. (2+4)+(2+3)+5+4

2) a) Explain one round of DES with detailed diagram.
   b) Explain the manglar function of IDEA. How is it different from DES?
   c) What were the issues of DES? 7+(6+4)+3

3) a) Differentiate MAC and Hash function.
   b) What is a hash in cryptography? What is the role of a compression function in a hash function? What are the applications of cryptographic hash function?
   c) What is the difference between weak and strong collisions resistance?
   d) Explain Diffie Hellman key Exchange in detail with an example. 4+(2+3+3)+3+5

4) a) What is digital signature? What is meet in the middle attack?
   b) What is dual signature? What is its purpose?
   c) What are the merits of Output-Feedback (OFB) as compared to Cipher Feedback (CFB)?
   d) How does NATing helps in security of message? (3+3)+(3+3)+4+4

5) a) What is the difference between SSL and TLS?
   b) How is the communication between the WAP client and WAP server done?
   c) What is Radix 64 format? What is its use in PGP?
   d) What are the security services provided by the IPsec? Explain the function of certificate authority.
   4+4+(3+3)+(3+3)

6) a) What is the use of SSL protocol? Explain SSL record protocol operation with SSL record format.
   b) What is the need for encapsulation of Security Payload? Write and explain different fields of top level format and substructure of ESP packet.
   c) What is are the various requirements of SET? Explain the role of different participants of SET. (3+4)+(3+4)+(3+3)

7) Write short note on: (any four) 5x4
   a) CFB
   b) HMAC
   c) Symmetric key cryptography
   d) RSA
   e) WAP stack structure
   f) PGP