Roll No. .....

Total Pages : 3

# 602305

**December 2022**

**MCA- III SEMESTER**

**Network Security (Paper code: 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

1. (a) Define a distributed denial-of-service attack. (1.5)

   (b) Explain the concept of security association in IP sec protocol. (1.5)

   (c) What types of attacks are addressed by message authentication? (1.5)

   (d) Differentiate between Internal Attack and External attack in MANET (1.5)

(e) What information is used by a typical packet filtering firewall? (1.5)

(f) What do you mean by spoofed, altered or replay routing? (1.5)

(g) What services are provided by SSL record protocol? (1.5)

(h) What are zombies? (1-5)

(i) What is mobile-adhoc network and list any *one* of its applications. (1.5)

(j) Write down the purpose of S-boxes in DES. (1.5)

## PART-B

**2.** (a) What do you mean by asymmetric key cryptography? Discuss any one asymmetric key algorithm. Perform encryption and decryption for RSA algorithm given that p = 3, q = 11, e = 7, plaintext = 5. (10)

(b) What are the security threats and issues in WSN? (5)

**3.** (a) What do you mean by digital certificate? Explain X.509 structure of digital certificate. (5)

(b) Discuss the Kerberos authentication protocol for network security along with its advantages. (10)



**4.** (a) Users A and B use Diffie Hellman key exchange technique with a common prime q = 71 and a primitive root $\alpha$ = 7. If user A has private key $X_A = 5$, what is A's public key $Y_A$? (5)

(b) Differentiate between link-to-link and end-to-end encryption. Consider the following bit pattern for 64 bits key given in hexadecimal for DES algorithm. Convert this key into 56 bits hexadecimal key by performing three left circular shifts.

key : FEDCBA9876543210 (10)

**5.** (a) What are the detection techniques for selective forwarding attack and sinkhole attack? (5)

(b) Explain the need for Gateways and write about Wireless Sensor Network tunneling. (10)

**6.** (a) Discuss how secure E-mails can be sent? Differentiate between PGP and S/MIME protocols. (10)

(b) Differentiate between stream cipher and block cipher. Encrypt the following message using play fair cipher using the key 'scholar' :

"An apple a day keeps doctor away" (5)

**7.** Differentiate between the following :

(a) Black hole attack, Warm hole attack, Grey hole attack.

(b) Internal and External attack in MANET.

(c) Session hijacking and man in the middle attack. (15)

---