Printed Pages:02 **Sub Code:CA 406**

Paper Id: 214212 **Roll No.**

MCA

(SEM-IV) THEORY EXAMINATION 2018-19

NETWORK SECURITY AND CRYPTOGRAPHY

Time: 3 Hours ***Total Marks: 100***

Note: 1. Attempt all Sections. If require any missing data; then choose suitably.

SECTION A

1. Attempt *all* questions in brief. 2 x 10 = 20

a. What do you mean by security mechanism? Give names of some security mechanisms.
b. How Steganography differs from cryptography?
c. What is the role of simplified DES in cryptography?
d. Give some examples of active and passive attack. Which one is more dangerous for our system?
e. What if the problem of birthday paradox?
f. Write the name of some popular algorithm of Hashing.
g. What is fishing?
h. What is man-in-the-middle attack? Is it active or passive attack?
i. Differentiate private and public key cryptography?
j. Name the various Block Cipher Modes of Operation?

SECTION B

2. Attempt any *three* of the following: 10x3=30

a. What is denial of service attack?
b. What is the most securitycritical component of DES round function? Give a brief description of this component.
c. What is the difference between block cipher and stream cipher? Explain any one mode of block cipher operation?
d. Describe the properties of a cryptographic hashing function. Clearly describe how a cryptographic hashing function can be implemented using a block cipher.
e. Describe the different Cipher Block Modes of operations.

SECTION C

3. Attempt any *one* part of the following: 10x1=10

a. What is repudiation? How can it be prevented in real life?
b. Discuss the vulnerabilities of DES.

4. Attempt any *one* part of the following: 10x1=10

a. What is Double DES? What kind of attack on Double DES makes it almost useless?
b. Draw the block diagram depicting the structure of Festal Cipher Structure. List the important features of the structure.

5. Attempt any *one* part of the following: 10x1=10

a. Write RSA algorithm if N = 187 and the encryption key E=17, find out the corresponding private key.
b. What are the security services provided by digital signature?

6. Attempt any *one* part of the following: 10x1=10

a. How the messages are generated and transmitted in pretty good privacy (PGP) protocol? Explain with clear diagrams.
b. Describe the role of Ticket granting server(TGS) in kerberos authentication protocol.

7. Attempt any *one* part of the following: 10x1=10

a. What is Trojan Horse? What is the principle behind it?
b. List the characteristics of a good firewall implementation? How is a circuit gateway different from an application gateway?