S.No. : 196 **MCA 2512**

No. of Printed Pages : 03

Following Paper ID and Roll No. to be filled in your Answer Book.

PAPER ID : 21259 **Roll No.** □□□□□□□□□□

MCA Examination 2018-19

(Fifth Semester)

CRYPTOGRAPHY AND NETWORK SECURITY

Time : Three Hours] *[Maximum Marks : 60*

Note :– Attempt all questions.

SECTION–A

1. Attempt all parts of the following : 8×1=8

   (a) What is Cryptography?

   (b) Differentiate between plain text and cipher text.

   (c) Define block cipher.

   (d) Describe avalanche effect.

   (e) Name the technique of public key with description.

[P. T. O.

(f) Define digital certificate.

(g) What is key bores?

(h) What is trusted system?

SECTION – B

2. Attempt any two parts of the following : 2×6=12

(a) Using play-fair cipher, show the encription and descryption of "BBD UNIVERSITY" where key word is "COMPUTER".

(b) Describe Diffie-Hellman key exchange algorithm. Also generate key for a prime no = N = 11.

(c) Differentiate between DES and triple DES. Also discuss about weakness of DES.

(d) Discuss about SSL and TLS.

SECTION – C

Note :– Attempt all questions from this section.

3. Attempt any two parts of the following : 5×2=10

(a) What is difference between monoalphabatic and polyalphabetic cipher?

(b) Describe different types of attack.

(c) What are the requirements for secure use of conventional encryption?

4. Attempt any two parts of the following : 5×2=10

(a) Describe feistal cipher structure with diagram.

(b) Describe different mode of operation of DES.

(c) Discuss RSA algorithm with one example.

5. Attempt any two parts of the following : 5×2=10

(a) Briefly describe keyberos V4.

(b) Describe Hashes and message digests with its uses.

(c) Describe digital signature algorithm.

6. Attempt any two parts of the following : 5×2=10

(a) Explain S/MIME in detail.

(b) What do you understand by Secure Electronic Transaction (SET)?

(c) What is PGP and list various services supported by PGP?

⌘⌘⌘