Roll No. : .....

Total No. of Questions : **16**] [Total No. of Printed Pages : **3**

SEM2021

M.Sc. (IInd Semester) Examination, 2021

CYBER SECURITY

Paper – MCSEC–201

(Information Security and Cryptography)

Time : 1½ Hours] [*Maximum Marks : **40***

Note :– This question paper contains *three* Sections.

Section–A **(Marks : 1 × 10 = 10)**

Note :– Answer all the *ten* questions carry **1** mark each. The answer should not exceed **50** words.

Section–B **(Marks : 3 × 5 = 15)**

Note :– Answer *five* questions by selecting at least *one* question from each Unit. Each question carries **3** marks. Answer should not exceed **200** words.

Section–C **(Marks : 5 × 3 = 15)**

Note :– Answer *three* questions by selecting *one* question from each Unit. Each question carries **5** marks. The answer should not exceed **500** words.

Section–A

1. Attempt all questions. Answers should not exceed **50** words in each question :

   (i) What is 'Mc-Cumber Cube' with reference to CNSS security model ?

(ii) Which are important approaches to 'Information Security Implementation' ?

(iii) Briefly discuss about 'Vigenere' Cipher in Cryptography.

(iv) Write down various types of symmetric key ciphers.

(v) Differentiate between symmetric and asymmetric key ciphers.

(vi) What are requirements of good 'Hash' function ?

(vii) How 'digital signature' is implemented using R.S.A. algorithm ?

(viii) Briefly explain handshake protocol in SSL.

(ix) Write down the steps for preparing S/MIME.

(x) What is the need and concept of MAC algorithms ?

Section–B

Note :– Answer *five* questions in about **200** words, by selection at least *one* question from each Unit. Each question carries 3 marks.

Unit–I

2. Explain CNSS security model with example.

3. Describe about Traditional Caesar Cipher. Also mention an example.

4. What are *two* general approaches for attacking a cipher ?

Unit–II

5. Differentiate between 'Diffusion' and 'Confusion' in context of ciphering.

6. Explain 'Avalanche effect' in DES. Use an example also.

7. How S-boxes are constructed in case of AES ?

Unit–III

8. What are the properties that a digital signature should have ?

9. Briefly explain the concept of IP Sec and write its applications.

10. Briefly discuss about linear cryptanalysis.

Section–C

Note :– Answer *three* questions in this Section, by selecting *one* question from each Unit, in about **500** words. Each question carries 5 marks.

Unit–I

11. Explain the security system development life-cycle with example.

12. Write a note on 'Substitution and transposition' concepts in context of ciphers.

Unit–II

13. Explain concept of Diffie-Hellman Key Exchange.

14. Describe about MAC and Hash functions used for message authentication.

Unit–III

15. Elaborate the concept of Kerberos. Compare it with its peer techniques.

16. Write short note on any *one* topic out of the following :

    (a) PGP

    (b) TLS

    (c) Steganography

    (d) Differential cryptanalysis