Roll No. ☐☐☐☐☐☐☐☐☐☐☐☐☐   Total No. of Pages : 02

Total No. of Questions : 09

BMCI (2014 & Onwards)   (Sem.–5)

INFORMATION SECURITY

Subject Code : BMCI-505

M.Code : 74107

Time : 3 Hrs.   Max. Marks : 60

INSTRUCTIONS TO CANDIDATES :

1. SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.
2. SECTION-B contains FIVE questions carrying FIVE marks each and students have to attempt any FOUR questions.
3. SECTION-C contains THREE questions carrying TEN marks each and students have to attempt any TWO questions.

SECTION-A

1. Answer briefly :

a) What is avalanche effect?

b) What are the types of attacks on encrypted message?

c) What is the international security standard

d) What is IPR?

e) What is SSL?

f) Define Weak Collision property of a hash function.

g) What is x.509 standard?

h) What is role based security.

i) What are honey pots?

j) List down the four phases of virus.

SECTION-B

2. Briefly describe the Shift Rows and Byte Substitution layers of Rijndael. Explain why we can apply them in either order with the same result.

3. What are Attacks and Threats? Explain about various mechanisms by which organizations can protect from them.

4. What is the need for Electronic mail security?

5. Who is an Intruder? Explain how intruders can be detected in a network.

6. What is a Firewall? Explain the design principles of a firewall.

SECTION-C

7. Explain the following with example:

a) Confidentiality

b) Authentication

c) Masquerade

8. How is the design of AES algorithm more secure & robust? Explain the key steps used in AES contributing to its security.

9. What is a Digital Signature? How are Digital Certificates generated? Explain Relationship between Digital Signature and Digital Certificate.

NOTE : Disclosure of Identity by writing Mobile No. or Making of passing request on any page of Answer Sheet will lead to UMC against the Student.