Total No. of Questions: 07

BCA (Only 2015 Batch) (Sem. – 6)

INFORMATION SECURITY

M Code: 75014

Subject Code: BSBC-604

Paper ID: [75014]

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 SIX questions carrying TEN marks each and students have to attempt any FOUR questions.**

SECTION A

1. a) What is a digital signature?

   b) What is denial service attack?

   c) What is ECB mode?

   d) What is the procedure for key generation using RSA?

   e) What is the purpose and the use of a KDC?

   f) What is non-repudiation?

   g) What is session key?

   h) What is avalanche effect?

   i) What is masquerading?

   j) What are honey pots?

SECTION B

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

3. What are the different block cipher modes of operation of DES? How does triple DES works?

4. What are the various Security services that a Cryptographic package has to provide?

5. What is Cryptography? Explain the key elements of a Cryptographic system. Write about Conventional and Public-key cryptographic methods available.

6. Explain

   a) Electronic Mail Security

   b) Web Security

7. a) What is Authentication? Explain in detail how password-based and addressed-based authentication services work.

   c) Explain Relationship between Digital Signature and Digital Certificate.