

Roll No.

Total No. of Pages : 02

Total No. of Questions : 07

BCA (2014 to 2018)) (Sem.-6)

**INFORMATION SECURITY**

Subject Code : BSBC-604

M.Code : 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. Answer briefly :**

- a) What are block ciphers?
- b) What are the active attacks?
- c) What is CIA?
- d) What is the concept of confusion and Diffusion?
- e) What is CBC mode of DES?
- f) Distinguish Threats, Vulnerabilities.
- g) What is phishing and types?
- h) Distinguish functioning of Virus and worm.
- i) What are different key sizes and number of rounds relation in AES?
- j) What is Steganography?

## SECTION-B

2. What are the Key principles of Security, discuss each in details?
3. Explain working and use of :
  - a) PGP
  - b) SSL
4. Write and explain RSA algorithm using P and Q prime numbers.
5. Discuss the different steps of security system development life cycle.
6. Explain the IDS systems for Network and nodes in detail.
7. What is Firewall; discuss different types and their functions of firewall.

**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.**