

Roll No.

Total No. of Pages : 02

Total No. of Questions : 16

B.Sc.(IT) (2015 & Onward) (Sem.–5)

INFORMATION SECURITY

Subject Code : BSIT-501

M.Code : 74375

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

Answer briefly :

1. What is Role-based access control?
2. What are the approaches used for implementing Information Security?
3. What is the major limitation of traditional substitution ciphers? How do the modern block ciphers address it?
4. What is Encryption?
5. What are flooding attacks?
6. What is injection attack?
7. What is rootkit?
8. What is intrusion detection?
9. What are the potential threats posed by Denial of Service attacks?
10. What is data authentication?

\

SECTION-B

11.
 - a. Explain the DES Algorithm.
 - b. Describe the cipher block modes operation.
12. What is public key cryptography? What are the principal ingredients of a public-key cryptosystem? Explain the steps followed in public key cryptography algorithms.
13. What are threats? Explain the different categories of Threats.
14.
 - a. Differentiate between access control list and a capability ticket.
 - b. What are the Principles for Access Control? Explain the Role - Based Access Control with example.
15.
 - a. During its lifetime, a typical virus goes through the four phases. Explain.
 - b. Describe Electronic mail security using PGP.
16.
 - a. Discuss several software security concerns associated with writing safe program code.
 - b. What are the main security concerns with virtualized systems? Explain.

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.