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

Total No. of Questions: 09

M.Sc. (IT) (2015 Onwards)   (Sem. – 4)
INFORMATION SECURITY
M Code: 74114
Subject Code: MSIT-402
Paper ID: [74114]

Time: 3 Hrs.   Max. Marks: 60

INSTRUCTIONS TO CANDIDATES:
1. **SECTIONS-A, B, C & D contains TWO questions each carrying TEN marks and students has to attempt any ONE question from each SECTION.**
2. **SECTION-E is COMPULSORY consisting of TEN questions carrying TWENTY marks in all.**
3. **Use of Non-programmable scientific calculator is allowed.**

SECTION A

1. Define Cryptography? Explain the given cryptographic tools along with given applications: Public key Encryption and Digital signatures.

2. Explain different strategies for providing security to open systems, also give detailed introduction to the security functional requirements.

SECTION B

3. In IT security management, how the organizational security risks can be identified and how Risk assessment and analysis can be done? Justify your answer with suitable example.

4. Explain the method for providing virtualization security? Also elaborate the terms: system security planning and system security hardening?

SECTION C

5. Why do we need database security? Explain different mechanisms to provide security to relational databases and statistical databases.

6. Explain symmetric encryption? Explain different kinds of hash functions to provide authentication and security.

SECTION D

7. State and differentiate between DDoS and reflector & amplifier attacks with suitable examples.

8. What is user authentication? How an Iris Biometric system works and fulfills this requirement?

SECTION E

9. a) What are Flooding attacks?

   b) What do you mean by message authentication? Where it is used?

   c) How can we write safe program code?

   d) Explain the working of token based authentication.

   e) How trusted computing can be performed?

   f) Why do we use cryptographic tools? Name any two.

   g) Illustrate the causes of stack overflow? How it can be defended?

   h) Write a short note on defenses against denial-of-service attacks.

   i) What are Bots? Give suitable examples.

   j) Write down the usage of security controls?