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

Total No. of Questions : 09

MCA (2015 Batch) (Sem.–3)

INFORMATION SECURITY

Subject Code : MCA-302

Paper ID : [74074]

Time : 3 Hrs. Max. Marks : 60

INSTRUCTIONS TO CANDIDATES :

1. **SECTIONS-A, B, C & D contains TWO questions each carrying TEN marks each and students have to attempt any ONE question from each SECTION.**
2. **SECTION-E is COMPULSORY consisting of TEN questions carrying TWENTY marks in all.**

SECTION-A

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

2 a) What is the purpose of a nonce in an end-point authentication protocol?

b) What is meant by IP spoofing? How can a router be used to prevent IP spoofing?

c) What is the main drawback of the one time pad cryptosystem?

SECTION-B

3. What are the differences between message confidentiality and message integrity? Can you have one without the other? Justify your answer.

4. What is the need of database security? Explain various methods using which a database can be secured in terms of Encryption, Access Control and Authenticates Access.

SECTION-C

5. a) What are different kinds of malware?

b) What are the different methods of malware propagation?

6. Which malware programs are known to be most severe in terms of damage that they can make? What do you understand by a stack and a buffer overflow? How are these two different? What are the practices of writing a safe program code?

SECTION-D

7. What are the various approaches to Risk Management? Compare the two approaches to Risk Prioritization. What is the difference between Risk Management and Risk Assessment?

8. a) State the complete Information Security Life Cycle. Explain the relevance of each phase.

   b) What is the need of having company-wide framework for BCM (Business Continuity Management)?

SECTION-E

9. Write briefly :

a. How are AES, DES and triple DES different on the basis of design and features? Also describe the operation of AES algorithm.

b. What requirements must a public key cryptosystem fulfill to be a secure algorithm?

c. In the RSA system, the public key of a given user is e = 31, n = 3599. What is the private key of the user?

d. What is the major limitation of traditional substitution ciphers? How do the modern block ciphers address it?

e. What is the major limitation of the traditional one-time pad? How do the modern stream ciphers address it?

f. Is AES a SYMMETRIC cipher? Why/why not?

g. You are sending confidential information to a colleague across the internet. How can you protect this message from being read by individuals other than the intended recipient?

h. What is a Social Engineer?

i. What are the potential threats posed by Denial of Service attacks?

j. What are the differences between a MAC and a digital signature? What are the respective advantages of each?