

Roll No.....

Total No. of Printed Pages: 1

Total No. of Questions: [09]

BCA-MCA Dual Degree (Semester – 6th)
NETWORK SECURITY
Subject Code: BMCAS1602
Paper ID: 19340125

Time: 03 Hours

Maximum Marks: 60

Instruction for candidates:

1. Section A is compulsory. It consists of 10 parts of two marks each.
2. Section B consist of 5 questions of 5 marks each. The student has to attempt any 4 questions out of it.
3. Section C consist of 3 questions of 10 marks each. The student has to attempt any 2 questions.

Section – A

(2 marks each)

Q1. Attempt the following:

- a. Explain active and passive attack with example.
- b. Differentiate symmetric and asymmetric encryption?
- c. Differentiate amongst spyware, malware, Adware.
- d. Explain the importance of Authentication.
- e. Write a short note on PGP
- f. What is Deffie-Hellman algorithm? What is the use of it in Network Security
- g. Explain Rail Fence algorithm
- h. What is meant by DDOS attacks?
- i. Discuss Ransomware attack.
- j. Describe the use of PGP

Section – B

(5 marks each)

Q2. Define & Differentiate between Diffusion & Confusion

Q3. P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 6, then what will be cipher text value according to RSA algorithm?

Q4. List the security services provided by digital signature. Write and explain the Digital Signature Algorithm

Q5. Explain DES key generation process in detail

Q6. What is Hash function why it is used? Describe the requirements for a Hash function.

Section – C

(10 marks each)

Q7. Define Cryptography and Crypt-analysis. Draw and explain conventional cryptosystem.

Q8. Explain the Firewall design principles.

Q9. Who are participants of SET? Give the sequence of events required for SET, explain it with proper example?