Paper / Subject Code: 70653 / Information Security

1T00162 - MCA (Sem-II) (R-2020-21) / 70653 - Information Security
QP CODE: 10031827 DATE: 28/07/2023

(3 Hours) **Total Marks: 80**

Note: 1) Question No.1 is compulsory.
2) Attempt any THREE from the remaining questions.
3) Figures to the right indicate full marks.

1. (a) Discuss various components of Information security. **5**
   (b) Explain Inference. **5**
   (c) Discuss various types of P-Boxes. **5**
   (d) Write a short note on SAML Assertion. **5**

2. (a) Discuss SHA-512. **10**
   (b) Discuss various types of authentication tokens. **10**

3. (a) What is a Digital Certificate? Explain the process of generating digital Certificate? **10**
   (b) Explain SSL as an internet security protocol and discuss three major protocol use at SSL? **10**

4. (a) What are firewalls? Discuss various methods used for firewall configuration, along with their advantages and disadvantages. **10**
   (b) In a system, an RSA algorithm with p=5 and q=11 is implemented for data security. What is the value of decryption key if value of encryption key is 27? Also verify that calculated value of decryption key is correct. **10**

5. (a) Why certificates are revoked? Explain the methods used for the same. **10**
   (b) Using the Euclidean algorithm, find the greatest common divisor of the following pairs: **10**

   84 and 320
   400 and 60

6 (a) Discuss one round structure of DES. **10**
  (b) Explain the security features of OS. **10**