1T00162 - M.C.A. (SEM-II) (R-2020-21) / 70653 - Information Security
QP CODE: 10043747 DATE : 4 JAN 2024

Time: 3 Hours **Max. Marks: 80**

- Q.1 is Compulsory
- Solve any three Questions from Q 2, Q 3, Q 4, Q 5 ,Q 6

Q.1 A) Explain PGP **(5M)**

B) Explain Kerberos. **(5M)**

C) Discuss Digital Certificate **(5M)**

D) Discuss Phone Rootkits. **(5M)**

Q.2 A) Explain Modes of Operation of Block Cipher CBC and OFB in detail. **(10M)**

B) What is SHA -512? Explain SHA- 512 in detail. **(10M)**

Q.3 A) Discuss Inference. What are the various approaches to deal with it? **(10M)**

B) What is Firewall? Discuss its types in detail. **(10M)**

Q.4) A) What is IDS? Explain Statistical Anomaly Detection and Rule based Detection. **(10M)**

B) Explain SSL Handshake Protocol in detail. **(10M)**

Q.5 A) Using Euclidean algorithm, find the greatest common divisor of the following:

i) 74 and 383 ii) 687 and 24 **(10M)**

B) Explain RSA algorithm with example. **(10M)**

Q.6 A) Explain Digital Encryption Standard (DES) in detail**.** **(10M)**

B) What are the different security services? Explain each in brief with example. **(10M)**
