10/12/2024 MCA SEM-II   CHOICE BASED (TWO YEAR COURSE) INFORMATION SECURITY
QP CODE: 10068243

Time: 3Hours   Max. Marks: 80M
- Q.1 is Compulsory
- Solve any three Questions from Q 2, Q 3, Q 4, Q 5 ,Q 6

Q.1 Write short note on the following:

  A) PGP   **(5M)**

  B) SOAP Web service   **(5M)**

  C) Phone Rootkits   **(5M)**

  D) MAC   **(5M)**

Q.2 A) What are the different security services? Explain each in brief with example.   **(10M)**

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

Q.3 A) Explain modes of Block Cipher CFB and CBC in detail.   **(10M)**

  B) What is Firewall? Explain Packet filter and Circuit level firewall in detail.   **(10M)**

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

  B) What is Message Digest? Explain MD5 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) Discuss Inference. What are the various approaches to deal with it?   **(10M)**

Q.6 A) What is Digital certificate? Explain Certificate creation and revocation process in detail. **(10M)**

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