Roll No. □□□□□□□□□□□□ **Total No. of Pages : 02**

Total No. of Questions : 09

MCA (2012 & Onward) (Sem.–5)

NETWORK SECURITY & ADMINISTRATION

Subject Code : MCA-502

Paper ID : [A3160]

Time : 3 Hrs. **Max. Marks : 100**

INSTRUCTIONS TO CANDIDATES :

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

SECTION-A

1. a) Explain the key principles of security. Discuss at least three security attack reported in last few years.

   b) Describe, in details, what is cipher block chaining (CBC). (*i.e.* how to encrypt and decrypt a message).

2. Define what a Message Authentication Code (MAC) system is and the properties it should have. Describe a practical use for a MAC. Describe how to build a MAC system from a given symmetric cryptosystem.

SECTION-B

3. What do you mean by Public key Cryptography? Give one advantage and one disadvantage of public-key cryptography over symmetric-key cryptography. Explain RSA algorithm with suitable example.

4. a) How does the Kerberos Version 5 Authentication Protocol Work? Summarize Kerberos Version 5 message exchange.

   b) What is the difference between digital certificates and digital signatures? Explain different “Digital Signature Standards (DSS)” in detail.

SECTION-C

5. a) List the characteristics of a good firewall implementation. How is a circuit gateway different from an application gateway?

   b) What do you mean by NAT? What is its purpose?

6. a) Explain the encapsulating security payload (ESP). Why does ESP include a padding field?

   b) Explain IP Security Architecture. How IPSec can be used to create VPN? How will you justify the need of IP security along with other security features?

SECTION-D

7. What is Requirement of Web Security? How web security goals can be achieved? What are different security issues for transport layer? Name and explain the cryptographic techniques used by Transport Layer Security (TLS).

8. What do you mean by Pretty Good Privacy (PGP)? How the messages are generated and transmitted in PGP protocol? Explain with clear diagrams.

SECTION-E

9. **Write briefly :**

   a) Why is mono-alphabetic cipher difficult to crack?

   b) What is meet-in-the-middle attack?

   c) What is the difference between substitution and transposition cipher?

   d) What do you mean by Authentication and Authorization? Explain.

   e) Explain the difference between a session key and a master key.

   f) Which of the following is not a fundamental security goal?

      i) Confidentiality

      ii) Integrity

      iii) Assurance

      iv) Availability

   g) The cryptographic strength of RSA depends on which hard problem?

      i) Discrete logarithms

      ii) Factoring large primes

      iii) Bin packing

      iv) Elliptic curves

   h) If all traffic that comes through the gateway is encrypted, how will it affect application level firewalls?

   i) **TRUE or FALSE :** An attraction of public key cryptography is that, if implemented properly, the algorithms generally run much faster than those for symmetric key cryptography.

   j) Define certificate and certificate authority.