MCA
(SEM V) THEORY EXAMINATION 2018-19
CRYPTOGRAPHY AND NETWORK SECURITY

Time: 3 Hours   *Total Marks: 100*

Note: 1.   Attempt all Sections. If require any missing data; then choose suitably.
2.   Any special paper specific instruction.

SECTION A

1.   **Attempt *all* questions in brief.**   **2 x10 = 20**

a.   Discuss the attacks.
b.   Explain steganography.
c.   What is data confidentiality?
d.   What is Triple DES?
e.   Define Stream Cipher.
f.   Discuss the Plain Text.
g.   Explain Encryption Process.
h.   Define Block principle.
i.   Explain Data Integrity.
j.   What do you mean by Traffic padding?

SECTION B

2.   **Attempt any *three* of the following:**   **10 x 3 = 30**

a.   What is Symmetric Cipher Model? Also explain difference between Symmetric and Asymmetric model.
b.   Explain Playfair cipher. If Plain Text=wearecomputersciencestudents find cipher text.
c.   What do you mean by mode of operations? Explain with the help of diagrams.
d.   Explain Multiple encryptions.
e.   Discuss the following-
      (i)   Link Encryption Approach
      (ii)   S/MIME

SECTION C

3.   **Attempt any *two* parts of the following:**   **5 x 2 = 10**

(a)   Explain Euler's theorem
(b)   Describe Random number generation.
(c)   Explain the Man-in-Middle attack.

4.   **Attempt any *one* part of the following:**   **10 x 1 = 10**

(a)   Explain the Security of Hash Function. Also explain SHA.
(b)   What do you mean by distribution of Public Key cryptosystem ?

5. **Attempt any *one* part of the following:**   **10 x 1 = 10**
    (a)   Explain RSA Algorithm with the help of example .
    (b)   What do you mean by digital Signature? Also explain DSA.

6. **Attempt any *one* part of the following:**   **10 x 1 = 10**
    (a)   Describe the following in brief:
          (i)   KDC.
          (ii)   MAC
    (b)   Describe Electronics mail Security? Explain PGP

7. **Attempt any *one* part of the following:**   **10 x 1 = 10**
    (a)   Explain following:
          (i)   Intrusion Detection
          (ii)   Password Detection.

    (b)   Explain Viruses and related Threats. Also explain Distributed Denial of service attacks.