**11819**

**3 Hours / 100 Marks**     Seat No.

*Instructions :*   (1)   All Questions are *compulsory.*

(2)   Illustrate your answers with neat sketches wherever necessary.

(3)   Figures to the right indicate full marks.

(4)   Assume suitable data, if necessary.

(5)   Use of Non-programmable Electronic Pocket Calculator is permissible.

(6)   Mobile Phone, Pager and any other Electronic Communication devices are not permissible in Examination Hall.

**Marks**

1.   **(A)   Attempt any THREE :**                                    **3 × 4 = 12**

(a)   List pillars of information security and explain any one with neat sketch.

(b)   Define RISK. Describe how RISK is managed for Information Security.

(c)   Define following terms :

(i)   Cryptography

(ii)   Cipher text

(iii)   Encryption

(iv)   Cryptology

(d)   Define following terms :

(i)   Hacking

(ii)   Cracking

(iii)   Cyber crime

(iv)   Data recovery

    **(B) Attempt any ONE :**      **1 × 6 = 6**

    (a) Define information classification. Describe criteria for information classification.

    (b) Describe following with neat sketch :

      (i) Ring of trust in single system

      (ii) Ring of trust in networked system.

**2. Attempt any TWO :**      **2 × 8 = 16**

    (a) Define Security. Describe principles of information security with neat sketch.

    (b) Explain different phases in play fair cipher with suitable example.

    (c) Explain concept hacking and cracking. Explain different types of Hackers.

**3. Attempt any FOUR :**      **4 × 4 = 16**

    (a) Describe confidentiality model of Information Security.

    (b) Describe any four major sources of physical security threats.

    (c) List any two integrity models & describe Clark & Wilson model.

    (d) Consider plaintext "PIET" and key "HILL" and convert into cipher text using Hill cipher.

    (e) Describe pornography & intellectual property.

**4. (A) Attempt any THREE :**      **3 × 4 = 12**

    (a) Describe TCB with neat sketch.

    (b) Describe following terms :

      (i) Authorization

      (ii) Authentication

      (iii) Access

      (iv) Identification

    (c) Explain Biba model for integrity.

    (d) Describe any four applications of cryptography.

   **(B) Attempt any ONE :**       $1 \times 6 = 6$

     (a) Elaborate what is cryptography. Explain integrity and non-repudiation with respect to cryptography.

     (b) Enlist authentication protocols and describe any two in details.

**5. Attempt any TWO :**       $2 \times 8 = 16$

     (a) Enlist two types of failures. How deleted files can be recovered ?

     (b) Describe COBIT framework with neat sketch.

     (c) Describe stepwise working of Single-Sign-On (SSO).

**6. Attempt any FOUR :**       $4 \times 4 = 16$

     (a) Describe IT Act, 2000.

     (b) Explain working of Virtual Private Network with neat sketch.

     (c) Describe what is ITSEC. List out various classes of ITSEC.

     (d) Describe TCSEC model.

     (e) Describe working of stegnography with neat diagram.

_____