(Use a separate answer book for **each unit**)

Unit - I

Answer **any one** question of the followings **:**   [1 × 5]

1. a) Write short notes on the following terms :   (3+2)

   i)   Cathode Ray Tube (CRT) display device

   ii) JPEG

   b) State whether the following statements are true or false, and justify your answer. $\left(2\frac{1}{2} \times 2\right)$

   i)   A point is described as exterior by odd even rule and can be described as an interior point by non-zero winding rule.

   ii) To double the size of an object, uniform scaling is needed.

Answer **any two** questions of the followings **:**   [10 × 2]

2. a) Write down the difference between Thin-film electroluminescent display and Liquid-crystal display techniques.   (2)

   b) What is refresh display file? What will be happened if the file is shorter in size?   (2)

   c) Which line drawing algorithm is more efficient between DDA and Bresenham's line algorithm and why?   (2)

   d) What is the fraction of the total refresh time per frame spent in retrace of the electron beam for a non-interlaced raster system with a resolution of 1280 by 1024, a refresh rate of 60 Hz, a horizontal retrace time of 5 microseconds and a vertical retrace time of 500 microseconds?   (4)

3. a) Show that a 2D reflection through X-axis followed by a 2D reflection through the line y = -x is equivalent to pure rotation about the origin.   (4)

   b) A cube with unit dimension is placed at origin in first octant. Reflect it with respect to plane z = 0. Then perform 500% scaling. Find the transformation matrix which can generate the target object.   (4)

   c) Explain Perspective Projections.   (2)

4. a) Why orthographic projections are useful in engineering and architectural drawings?   (1)

   b) Explain the four blending functions for cubic Bezier curves with geometrical representation. (4)

   c) Consider a line in 3D, which does not pass through origin and is not parallel to any co-ordinate axis. Find out the composite transformation matrix to align this line into Z-X plane such that it passes through the origin.   (5)

5. a) Describe the different steps to design an animation sequence.   (3)

   b) For an object transformation, two key frames are given. Key frame k has 4 line segments and that of key frame (k+1) is 11. For this transformation explain the general pre-processing rules for equalizing key frames in terms of number of edges.   (3)

c) Evaluate the new location of a point (1,2,3) after taking perspective projection on a plane z=7 with the projection reference point (0,0,11). (4)

Unit – II

Answer **any three** questions of the followings **:** [3 × 10]

6. a) Explain the term Integrity, Digital Envelop & Digital Certificate.

   b) Briefly discuss about the usefulness of Modular Arithmetic in cryptography.

   c) Consider a columnar transposition where cipher text is ARIFSVALOHLMASTTININE IDDFEBFYIEOEE and the keyword is HOSTEL. Find the plaintext. (1.5+3.5+5)

7. a) What do you mean by multiplicative

      i) inverse in the context of cryptography?

      ii) Find the multiplicative inverse of z3 in Z_{100}.

   b) Define congruence and compare with equality.

   c) Perform the following operations (the input come from Z or Z_n):

      i) Add 17 to 27 in Z_{14}.

      ii) Subtract 34 from 12 in Z_{13}.

      iii) Multiply 123 by -10 in Z_{19}. ((2+3)+2+(1+1+1))

8. a) State and explain Fermat's little Theorem and Chinese Remainder Theorem.

   b) Find the solution to the simultaneous equations:

      $x \equiv 2 \bmod 3$
      $x \equiv 3 \bmod 5$
      $x \equiv 2 \bmod 7$

      Using Chinese Remainder Theorem (CRT).

   c) What is the difference between monoalphabetic and polyalphabetic cipher? $\left(\left(2\frac{1}{2}+2\frac{1}{2}\right)+3+2\right)$

9. a) Suppose two parties Alice & Bob want to establish a secret key using the Diffie-Hellman (D-H) key exchange protocol. They agree on 7 as modulus and 5 as the primitive root, Alice chooses 2 and Bob chooses 3 as their respective secrets. Find out D-H secret key.

   b) Briefly discuss the rounds of DES algorithm.

   c) What do you mean by Avalanche effects in the context of DES? (4+4+2)

10. a) What do you mean by trapdoor one way function in cryptography?

    b) Briefly discuss about RSA algorithm.

    c) Explain the Fiat-Shamir Protocol for zero-knowledge authentication. (2+3+5)

———— × ————