RAMAKRISHNA MISSION VIDYAMANDIRA

(Residential Autonomous College affiliated to University of Calcutta)

B.A./B.Sc. SIXTH SEMESTER EXAMINATION, MAY 2017

THIRD YEAR [BATCH 2014-17]

Date : 02/05/2017 **COMPUTER SCIENCE (Honours)**

Time : 11 am – 3 pm **Paper :** VII Full Marks : 100

[Use a separate Answer Book for each group]

Group – A

1. Answer **any one** question : [1×5]
   a) Explain JPEG Compression Technique.
   b) Explain the role of Homogeneous Co-ordinate system in Computer Graphics.

   Answer **any two** questions : [2×10]

2. a) Compare Raster Scan and Random Scan display principles.
   b) Do you think that interlacing gives any extra benefit in the scanning process? Explain.
   c) Write a short note on Morphing. (4+2+4)

3. a) Trace the Bresenham's line drawing algorithm for drawing a line segment from (8,5) to (2,10).
   b) Show the symmetric points corresponding to (x, y), on a circle How do they help in scan conversion?
   c) Write down the conditions upon which a co-ordinate is selected as a part of a circle in mid-point circle drawing algorithm. (6+3+1)

4. a) Write the procedure to determine the seed pixel in polygon fill using odd even method.
   b) Using Cohen-Sutherland line clipping algorithm clip a line with endpoints $(x_1, y_1) = (4, 12)$ and $(x_2, y_2) = (8, 8)$ within the viewport of $xw_{\min} = 5,\ xw_{\max} = 9,\ yw_{\min} = 5, yw_{\max} = 9$. (4+6)

5. a) Derive the transformation matrix to rotate an object 30° about the origin. What will be the effect of applying their matrix operator on the point P(2, –6).
   b) Derive a composite transformation matrix after a 90° rotation about origin followed by reflection through the line $y = x$. (5+5)

Group – B

6. Answer **any one** question: [1×5]
   a) Write a short note on (i) HTTP, (ii) SSH (2½+2½)
   b) (i) "In TCP, acknowledgement number is cumulative" — Justify.
      (ii) What is the use of urgent pointer field in TCP header?
      (iii) Differentiate between internet and Internet. (2+2+1)

   Answer **any four** questions: [4×10]

7. a) Write a practical example where inverse domain of DNS mapping is used.
   b) Explain the step of POP3 protocol.
   c) Explain the matrices on which routing of a packet depends.
   d) "In CRC, a polynomial generator that contains a factor of $x + 1$ can detect all odd-numbered errors"— Justify.
   e) What is the difference between a hub and a switch? (1+2+4+2+1)

8. a) Differentiate between protocol and standard.
   b) A telephone line has frequencies ranging from 300 Hz to 3300 Hz assigned for data communication. The signal-to-noise ratio is 3162. Find out the channel capacity of the telephone line.
   c) What the advantages of IPV6 over IPV4 Addressing?
   d) Find out the Hamming Code for the data bit 10110101101. (2+2+3+3)

9. a) Explain the addressing mechanism of IEEE 802.11 wireless LAN.
   b) What is socket address?
   c) Explain different propagation modes of optical fiber cable. (4+2+4)

10. a) What do you mean by "this host on this network"?
   b) An organization is granted a block of addresses with beginning address 14.24.74.0/24. The organization needs to have 11 subnets as shown below:
      i) two subnets, each with 64 addresses
      ii) two subnets, each with 32 addresses
      iii) three subnets, each with 16 addresses
      iv) four subnets, each with 4 addresses.
      Design the subnets.
   c) Explain the working of ADSL Modem. (2+6+2)

11. a) Draw the digital signal for the following bit string using Alternate Mark Inversion (AMI) coding: 10111010
   b) Explain the working of QAM.
   c) How NAT is useful in solving address depletion problem?
   d) Explain pulse code modulation encoding process in brief. (2+2+2½+3½)

12. a) Explain the term Noise, Distortion and Alternation with example.
   b) What is Van Allen band?
   c) Explain the 3-way handshake of TCP connection establishment.
   d) Differentiate between packet switching and circuit switching. (3+2+2+3)

Group – C

(Cryptography)

Answer **any three** questions from **Question No. 13 – 17** : [3×10]

13. a) Explain the different types of attack on the different Key principle of security.
   b) Give the difference between Block Cipher & Stream Cipher.
   c) Assume a plain text security is important and generate the corresponding cipher text using Rail Fence technique. (4+2+4)

14. a) "Euler's Theorem is a generalization of Fermat's little theorem" — Justify.
   b) Suppose two parties Alice and Bob want to establish a secret key using the Diffie–Hellman (D–H) Key Exchange protocol. They agree on 11 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.
   c) Explain different application of Chinese Remainder Theorem. (3+5+2)

15. a) Describe the advantages and disadvantages of Public Key and Private Key Cryptography.
    b) Consider a columnar transposition cipher where cipher text is AFLLSKSOSELAWAIATOOSSCTCLNMOMANTESILYNTWRNNTSOWDPAEDOBUOERIRICXB and the keyword is MEGABUCK. Find the plaintext.
    c) Explain the concept of Confusion & Diffusion in Symmetric Key Cryptography. (3+5+2)

16. a) Briefly discuss the steps involved in one round in Data Encryption Standard algorithm.
    b) Explain the concept of Digital Envelop,
    c) Briefly mention the strength and weakness of DES algorithm. (5+2+3)

17. a) Briefly discuss about on entity authentication scheme where the protocol works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.
    b) Explain the strength of RSA algorithm.
    c) What do you mean by Digital Certificate – Explain with example. (6+2+2)

OR

Group - C

(Data Mining & Data Warehouse)

Answer **any three** questions from **Question No. 18 – 22 :** [3×10]

18. a) A factory production line manufacture bolts using three machines A, B and C of the total output, machine A is responsible for 40%, machine B for 25% and machine C for the rest. It is known from the part experience that 5% output of machine A, 4% of machine B and 3% of machine C are defective. A bolt is chosen at random and found to be defective. What is the probability that it came from
    (i) Machine B (ii) Machine C.
    b) In the process of PCA computation, we compute eigenvalues. Whether all eigen values in PCA will be real or they may be imaginary? Justify your answer.
    c) Explain the term DMQL. (4+4+2)

19. a) Explain different types of Data Cleaning approaches.
    b) Develop the mathematical model for a multi-layer back propagation neural network model. (2+8)

20. a) What do you mean by information gain in the context of decision tree? Explain with example.
    b) Explain the Data Warehousing architecture.
    c) Explain association rule mining. (4+4+2)

21. a) What do you mean by full cube and iceberg cube?
    b) Discuss any one data cube computation method in brief.
    c) Explain the method of Bayesian classification. (3+5+2)

22. a) A car marketing company considers three attributes for their analysis, namely color, brand and type. It considers only three colors, two brands namely Honda and Hyundai and three types namely SUV, Sedan and Hatchback.
    Consider the following table and the persons whose tests are more similar than the third one.

Person	Color	Brand	Type
P_1	Red	Hyundai	Sedan
P_2	Red	Honda	SUV
P_3	Red	Hyundai	Sedan

b) Edit distance computes dissimilarity of two strings (e.g. words) by counting the minimum number of operations required to transform one string into other. The operations are mention, deletion and substitution of a single character at any position of the string. For example, edit distance between *a* = "11" and *b* = "110" is 1 because deleting last bit of *b* (one operation) makes them same.

Hamming distance between two strings of equal length is the number of positions at which the characters are different.

Consider the two-strings:

Str1 = "bccbbcb", Str2 = "ccbbccb" and find the edit distance and Hamming distance between them.

c) Explain the term Web Usage mining. (3+4+3)

———— × ————