19

[This question paper contains 7 printed pages]

Your Roll No. : 2019

Sl. No. of Q. Paper : **7466** **J**

Unique Paper Code : 32351501

Name of the Course : **B.Sc.(Hons.) Mathematics**

Name of the Paper : Metric Spaces

Semester : V

Time : 3 Hours ***Maximum Marks : 75***

Instructions for Candidates :

(a) Write your Roll No. on the top immediately on receipt of this question paper.

(b) Attempt any **two** parts from each question.

1. (a) Define a metric space. Let $p \geq 1$. Define $d_p : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ as $d_p(x,y) = \left(\sum_{i=1}^{n} |x_i - y_i|^p\right)^{1/p}$, $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{R}^n$. Show that $(\mathbb{R}^n, d_p)$ is a metric space.

(b) When is a metric space said to be complete ? Is discrete metric space complete ? Justify. 6.5

(c) Let (X, d) be a metric space. Define $d_1 : X \times X \to \mathbb{R}$ by $d_1(x,y) = \frac{d(x,y)}{1+d(x,y)}$, for all $x, y \in X$. Prove that d_1 is a metric on X and d_1 is equivalent to d. 6.5

2. (a) Prove that every open ball in a metric space (X, d) is an open set in (X, d). What about the converse ? Justify. 6

(b) Define a homeomorphism from a metric space (X, d_1) to a metric space (Y, d_2). Show that the function $f : \mathbb{R} \to]-1, 1[$ defined by $f(x) = \frac{x}{1+|x|}$ is a homeomorphism. 6

(c) Let (X, d) be a metric space and let A, B be non-empty subsets of X. Prove that : 6

(i) $(A \cap B)^0 = A^0 \cap B^0$

(ii) $\overline{A \cup B} = \bar{A} \cup \bar{B}$

3. (a) Let (X, d) be a metric space and $F \subseteq X$. Prove that the following statements are equivalent : 6

(i) $x \in \bar{F}$

(ii) $S(x, \varepsilon) \cap F \neq \phi$, for every open ball $S(x, \varepsilon)$ centred at x

(iii) There exists an infinite sequence $\{x_n\}$ of point (not necessarily distinct) of F such that $x_n \to X$.

(b) Let (X,d) be a metric space and $F \subseteq X$. Prove that F is closed in X if and only if F^c is open in X, where F^c is complement of F in X. 6

(c) Let (X,d) be a metric space such that for every nested sequence $\{F_n\}_{n\geq 1}$ of non-empty closed subsets of X satisfying $d(F_n) \to 0$ as $n \to \infty$, the intersection $\bigcap_{n=1}^{\infty} F_n$ contains exactly one point. Prove that (X,d) is complete. 6

4. (a) Let f be a mapping from a metric space (X, d_1) to a metric space (Y, d_2). Prove that f is continuous on X if and only if $f^{-1}(G)$ is open in X for all open subsets G of Y. 6.5

(b) Let (X, d_1) and (Y, d_2) be two metric spaces. Prove that the following statements are equivalent : 6.5

(i) f is continuous on X

(ii) $\overline{f^{-1}(B)} \subseteq f^{-1}(\overline{B})$, for all subsets B of Y

(iii) $f(\overline{A}) \subseteq \overline{f(A)}$, for all subsets A of X.

(c) Define uniform continuity of a function f from a metric space (X, d_1) to a metric space (Y, d_2). Let (X, d) be a metric space and A be a non-empty subset of X. Show that the function $f : (X, d) \to \mathbb{R}$ defined as $f(x) = d(x, A)$, for all $x \in X$, is uniformly continuous on X. 6.5

5. (a) State and prove contraction mapping theorem. 6

(b) (i) Let Y be a non-empty subset of a metric space (X, d) and (Y, d_y) be complete, where d_y is restriction of d to $Y \times Y$. Prove that Y is closed in X. 3

(ii) Let A be a non-empty bounded subset of a metric space (X, d). Prove that $d(A) = d(\bar{A})$. 3

(c) Let (X, d) be a metric space. Then prove that following statements are equivalent : 1.5×4=6

(i) (X, d) is disconnected.

(ii) There exist two non-empty disjoint subsets A and B, both open in X, such that $X = A \cup B$.

(iii) There exist two non-empty disjoint subsets A and B, both closed in X, such that $X = A \cup B$.

(iv) There exists a proper subset of X, which is both open and closed in X.

6. (a) Let ($\mathbb{R}$, d) be the space of real numbers with the usual metric. Show that a connected subset of $\mathbb{R}$ must be an interval. Give example of two connected subsets of $\mathbb{R}$ such that their union is disconnected. 6.5

(b) Let (X, d) be a metric space and Y be a subset of X. If Y is compact subset of (X, d), then prove that Y is closed. 6.5

(c) Let f be a continuous function from a compact metric space (X, d_1) to a metric space (Y, d_2). Prove that f is uniformly continuous on X. 6.5

(20)

[This question paper contains 4 printed pages]

Your Roll No. : 2019

Sl. No. of Q. Paper : **7467** **J**

Unique Paper Code : 32351502

Name of the Course : **B.Sc.(Hons.) Mathematics**

Name of the Paper : Group Theory - II

Semester : V

Time : 3 Hours ***Maximum Marks : 75***

Instructions for Candidates :

(a) Write your Roll No. on the top immediately on receipt of this question paper.

(b) Attempt any **two** parts from each question.

(c) All questions carry equal marks.

1. (a) Let Inn (D_8) denotes the group of inner automorphisms on the dihedral group D_8 of order 8. Find Inn (D_8). 6

(b) Define inner automorphism of a group G induced by $g \in G$. Then prove that the set Inn(G) of all inner automorphism of a group G is a normal subgroup of the group Aut(G) of all automorphisms of G. 2+4

P.T.O.

(c) Let G be a cyclic group of order n. Then prove that Aut(G) is isomorphic to U(n). Here Aut(G) denotes the group of automorphisms on G and $U(n) = \{m \in N : m < n \text{ and } \gcd(m, n) = 1\}$ is a group under multiplication modulo n. 6

2. (a) Prove that every characteristic subgroup of a group G is a normal subgroup of G. Is the converse true ? Justify. 4+2

(b) Let G_1 and G_2 be finite groups. If $(g_1, g_2) \in G_1 \oplus G_2$, then prove that

$$|(g_1, g_2)| = \text{lcm}(|g_1|, |g_2|)$$

where $|g|$ denotes order of an element g in a group G. 6

(c) Prove that D_8 and S_3 cannot be expressed as an internal direct product of two of its proper subgroups. Here D_8 and S_3 denote the dihedral group of order 8 and the symmetric group on the set {1, 2, 3} respectively. 3+3

3. (a) State Fundamental Theorem for Finite Abelian Groups. Find all Abelian groups (upto isomorphism) of order 1176. 2+4

(b) Let G be an Abelian group of order 120 and G has exactly three elements of order 2. Determine the isomorphism class of G. 6

(c) For a group G, let the mapping from $G \times G \to G$ be defined by $(g, a) \to gag^{-1}$. Then prove that this mapping is a group action of G on itself. Also, find kernel of this action and the stabilizer G_x of an element $x \in G$. 2+2+2

4. (a) Let G={1,a,b,c} be the Klein 4-group. Label the group elements 1,a,b,c as integers 1,2,3,4 respectively. Compute the permutation σ_a, σ_b and σ_c induced by the group element a, b, c respectively under the group action of G on itself by left multiplication. 6.5

(b) Let G act on a set A. If $a,b \in A$ and $b=g.a$ for some $g \in G$, then prove that $G_b = gG_ag^{-1}$ where G_a is the stabilizer of a . Deduce that if G acts transitively on A then kernel of the action is $\bigcap_{g \in G} g\, G_a\, g^{-1}$. 3+3.5

(c) Let G be a group acting on a non empty set A and $a \in A$. Then prove that the number of elements in orbit containing a is equal to index of the stabilizer of a. 6.5

5. (a) State the class equation for finite groups. Find conjugacy classes of the quaternion group Q_8 and hence verify the class equation for Q_8. 2+3+1.5

(b) Let p be a prime and P be a group of prime power order p^α for some $\alpha \geq 1$. Then prove that P has a non trivial centre. Deduce that a group of order p^2 is an Abelian group. 4+2.5

(c) Let G be a non-Abelian group of order 231. Then prove that a Sylow 11-subgroup is normal and is contained in the centre of G. 2.5+4

6. (a) Let G be a group of order pq such that $p < q$ and p does not divide (q -1). Then prove that G is a cyclic group. Hence deduce that a group of order 33 is cyclic. 4.5+2

(b) Define a simple group. Prove that groups of order 72 and 56 are not simple. 1 + 2.5 + 3

(c) Let G be a group such that $|G|=2n$, where $n \geq 3$ is an odd integer. Then prove that G is not simple. 6.5

This question paper contains **8** printed pages]

Roll No. | | | | | | | | 2 | 0 | 1 | 9 |

S. No. of Question Paper : **7945** (21)

Unique Paper Code : **32357505** **J**

Name of the Paper : **Discrete Mathematics**

Name of the Course : **B.Sc. (Hons.) Mathematics : DSE-1**

Semester : **V**

Duration : **3 Hours** Maximum Marks : **75**

(Write your Roll No. on the top immediately on receipt of this question paper.)

Do any *two* parts from each question.

SECTION I

1. (*a*) (*i*) Let N_0 be the set of non-negative integers. Define a relation $\leq$ on N_0 as :

For $m, n \in N_0$, $m \leq n$ if m divides n, that is, if there exists $k \in N_0 : n = km$, then show that $\leq$ is an order relation on N_0.

(*ii*) Draw Hasse diagram for the subset $P = \{1, 2, 3, 12, 18, 0\}$ of $(N_0; \leq)$, where $\leq$ same as defined above. 3+3

(*b*) Show that two finite ordered sets P and Q are order isomorphic iff they can be drawn with identical diagrams. 6

(*c*) Let P and Q be ordered sets. Then show that the ordered sets P and Q are order isomorphic iff there exist order preserving maps $\varphi : P \to Q$ and $\psi : Q \to P$ such that :

$\varphi o \psi = id_Q$ and $\psi o \varphi = id_P$ where $id_S : S \to S$ denotes the identity map on S given by : $id_S(x) = x$, $\forall\, x \in S$. 6

2. (*a*) Let $(L, \wedge, \vee)$ be a non-empty set equipped with two binary operations $\wedge$ and $\vee$. Also L is such that the following laws, associative law, commutative law, idempotency law and absorption law and their duals hold. Then show that :

(*i*) $(a \vee b) = b$ iff $(a \wedge b) = a (\forall\, a, b \in L)$

(*ii*) Define a relation $\leq$ on L as $a \leq b$ if $(a \vee b) = b$. Then prove that $\leq$ is an order relation on L. 6.5

(*b*) Let L and K be lattices and $f : L \to K$ be a map. Then show that the following are equivalent :

(*i*) f is order preserving

(*ii*) $(\forall\ a, b, \in L)\ f(a \vee b) \geq f(a) \vee f(b)$. 6.5

(*c*) Prove that in any lattice L, we have :

$((x \wedge y) \vee (x \wedge z)) \wedge ((x \wedge y) \vee (y \wedge z)) = x \wedge y$

$(\forall\ x, y, z \in L)$. 6.5

SECTION II

3. (*a*) Let L be a lattice. Prove that L is distributive if and only if for all elements a, b, c of L,

$(a \vee b = c \vee b$ and $a \wedge b = c \wedge b)$ implies $a = c$. 6

(*b*) Find the conjunctive normal form of $f = (x(y' + z)) + z'$ in three variables. Also find its disjunctive normal form. 6

(*c*) Prove that every Boolean algebra is sectionally complemented. 6

4. (*a*) Find the prime implicants of $xy + xy'z + x'y'z$ and form the corresponding prime implicant table. 6.5

(*b*) Simplify the following function using the Karnaugh diagram : 6.5

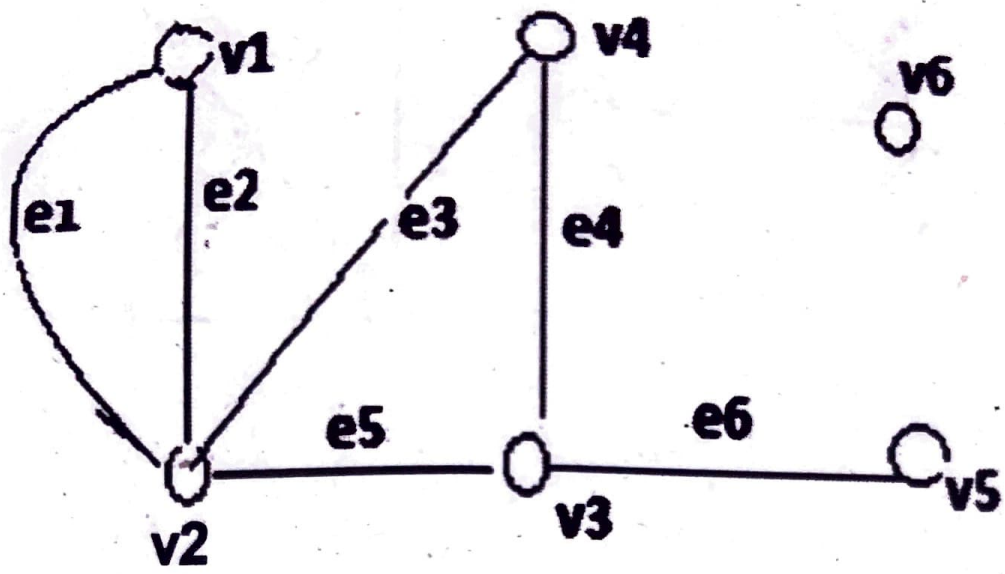
$$x_1x_2x'_3 + x'_1x_2x'_3 + (x_1 + x'_2x'_3)(x_1 + x_2 + x_3)' + x_3(x'_1 + x_2).$$

(*c*) A motor is supplied by three generators. The operation of each generator is monitored by a corresponding switching element which closes a circuit as soon as generator fails. In the electrical monitoring system, a warning lamp lights up if one or two generators fail. Determine a symbolic representation as a mathematical model of this problem. 6.5

SECTION III

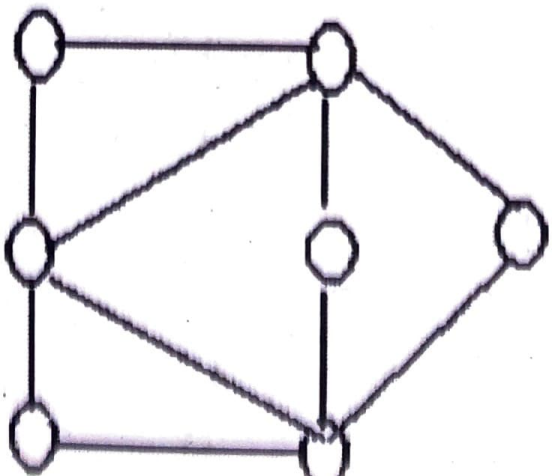
5. (*a*) (*i*) Prove that number of odd vertices in a pseudo graph is even.

(*ii*) Find the degree sequence for G; verify that the sum of the degrees of the vertices is an even number. Which vertices are even ? Which are odd ?

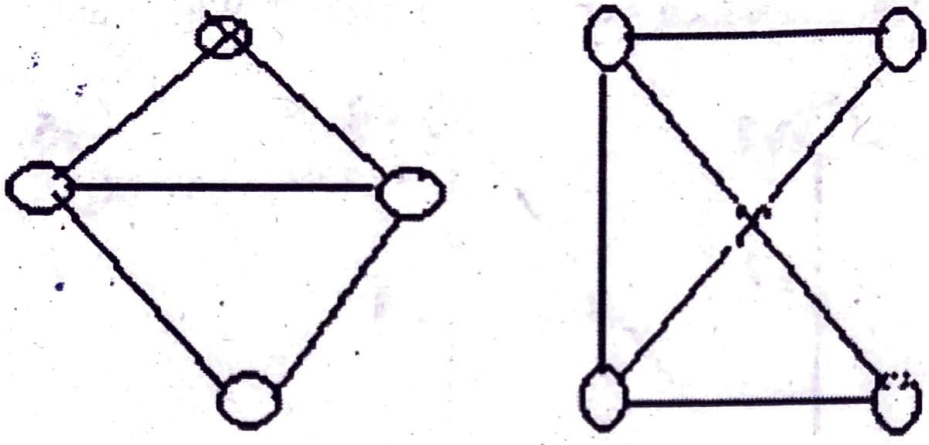


2+4

(*b*) (*i*) What is bipartite graph ? Determine whether the graph given below is bipartite or not. Give the bipartition sets or explain why the graph is not bipartite.



(*ii*) Define isomorphism of graph. Also label the graphs so as to show an isomorphism.

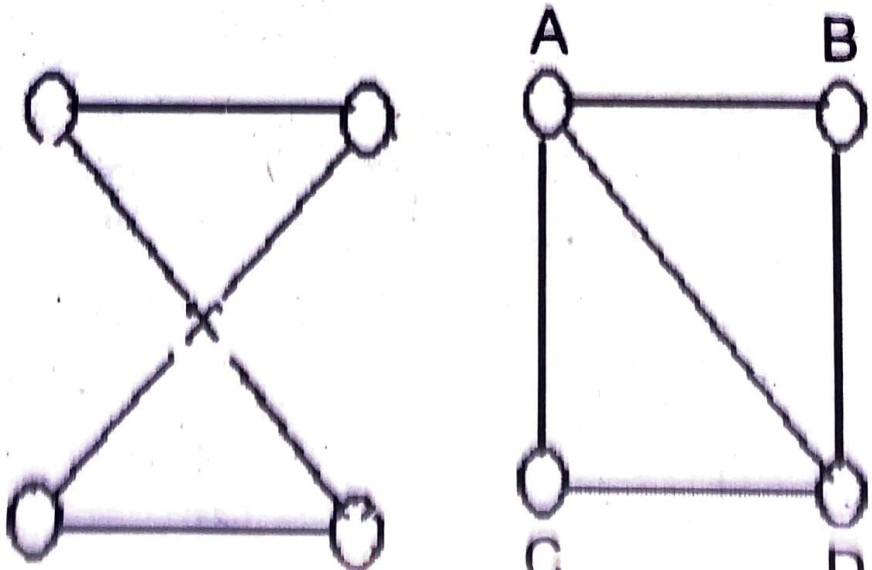


3+3

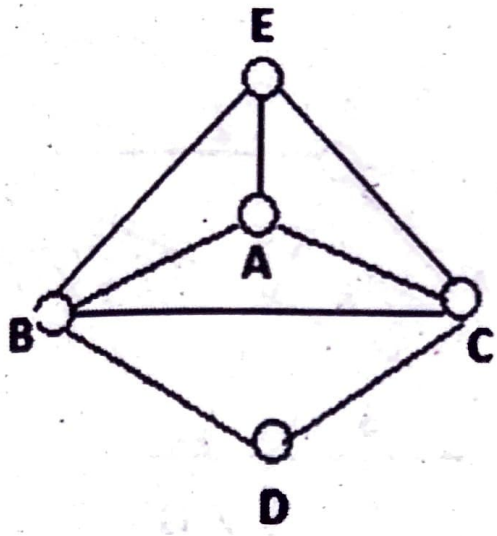
(*c*) (*i*) A graph has five vertices of degree 4 and two vertices of degree 2. How many edges does it have ?

(*ii*) Why can there not exist a graph whose degree sequence is 5, 4, 4, 3, 2, 1.

(*iii*) Explain why the graphs are not isomorphic.

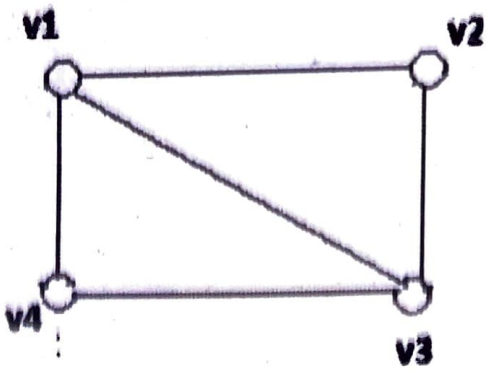


6. (*a*) (*i*) Define Hamiltonian graph. Is the graph given below Hamiltonian ? If no, explain. If yes, find a Hamiltonian cycle.

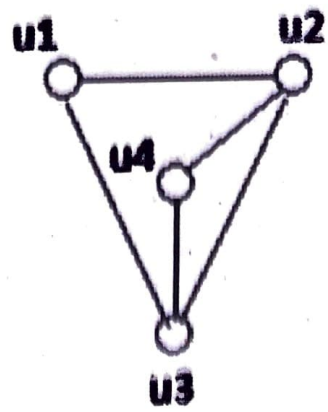


(*ii*) Answer the Konisberg bridge problem and explain. 6.5

(*b*) Find the adjacency matrices A_1 and A_2 of the graphs G_1 and G_2 as shown below. Find a permutation matrix P such that $A_2 = PA_1P^T$.



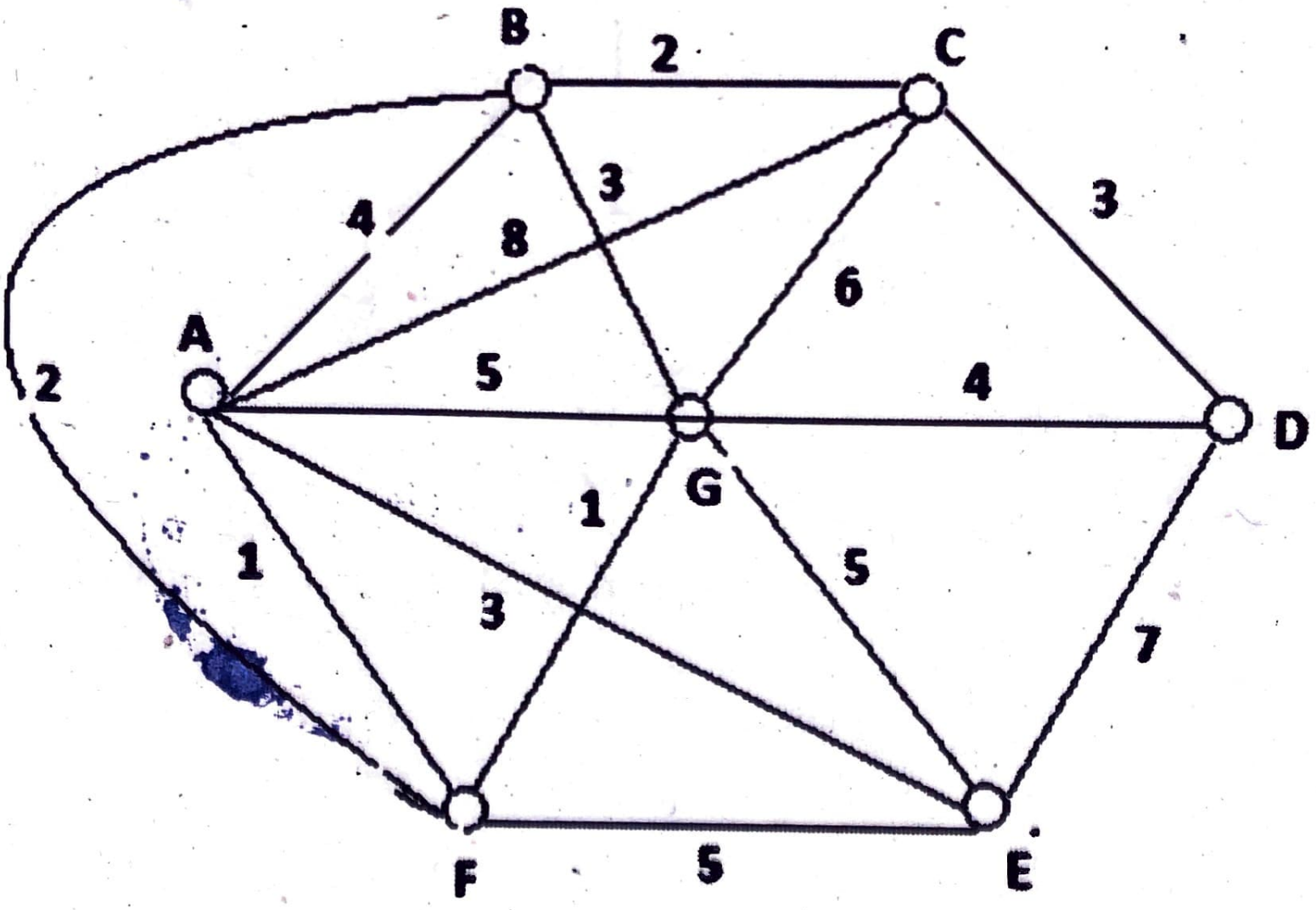
G_1



G_2

6.5

(c) Apply the improved version of Dijkstra's algorithm to find the length of a shortest path from A to D in the graph shown below. Write steps.



6.5

This question paper contains 4+1 printed pages]

Roll No. | | | | | | | | 2 | 0 | 1 | 9 |

22

S. No. of Question Paper : **7946**

Unique Paper Code : **32357506** **J**

Name of the Paper : **Cryptography and Network Security**

Name of the Course : **B.Sc. (Hons.) Mathematics : DSE-1**

Semester : **V**

Duration : **3 Hours** Maximum Marks : **75**

(Write your Roll No. on the top immediately on receipt of this question paper.)

All questions are compulsory.

Attempt any *five* parts from question **1**, each part carries **3** marks.

Attempt any *two* parts from questions **2** to **6**, each part carries **6** marks.

1. (*a*) Define a stream cipher. State the *three* important design considerations for a stream cipher.

(*b*) Briefly describe ShiftRows transformation of AES.

(*c*) What is an Avalanche effect ? Does DES show avalanche effect ? Justify your answer.

5. (*a*) Perform encryption and decryption using the RSA algorithm for $p = 5$, $q = 7$, $e = 7$ and $M = 12$.

(*b*) Consider the following Key exchange mechanism known a *Elliptic Curve Key exchange* :

Step 1 : Alice and Bob chooses an elliptic curve $y^2 = x^3 + rx + s$ over the field GF(p), p is prime with an element G of order n on this curve.

Step 2 : Alice chooses secret $a < n$ and sends a.G to Bob.

Step 3 : Bob chooses secret $b < n$ and sends b.G to Alice.

Step 4 : Alice calculates $a.(b.G) = abG$.

Step 5 : Bob calculates $b.(a.G) = abG$. Thus Alice and Bob have same shared secret key abG.

Suppose Alice and Bob chooses an elliptic curve $y^2 = x^3 + x + 6$ over the field GF(11) and G = (2, 7) on this curve. Alice and Bob selected secret keys $a = 2$, $b = 3$ respectively. Given 3G = (8, 3), find the secret key shared by Alice and Bob

(*c*) Through help of a diagram show how hash function can be used to achieve integrity, authentication and confidentiality using only a symmetric key encryption scheme.

(*a*) Describe the Elgamal Digital signature scheme, that is, its public/private parameters, signing algorithm and verification algorithm.

(*b*) Write the services provided by PGP. Mention the different Symmetric key schemes, Public Key schemes and Hash function used in PGP.

(*c*) Describe a hash function. What is the main functionality of a hash function in a cryptographic secure communication mechanism ? Give *three* applications of hash functions, clearly specifying role of hash function in each application.

This question paper contains 4+1 printed pages]

Roll No. | | | | | | | | 2 | 0 | 1 | 9 |

(23)

S. No. of Question Paper : **8081**

Unique Paper Code : **32357501** **J**

Name of the Paper : **Numerical Methods**

Name of the Course : **B.Sc. (H) Mathematics : DSE-2**

Semester : **V**

Duration : **3 Hours** Maximum Marks : **75**

(Write your Roll No. on the top immediately on receipt of this question paper.)

All the *six* questions are compulsory.

Attempt any *two* parts from each question.

Marks are indicated against each question.

Use of Non-Programmable Scientific Calculator is allowed.

1. (*a*) A real root of the equation $x^3 - 5x + 1 = 0$ lies in $]0, 1[$. Perform three iterations of Regula Falsi Method to obtain the root. 6

(b) Perform three iteration of Bisection Method to obtain root of the equation $\cos(x) - xe^x$ in $]0, 1[$. 6

(c) Discuss the order of convergence of the Secant method and give the geometrical interpretation of the method. 6

2. (a) Verify $x = \sqrt{a}$ is a fixed point of the function $h(x) = \frac{1}{2}\left(x + \frac{a}{x^2}\right)$. Determine order of convergence of sequence $p_n = h(p_{n-1})$ towards $x = \sqrt{a}$. 6.5

(b) Use Secant method to find root of $3x + \sin(x) - e^x = 0$ in $]0, 1[$. Perform three iterations. 6.5

(c) Prove that Newton's Method is of order two using $x^3 + 2x^2 - 3x - 1 = 0$ and initial approximation $x_0 = 2$. 6.5

3. (a) Define a lower and an upper triangular matrix. Solve the system of equations :

$$-3x_1 + 2x_2 - x_3 = -12$$

$$6x_1 + 8x_2 + x_3 = 1$$

$$4x_1 + 2x_2 + 7x_3 = 1$$

by obtaining an LU decomposition of the coefficient matrix A of the above system. 6

(b) For Jacobi method, calculate T_{jac}, C_{jac} and spectral radius of the following matrix :

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$ 6

(c) Set up the Gauss-Seidel iteration scheme to solve the system of equations :

$$4x_1 + 2x_2 - x_3 = 1$$

$$2x_1 + 4x_2 + x_3 = -1$$

$$-x_1 + x_2 + 4x_3 = 1$$

Take the initial approximation as $X^{(0)} = (0, 0, 0)$ and do three iterations. 6

4. (a) Construct the Lagrange form of the interpolating polynomial from the following data :

x	1	2	3
$f(x) = \ln x$	ln 1	ln 2	ln 3

6.5

(*b*) Prove that for $n + 1$ distinct nodal points $x_0, x_1, x_2, \ldots x_n$, there exists a unique interpolating polynomial of at most degree n. 6.5

(*c*) Find the maximum value of the step size h that can be used in the tabulation of $f(x) = e^x$ on the interval $[0, 1]$ so that the error in the linear interpolation of $f(x)$ is less than 5×10^{-4}. 6.5

5. (*a*) Define the backward difference operator ∇ and the Newton divided difference. Prove that :

$$f[x_0, x_1, -----, x_n] = \frac{\nabla^n f_n}{n! h^n} \text{ where } h = x_{i+1} - x_i . \quad 6$$

(*b*) Construct the divided difference table for the following data set and then write out the Newton form of the interpolating polynomial :

x	–7	–5	–4	–1
y	10	5	2	10

Find the approximation of y for $x = -3$. 6

(c) Use the formula

$$f'(x_0) \approx \frac{f(x_0+h)-f(x_0)}{h}$$

to approximate the derivative of $f(x)=1+x+x^3$ at $x_0 = 1$ taking $h = 1, 0.1, 0.001$. What is the order of approximation ? 6

(a) Approximate the value of $\int_0^1 e^{-x}dx$ using the Trapezoidal rule and verify that the theoretical error bound holds for the same. 6.5

(b) State Simpson's 1/3rd rule for the evaluation of $\int_a^b f(x)dx$ and prove that it has degree of precision 3. 6.5

(c) Use Euler's method to approximate the solution of the initial value problem.

$x' = (1+x^2)/t$, $x(1) = 0$, $1 \le t \le 4$ taking 5 steps. 6.5

This question paper contains 4+1 printed pages]

Roll No. | | | | | | | | 2 | 0 | 1 | 9 |

(24)

S. No. of Question Paper : **8086**

Unique Paper Code : **32357506** **J**

Name of the Paper : **Cryptography and Network Security**

Name of the Course : **B.Sc. (Hons) Mathematics : DSE-1**

Semester : **V**

Duration : **3 Hours** Maximum Marks : **75**

(Write your Roll No. on the top immediately on receipt of this question paper.)

All questions are compulsory.

Attempt any *five* parts from question No. **1**, each part carries **3** marks.

Attempt any *two* parts from questions **2** to **6**, each part carries **6** marks.

1. (*a*) Use the Rail fence cipher of depth 3 to encrypt "there could be better questions." Which attack is this cipher vulnerable to ?

(*b*) Explain the term diffusion in the context of a block cipher. How does DES achieve diffusion ?

(*c*) What is the difference between a stream cipher and a block cipher ?

(*d*) Describe a trap-door-one-way function.

(*e*) Define Euler totient function ϕ. Compute ϕ (105).

(*f*) Write the order in which Compression, Encryption and Digital Signatures are applied in PGP, while achieving both Authentication and Confidentiality, clearly state the reason behind this order.

(*g*) Describe the terms Non-Repudiation and Integrity in context of Cryptography. Mention the cryptographic primitives used to achieve these.

2. (*a*) Decrypt the following message encrypted using playfair cipher with the key "HER MAJESTY'S SHIP".

LVHZ CRJE RQQO ZRTY ERGM JRRM XOJR RANF RMOW ODNM AHYN WDER NMFM.

(*b*) What does it mean to say that the one time pad is unbreakable ? If the one time pad is unconditionally secure, why is it not widely used ?

(*c*) Describe the key expansion algorithm of DES with the help of a diagram.

3. (*a*) For any positive integers a and n, show that $b \equiv c \ mod(n)$ implies $ab \equiv ac \ mod(n)$. Show that converse is not true in general. In which case converse is also true ?

(*b*) Determine the GCD of $x^4 + 2x^3 + 5x^2 + 5x + 4$ and $x^3 + 2x^2 + 3x + 6$ over GF(7).

(*c*) State Fermat's Theorem. Use Fermat's Theorem to reduce $8^{109} \pmod{37}$.

4. (*a*) Describe the general structure of the encryption process in AES with the help of a diagram. Briefly comment on the various transformations performed in each round.

(*b*) Suppose that we have the following 128-bit AES key, given in haxadecimal notation :

287E151628AED2A6ABF7158809CF4F3C

(*i*) Express the initial round key (w_0 w_1 w_2 w_3) as a State matrix.

(*ii*) Given that RC[1] = 01, S(09) = 01, S(CF) = 8A, S(4F) = 84 and S(3C) = EB, where S denotes the S-box, calculate the first four bytes (w_4) for round one.

(c) Define the discrete logarithm of a number b for the base a $(mod\ p)$. Prove that : $dlog_{a,p}\ (xy) = [dlog_{a,p}\ (x) + dlog_{a,p}\ (y)]\ (mod\ \phi(p))$.

5. (a) Perform encryption and decryption using the RSA algorithm for $p = 7$, $q = 13$, $e = 5$ and $M = 8$.

(b) The public parameters of Alice consists of an elliptic curve $y^2 = x^3 + x + 6$ over the field GF(11) and a point $G = (2, 7)$ on this curve. Suppose Alice's private key is $a = 2$. Bob sends the ciphertext ((8,3), (5,9)) to Alice. Find the message sent by Bob to Alice.

(c) For the elliptic curve $y^2 = x^3 + x + 6$ over the field GF(11) :

(i) Calculate P + Q, where P = (5,2), Q = (8, 3).

(ii) Calculate 2P, where P = (5,2).

6. (a) What is the maximum input size and length of output of hash function SHA-512. State the value of padding field and length fields if the message length is 1920 bits. What is the size of word (register used) in SHA-512 ?

(*b*) Alice uses Flgamal Digital signature scheme to sign a document with the parameters : A cyclic group GF(19) with generator $a = 10$ and private key $X = 16$. He generated the random $K = 5$, gcd $(K, 18) = 1$ as part of signing process. If Alice signed the document with hash value $m = 14$, claculate the signature.

(*c*) Define Digital Signatures, its parameters, input/output, and general working of signing and verification algorithms. Define three types of attacks on a Digital signature.

Sl. No. 07 QP: 8903

(25)

2019

Unique Paper Code: 235504

Name of the Paper: Algebra IV (MAHT-503)

Name of the Course: B.Sc. (Hons.) Mathematics, ~~Part-III~~

Semester: V

Duration : 3 Hours

Maximum Marks : 75

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. Attempt any five parts from Question 1. Each part carries three marks.
3. Attempt any two parts each from each of Questions 2 to 6. Each part carries six marks.

1. (a) Show that $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$ is basis of $Q(\sqrt{3}, \sqrt{5})$ over Q.

(b) Prove that $\sin\theta$ is constructible if and only if $\cos\theta$ is constructible.

(c) If β is a zero of the polynomial $x^2 + x + 2$ over Z_5, show that the other zero is $4\beta + 4$.

(d) Let T be a linear operator on $P_2(\mathbb{R})$ defined by $T(f(x)) = f(x) + (x+1)f'(x)$. Find the characterstic polynomial of T.

(e) Let T be a linear operator on the vector space $P(\mathbb{R})$ defined by $T(f(x)) = f'(x)$. Determine the T-cyclic subspace generated by $x^2 \in P(\mathbb{R})$.

(f) Let T be a linear operator on $\mathbb{R}^2$ defined by $T(a, b) = (a + b,\ a - b)$. Determine the minimal polynomial of T.

(g) Let T be a linear operator on an inner product space V. If $\|T(x)\| = \|x\|$, for all $x \in V$, prove that T is one to one.

(h) Let $W = \text{span}(\{(i,\ 0,\ 1)\})$ be a subspace of the inner product space $\mathbb{C}^3$. Compute $W^{\perp}$.

2. (a) Prove that a polynomial $f(x)$ over a field F has multiple zeros in some extension E of F if and only if both $f(x)$ and $f'(x)$ have a common factor of positive degree in $F[x]$.

(b) Prove that $Q(\sqrt{2+3}) = Q(\sqrt{2}, \sqrt{3})$.

(c) Let a be algebraic over F and, let $p(x)$ be the minimal polynomial for the element a over F. Show that if $f(x) \in F[x]$ and $f(a) = 0$, then $p(x)$ divides $f(x)$ in $F[x]$.

3. (a) Let K be a finite extension of the field E and E be a finite extension of the field F. Prove that K is a finite extension of F and $[K : F] = [K : E]\ [E : F]$.

(b) Prove that $\cos 2\theta$ is constructible if and only if $\cos\theta$ is constructible.

(c) Show that a regular 9-gon cannot be constructed with a straightedge and compass.

4. (a) Let $V = P_1(\mathbb{R})$. For $p(x) \in V$, let $f_1, f_2 \in V^*$ be defined as

$$f_1(p(x)) = \int_0^1 p(t)dt \text{ and } f_2(p(x)) = \int_0^2 p(t)dt.$$

Prove that $\{f_1, f_2\}$ forms a basis for V^*, and find a basis for V for which it is the dual basis.

(b) Test the diagonalizability of the matrix given by

6. (a) Let V be an inner product space over F. Prove that

$$|\langle x, y\rangle| \leq \|x\| \, \|y\|, \text{ for all } x, y \in V.$$

Also, verify the above inequality for vectors $x = (2, 1+i, i)$ and $y = (2-i, 2, 1+2i)$ in $\mathbb{C}^3$.

(b) For the data $\{(-3, 9), (-2, 6), (0, 2), (1, 1)\}$, use the least squares approximation method to obtain the linear function of best fit.

(c) Let V be a finite dimensional inner product space and let W be a subspace of V. Prove that $V = W \oplus W^{\perp}$, where $W^{\perp}$ denotes the orthogonal complement of W.

(26)

Roll No 2019

Sr. No. of Question Paper: 8904

Unique Paper Code :235505

Name of the Course :BSc(Hons) Mathematics

Name of the Paper : Linear Programming and Theory of Games

Semester : V

Duration: 3 Hours

Maximum Marks: 75

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. Attempt any two parts of each question.
3. All questions carry equal marks.

1.(a) If for a basic feasible solution $x_B = B^{-1}b$ to the linear programming problem:

Minimize $z = cx$

$Ax = b$

$x \geq 0$

there is some column x_j in A but not in B for which $z_j - c_j > 0$ and $y_{ij} \leq 0$, then prove that the problem has an unbounded solution.

(b) Let $x_1 = 2$, $x_2 = 3$, $x_3 = 1$ is a feasible solution of the system of equations

$$2x_1 + x_2 + 4x_3 = 11$$

$$3x_1 + x_2 + 5x_3 = 14$$

Reduce this feasible solution to a basic feasible solution.

(c) Solve the following LPP using Simplex method:

Max $z = 10x_1 + x_2 + 2x_3$

Subject to

$$x_1 + x_2 - 2x_3 \leq 10$$

$$4x_1 + x_2 + x_3 \leq 20$$

$x_1, x_2 \geq 0$, x_3 unrestricted.

2) (a) Solve the linear programming problem by Big M method.

Max $z = 3x_1 - x_2$

Subject to

$$2x_1 + x_2 \geq 2$$

$$x_1 + 3x_2 \leq 3$$

$$x_2 \leq 4$$

$$x_1, x_2 \geq 0.$$

(b) Use Simplex method to solve the system of equation:

$$3x_1 + 2x_2 = 5$$

$$2x_1 + x_2 = 4$$

(c) Find the dual of the following LPP

Minimize $Z = x_1 + x_2 + 2x_3$

subject to $x_1 + x_2 + x_3 \leq 9$

$$2x_1 - 3x_2 + 3x_3 \geq 1$$

$$-3x_1 + 6x_2 - 4x_3 = 3$$

$x_1 \leq 0, x_2 \geq 0, x_3$ unrestricted.

3 (a) Solve the following LPP by Two Phase method.

Max $z = x_1 + 5x_2$

Subject to

$$3x_1 + 4x_2 \leq 6$$

$$x_1 + 3x_2 \geq 2$$

$$x_1, x_2 \geq 0.$$

(b) State and prove Strong Duality theorem.

(c) Apply the principle of duality to solve the linear programming problem

Minimize $x = 3x_1 + 2x_2$

Subject to $x_1 + x_2 \geq 1$

$$x_1 + x_2 \leq 7$$

$$x_1 + 2x_2 \leq 10$$

$$x_2 \leq 3$$
$$x_1, x_2 \geq 0$$

4) (a) Solve the following cost-minimizing transportation problem:

	D_1	D_2	D_3	Supply
O_1	6	8	4	14
O_2	4	9	3	12
O_3	6	10	15	5
Demand	6	10	15	

(b) Minimize the total man hours in the following assignment matrix by Hungarian method.

	I	II	III	IV	V
A	11	17	8	16	20
B	9	7	12	6	15
C	13	16	15	12	16
D	21	24	17	28	26
E	14	10	12	11	15

(c) Define saddle point of a two person zero sum game. Use the minimax criteria to find the best strategy for each player for the game having the following pay off matrix

Player II

$$\text{Player I} \begin{bmatrix} 1 & -1 \\ -2 & 0 \\ 3 & 1 \end{bmatrix}$$

Is it a stable game?

5) (a) Solve graphically the game whose payoff matrix is

$$\begin{bmatrix} 2 & 4 & 11 \\ 7 & 4 & 2 \end{bmatrix}$$

(b) Use the relation of dominance to solve the game whose payoff matrix is given by

$$\begin{bmatrix} 1 & 7 & 3 & 4 \\ 5 & 6 & 4 & 5 \\ 7 & 2 & 0 & 3 \end{bmatrix}$$

(c) Reduce the following game to a Linear Programming Problem and then solve by simplex method.

Shift at ← to the previous sheet.

$$\begin{bmatrix} 1 & -3 & 2 \\ -4 & 4 & -2 \end{bmatrix}$$

[This question paper contains 7 printed pages]

Your Roll No. : .....

Sl. No. of Q. Paper : **7466** **J**

Unique Paper Code : 32351501

Name of the Course : **B.Sc.(Hons.) Mathematics**

Name of the Paper : Metric Spaces

Semester : V

Time : 3 Hours ***Maximum Marks : 75***

Instructions for Candidates :

(a) Write your Roll No. on the top immediately on receipt of this question paper.

(b) Attempt any **two** parts from each question.

1. (a) Define a metric space. Let $p \geq 1$. Define $d_p : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ as $d_p(x,y) = \left(\sum_{i=1}^{n} |x_i - y_i|^p\right)^{1/p}$, $x (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{R}^n$. Show that $(\mathbb{R}^n, d_p)$ is a metric space.

6.5

(b) When is a metric space said to be complete ? Is discrete metric space complete ? Justify. 6.5

(c) Let (X, d) be a metric space. Define $d_1 : X \times X \to \mathbb{R}$ by $d_1(x,y) = \frac{d(x,y)}{1+d(x,y)}$, for all $x, y \in X$. Prove that d_1 is a metric on X and d_1 is equivalent to d. 6.5

2. (a) Prove that every open ball in a metric space (X, d) is an open set in (X, d). What about the converse ? Justify. 6

(b) Define a homeomorphism from a metric space (X, d_1) to a metric space (Y, d_2). Show that the function $f : \mathbb{R} \to]-1, 1[$ defined by $f(x) = \frac{x}{1+|x|}$ is a homeomorphism. 6

(c) Let (X, d) be a metric space and let A, B be non-empty subsets of X. Prove that : 6

(i) $(A \cap B)^0 = A^0 \cap B^0$

(ii) $\overline{A \cup B} = \bar{A} \cup \bar{B}$

3. (a) Let (X, d) be a metric space and $F \subseteq X$. Prove that the following statements are equivalent : 6

(i) $x \in \bar{F}$

(ii) $S(x, \varepsilon) \cap F \neq \phi$, for every open ball $S(x, \varepsilon)$ centred at x

(iii) There exists an infinite sequence $\{x_n\}$ of point (not necessarily distinct) of F such that $x_n \to X$.

(b) Let (X,d) be a metric space and $F \subseteq X$. Prove that F is closed in X if and only if F^c is open in X, where F^c is complement of F in X. 6

(c) Let (X,d) be a metric space such that for every nested sequence $\{F_n\}_{n \geq 1}$ of non-empty closed subsets of X satisfying $d(F_n) \to 0$ as $n \to \infty$, the intersection $\bigcap_{n=1}^{\infty} F_n$ contains exactly one point. Prove that (X,d) is complete. 6

4. (a) Let f be a mapping from a metric space (X, d_1) to a metric space (Y, d_2). Prove that f is continuous on X if and only if $f^{-1}(G)$ is open in X for all open subsets G of Y. 6.5

(b) Let (X, d_1) and (Y, d_2) be two metric spaces. Prove that the following statements are equivalent : 6.5

(i) f is continuous on X

(ii) $\overline{f^{-1}(B)} \subseteq f^{-1}(\bar{B})$, for all subsets B of Y

(iii) $f(\bar{A}) \subseteq \overline{f(A)}$, for all subsets A of X.

(c) Define uniform continuity of a function f from a metric space (X, d_1) to a metric space (Y, d_2). Let (X, d) be a metric space and A be a non-empty subset of X. Show that the function $f : (X, d) \to \mathbb{R}$ defined as $f(x) = d(x, A)$, for all $x \in X$, is uniformly continuous on X. 6.5

5. (a) State and prove contraction mapping theorem. 6

(b) (i) Let Y be a non-empty subset of a metric space (X, d) and (Y, d_y) be complete, where d_y is restriction of d to $Y \times Y$. Prove that Y is closed in X. 3

(ii) Let A be a non-empty bounded subset of a metric space (X, d). Prove that $d(A) = d(\bar{A})$. 3

(c) Let (X, d) be a metric space. Then prove that following statements are equivalent : 1.5×4=6

(i) (X, d) is disconnected.

(ii) There exist two non-empty disjoint subsets A and B, both open in X, such that $X = A \cup B$.

(iii) There exist two non-empty disjoint subsets A and B, both closed in X, such that $X = A \cup B$.

(iv) There exists a proper subset of X, which is both open and closed in X.

6. (a) Let ($\mathbb{R}$, d) be the space of real numbers with the usual metric. Show that a connected subset of $\mathbb{R}$ must be an interval. Give example of two connected subsets of $\mathbb{R}$ such that their union is disconnected. 6.5

(b) Let (X, d) be a metric space and Y be a subset of X. If Y is compact subset of (X, d), then prove that Y is closed. 6.5

(c) Let f be a continuous function from a compact metric space (X, d_1) to a metric space (Y, d_2). Prove that f is uniformly continuous on X. 6.5

[This question paper contains 4 printed pages]

Your Roll No. : .....

Sl. No. of Q. Paper : **7467** **J**

Unique Paper Code : 32351502

Name of the Course : **B.Sc.(Hons.) Mathematics**

Name of the Paper : Group Theory - II

Semester : V

Time : 3 Hours ***Maximum Marks : 75***

Instructions for Candidates :

(a) Write your Roll No. on the top immediately on receipt of this question paper.

(b) Attempt any **two** parts from each question.

(c) All questions carry equal marks.

1. (a) Let Inn (D_8) denotes the group of inner automorphisms on the dihedral group D_8 of order 8. Find Inn (D_8). 6

(b) Define inner automorphism of a group G induced by $g \in G$. Then prove that the set Inn(G) of all inner automorphism of a group G is a normal subgroup of the group Aut(G) of all automorphisms of G. 2+4

P.T.O.

(c) Let G be a cyclic group of order n. Then prove that Aut(G) is isomorphic to U(n). Here Aut(G) denotes the group of automorphisms on G and $U(n) = \{m \in N : m < n \text{ and } \gcd(m, n) = 1\}$ is a group under multiplication modulo n. 6

2. (a) Prove that every characteristic subgroup of a group G is a normal subgroup of G. Is the converse true ? Justify. 4+2

(b) Let G_1 and G_2 be finite groups. If $(g_1, g_2) \in G_1 \oplus G_2$, then prove that

$$|(g_1, g_2)| = \text{lcm}(|g_1|, |g_2|)$$

where $|g|$ denotes order of an element g in a group G. 6

(c) Prove that D_8 and S_3 cannot be expressed as an internal direct product of two of its proper subgroups. Here D_8 and S_3 denote the dihedral group of order 8 and the symmetric group on the set {1, 2, 3} respectively. 3+3

3. (a) State Fundamental Theorem for Finite Abelian Groups. Find all Abelian groups (upto isomorphism) of order 1176. 2+4

(b) Let G be an Abelian group of order 120 and G has exactly three elements of order 2. Determine the isomorphism class of G. 6

(c) For a group G, let the mapping from $G \times G \to G$ be defined by $(g, a) \to gag^{-1}$. Then prove that this mapping is a group action of G on itself. Also, find kernel of this action and the stabilizer G_x of an element $x \in G$. 2+2+2

4. (a) Let G={1,a,b,c} be the Klein 4-group. Label the group elements 1,a,b,c as integers 1,2,3,4 respectively. Compute the permutation σ_a, σ_b and σ_c induced by the group element a, b, c respectively under the group action of G on itself by left multiplication. 6.5

(b) Let G act on a set A. If $a,b \in A$ and b=g.a for some $g \in G$, then prove that $G_b = gG_ag^{-1}$ where G_a is the stabilizer of a . Deduce that if G acts transitively on A then kernel of the action is $\bigcap_{g \in G} g\, G_a\, g^{-1}$. 3+3.5

(c) Let G be a group acting on a non empty set A and $a \in A$. Then prove that the number of elements in orbit containing a is equal to index of the stabilizer of a. 6.5

5. (a) State the class equation for finite groups. Find conjugacy classes of the quaternion group Q_8 and hence verify the class equation for Q_8. 2+3+1.5

(b) Let p be a prime and P be a group of prime power order p^α for some $\alpha \geq 1$. Then prove that P has a non trivial centre. Deduce that a group of order p^2 is an Abelian group. 4+2.5

(c) Let G be a non-Abelian group of order 231. Then prove that a Sylow 11-subgroup is normal and is contained in the centre of G. 2.5+4

6. (a) Let G be a group of order pq such that $p < q$ and p does not divide $(q-1)$. Then prove that G is a cyclic group. Hence deduce that a group of order 33 is cyclic. 4.5+2

(b) Define a simple group. Prove that groups of order 72 and 56 are not simple. 1 + 2.5 + 3

(c) Let G be a group such that $|G|=2n$, where $n \geq 3$ is an odd integer. Then prove that G is not simple. 6.5

This question paper contains 8 printed pages]

Roll No. | | | | | | | | | | |

S. No. of Question Paper : **7945**

Unique Paper Code : **32357505** **J**

Name of the Paper : **Discrete Mathematics**

Name of the Course : **B.Sc. (Hons.) Mathematics : DSE-1**

Semester : **V**

Duration : **3 Hours** Maximum Marks : **75**

(Write your Roll No. on the top immediately on receipt of this question paper.)

Do any *two* parts from each question.

SECTION I

1. (*a*) (*i*) Let N_0 be the set of non-negative integers. Define a relation $\leq$ on N_0 as :

For $m, n \in N_0$, $m \leq n$ if m divides n, that is, if there exists $k \in N_0 : n = km$, then show that $\leq$ is an order relation on N_0.

(*ii*) Draw Hasse diagram for the subset $P = \{1, 2, 3, 12, 18, 0\}$ of $(N_0; \leq)$, where $\leq$ same as defined above. 3+3

(*b*) Show that two finite ordered sets P and Q are order isomorphic iff they can be drawn with identical diagrams. 6

(*c*) Let P and Q be ordered sets. Then show that the ordered sets P and Q are order isomorphic iff there exist order preserving maps $\varphi : P \to Q$ and $\psi : Q \to P$ such that :

$\varphi o \psi = id_Q$ and $\psi o \varphi = id_P$ where $id_S : S \to S$ denotes the identity map on S given by : $id_S(x) = x$, $\forall\, x \in S$. 6

2. (*a*) Let $(L, \wedge, \vee)$ be a non-empty set equipped with two binary operations $\wedge$ and $\vee$. Also L is such that the following laws, associative law, commutative law, idempotency law and absorption law and their duals hold. Then show that :

(*i*) $(a \vee b) = b$ iff $(a \wedge b) = a (\forall\, a, b \in L)$

(*ii*) Define a relation $\leq$ on L as $a \leq b$ if $(a \vee b) = b$. Then prove that $\leq$ is an order relation on L. 6.5

(*b*) Let L and K be lattices and $f : L \to K$ be a map. Then show that the following are equivalent :

(*i*) f is order preserving

(*ii*) $(\forall\ a, b, \in L)\ f(a \vee b) \geq f(a) \vee f(b)$. 6.5

(*c*) Prove that in any lattice L, we have :

$((x \wedge y) \vee (x \wedge z)) \wedge ((x \wedge y) \vee (y \wedge z)) = x \wedge y$

$(\forall\ x, y, z \in L)$. 6.5

SECTION II

(*a*) Let L be a lattice. Prove that L is distributive if and only if for all elements a, b, c of L,

$(a \vee b = c \vee b$ and $a \wedge b = c \wedge b)$ implies $a = c$. 6

(*b*) Find the conjunctive normal form of $f = (x(y' + z)) + z'$ in three variables. Also find its disjunctive normal form. 6

(*c*) Prove that every Boolean algebra is sectionally complemented. 6

4. (*a*) Find the prime implicants of $xy + xy'z + x'y'z$ and form the corresponding prime implicant table. 6.5

(*b*) Simplify the following function using the Karnaugh diagram : 6.5

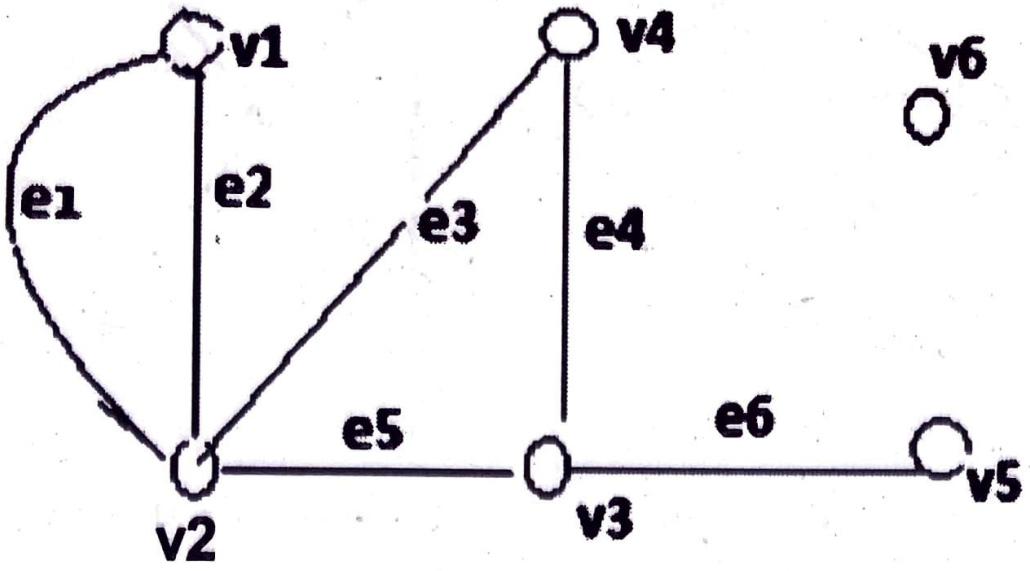
$$x_1x_2x'_3 + x'_1x_2x'_3 + (x_1 + x'_2x'_3)(x_1 + x_2 + x_3)' + x_3(x'_1 + x_2).$$

(*c*) A motor is supplied by three generators. The operation of each generator is monitored by a corresponding switching element which closes a circuit as soon as generator fails. In the electrical monitoring system, a warning lamp lights up if one or two generators fail. Determine a symbolic representation as a mathematical model of this problem. 6.5

SECTION III

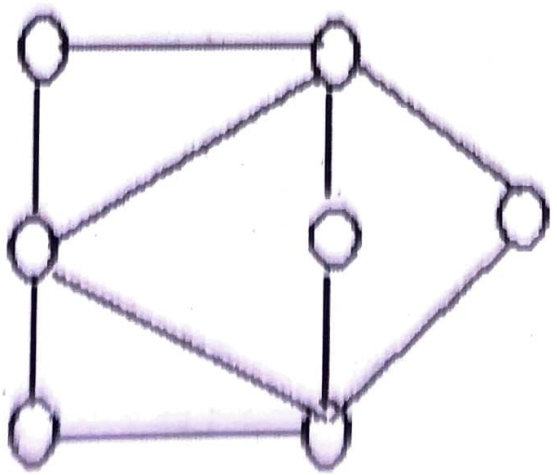
5. (*a*) (*i*) Prove that number of odd vertices in a pseudo graph is even.

(*ii*) Find the degree sequence for G; verify that the sum of the degrees of the vertices is an even number. Which vertices are even ? Which are odd ?

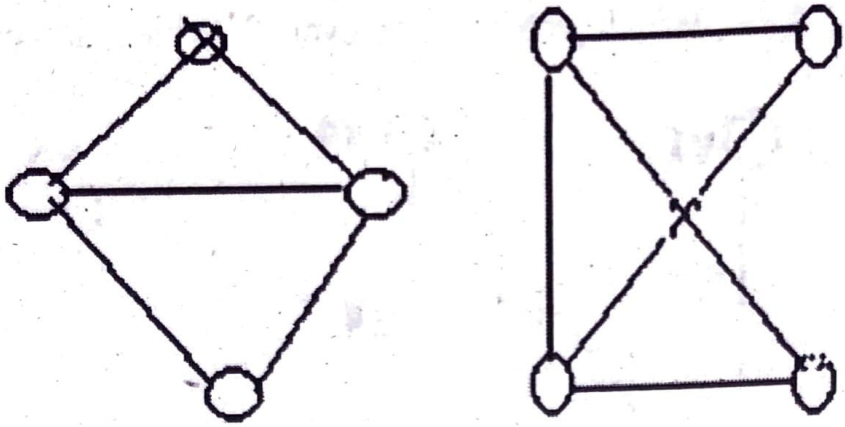


2+4

(*b*) (*i*) What is bipartite graph ? Determine whether the graph given below is bipartite or not. Give the bipartition sets or explain why the graph is not bipartite.



(*ii*) Define isomorphism of graph. Also label the graphs so as to show an isomorphism.

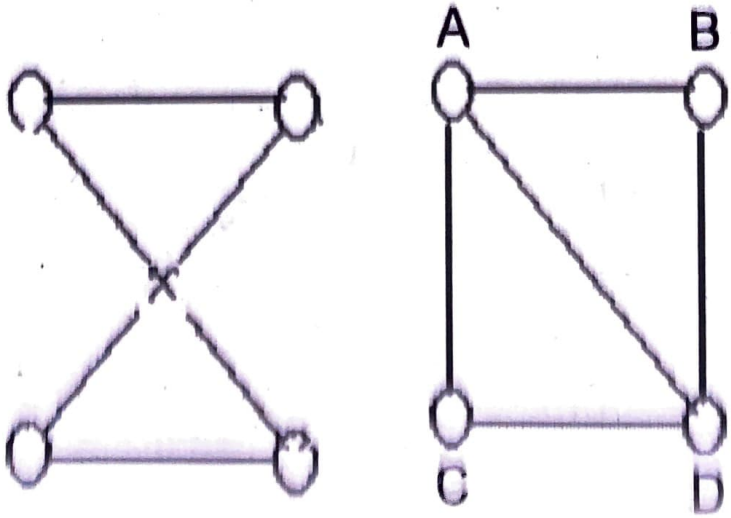


3+3

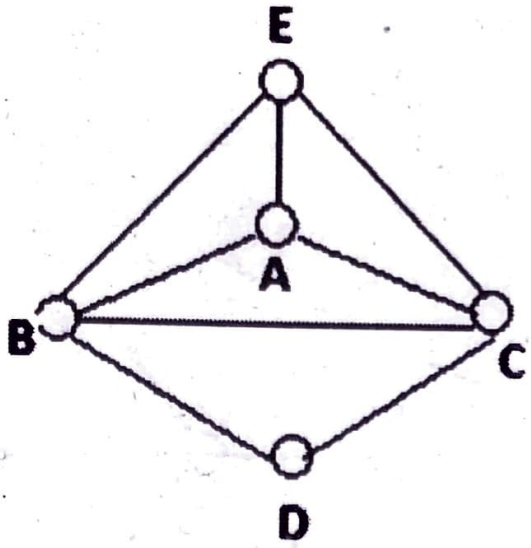
(*c*) (*i*) A graph has five vertices of degree 4 and two vertices of degree 2. How many edges does it have ?

(*ii*) Why can there not exist a graph whose degree sequence is 5, 4, 4, 3, 2, 1.

(*iii*) Explain why the graphs are not isomorphic.

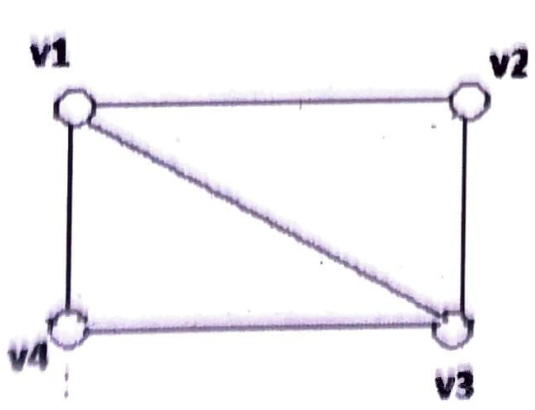


6. (*a*) (*i*) Define Hamiltonian graph. Is the graph given below Hamiltonian ? If no, explain. If yes, find a Hamiltonian cycle.

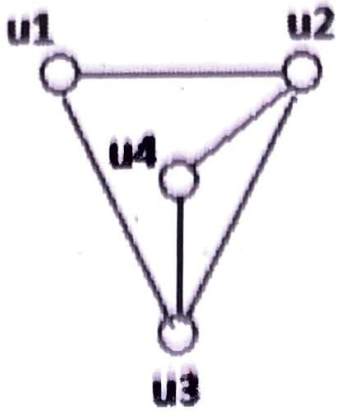


(*ii*) Answer the Konisberg bridge problem and explain. 6.5

(*b*) Find the adjacency matrices A_1 and A_2 of the graphs G_1 and G_2 as shown below. Find a permutation matrix P such that $A_2 = PA_1P^T$.



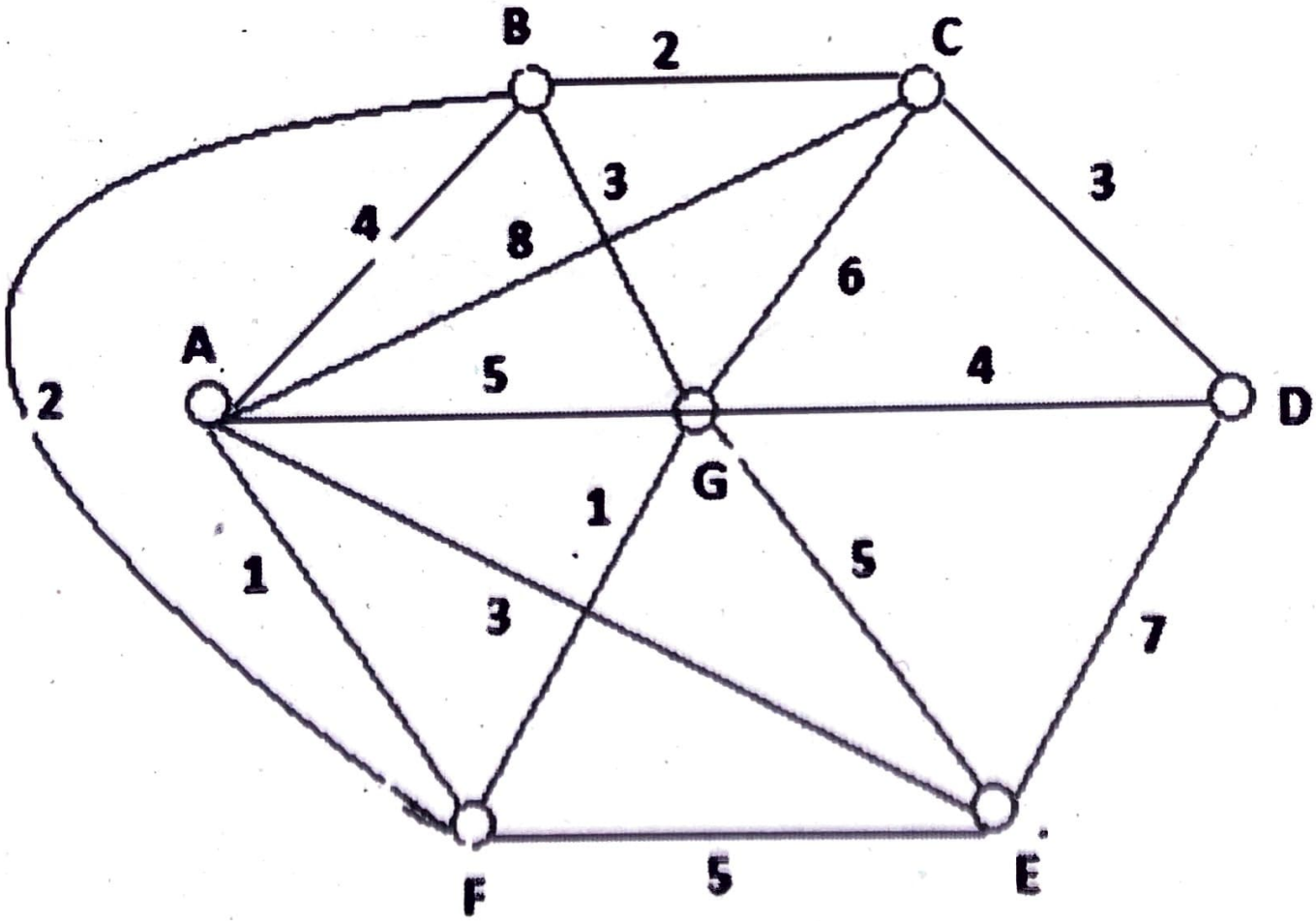
G_1



G_2

6.5

(*c*) Apply the improved version of Dijkstra's algorithm to find the length of a shortest path from A to D in the graph shown below. Write steps.



6.5

This question paper contains 4+1 printed pages]

Roll No. | | | | | | | | | | |

S. No. of Question Paper : **7946**

Unique Paper Code : **32357506** **J**

Name of the Paper : **Cryptography and Network Security**

Name of the Course : **B.Sc. (Hons.) Mathematics : DSE-1**

Semester : **V**

Duration : **3 Hours** Maximum Marks : **75**

(Write your Roll No. on the top immediately on receipt of this question paper.)

All questions are compulsory.

Attempt any *five* parts from question **1**, each part carries **3** marks.

Attempt any *two* parts from questions **2** to **6**, each part carries **6** marks.

1. (*a*) Define a stream cipher. State the *three* important design considerations for a stream cipher.

(*b*) Briefly describe ShiftRows transformation of AES.

(*c*) What is an Avalanche effect ? Does DES show avalanche effect ? Justify your answer.

(*d*) What is an ideal block cipher ? Why it cannot be used practically ?

(*e*) What does SHA stand for in SHA family of hash functions ? Mention any *two* hash functions from SHA family with the length of message digest.

(*f*) Write the general equation of an Elliptic curve. State the Discrete Log Problem over the Elliptic curve

(*g*) Describe requirements of a good digital signature scheme.

2. (*a*) Encrypt the message "CRYPTO" using the Hill Cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. What is the decryption matrix ?

(*b*) Explain the Feistel structure of a block cipher with the help of a diagram.

(*c*) Discuss various types of active and passive security attacks on a communication network.

3. (*a*) Use the Euclidean Algorithm to find the multiplicative inverse of 5994 modulo 20736.

(*b*) Identify GF(2^8) with the field of polynomials over GF(2) modulo $m(x) = x^8 + x^4 + x^3 + x + 1$. If the byte $b_7b_6b_5b_4b_3b_2b_1b_0$ represents the polynomial $b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$ in the field, find the product :

$$(01010111) \times (10111011).$$

(*c*) State Fermat's Theorem. Is the converse true ? Justify your answer.

4. (*a*) Describe the forward and inverse SubBytes transformation of AES and the rationale behind it.

(*b*) Represent the hexadecimal {53} as a bit-string and a polynomial. Find the inverse of the polynomial obtained in GF(2^8) modulo irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$.

(*c*) State the Chinese Remainder Theorem. If $x \equiv 23 \bmod 37$ and $x \equiv 34 \bmod 49$ then find x.

5. (*a*) Perform encryption and decryption using the RSA algorithm for $p = 5$, $q = 7$, $e = 7$ and M = 12.

(*b*) Consider the following Key exchange mechanism known a *Elliptic Curve Key exchange* :

Step 1 : Alice and Bob chooses an elliptic curve $y^2 = x^3 + rx + s$ over the field GF(p), p is prime with an element G of order n on this curve.

Step 2 : Alice chooses secret $a < n$ and sends a.G to Bob.

Step 3 : Bob chooses secret $b < n$ and sends b.G to Alice.

Step 4 : Alice calculates $a.(b.G) = abG$.

Step 5 : Bob calculates $b.(a.G) = abG$. Thus Alice and Bob have same shared secret key abG.

Suppose Alice and Bob chooses an elliptic curve $y^2 = x^3 + x + 6$ over the field GF(11) and G = (2, 7) on this curve. Alice and Bob selected secret keys $a = 2$, $b = 3$ respectively. Given 3G = (8, 3), find the secret key shared by Alice and Bob.

(*c*) Through help of a diagram show how hash function can be used to achieve integrity, authentication and confidentiality using only a symmetric key encryption scheme.

6. (*a*) Describe the Elgamal Digital signature scheme, that is, its public/private parameters, signing algorithm and verification algorithm.

(*b*) Write the services provided by PGP. Mention the different Symmetric key schemes, Public Key schemes and Hash function used in PGP.

(*c*) Describe a hash function. What is the main functionality of a hash function in a cryptographic secure communication mechanism ? Give *three* applications of hash functions, clearly specifying role of hash function in each application.

Roll No. | | | | | | | | | | |

S. No. of Question Paper : **8081**

Unique Paper Code : **32357501** **J**

Name of the Paper : **Numerical Methods**

Name of the Course : **B.Sc. (H) Mathematics : DSE-2**

Semester : **V**

Duration : **3 Hours** Maximum Marks : **75**

(Write your Roll No. on the top immediately on receipt of this question paper.)

All the *six* questions are compulsory.

Attempt any *two* parts from each question.

Marks are indicated against each question.

Use of Non-Programmable Scientific Calculator is allowed.

1. (*a*) A real root of the equation $x^3 - 5x + 1 = 0$ lies in $]0, 1[$. Perform three iterations of Regula Falsi Method to obtain the root. 6

(b) Perform three iteration of Bisection Method to obtain root of the equation $\cos(x) - xe^x$ in]0, 1[. 6

(c) Discuss the order of convergence of the Secant method and give the geometrical interpretation of the method. 6

2. (a) Verify $x = \sqrt{a}$ is a fixed point of the function $h(x) = \frac{1}{2}\left(x + \frac{a}{x^2}\right)$. Determine order of convergence of sequence $p_n = h(p_{n-1})$ towards $x = \sqrt{a}$. 6.5

(b) Use Secant method to find root of $3x + \sin(x) - e^x = 0$ in]0, 1[. Perform three iterations. 6.5

(c) Prove that Newton's Method is of order two using $x^3 + 2x^2 - 3x - 1 = 0$ and initial approximation $x_0 = 2$. 6.5

3. (a) Define a lower and an upper triangular matrix. Solve the system of equations :

$$-3x_1 + 2x_2 - x_3 = -12$$

$$6x_1 + 8x_2 + x_3 = 1$$

$$4x_1 + 2x_2 + 7x_3 = 1$$

by obtaining an LU decomposition of the coefficient matrix A of the above system. 6

(*b*) For Jacobi method, calculate T_{jac}, C_{jac} and spectral radius of the following matrix :

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$ 6

(*c*) Set up the Gauss-Seidel iteration scheme to solve the system of equations :

$$4x_1 + 2x_2 - x_3 = 1$$

$$2x_1 + 4x_2 + x_3 = -1$$

$$-x_1 + x_2 + 4x_3 = 1$$

Take the initial approximation as $X^{(0)} = (0, 0, 0)$ and do three iterations. 6

4. (*a*) Construct the Lagrange form of the interpolating polynomial from the following data :

x	1	2	3
$f(x) = \ln x$	ln 1	ln 2	ln 3

6.5

(*b*) Prove that for $n + 1$ distinct nodal points $x_0, x_1, x_2, \ldots x_n$, there exists a unique interpolating polynomial of at most degree n. 6.5

(*c*) Find the maximum value of the step size h that can be used in the tabulation of $f(x) = e^x$ on the interval [0, 1] so that the error in the linear interpolation of $f(x)$ is less than 5×10^{-4}. 6.5

5. (*a*) Define the backward difference operator ∇ and the Newton divided difference. Prove that :

$$f[x_0, x_1, -----, x_n] = \frac{\nabla^n f_n}{n! h^n} \text{ where } h = x_{i+1} - x_i . \quad 6$$

(*b*) Construct the divided difference table for the following data set and then write out the Newton form of the interpolating polynomial :

x	–7	–5	–4	–1
y	10	5	2	10

Find the approximation of y for $x = -3$. 6

(c) Use the formula

$$f'(x_0) \approx \frac{f(x_0+h)-f(x_0)}{h}$$

to approximate the derivative of $f(x)=1+x+x^3$ at $x_0 = 1$ taking $h = 1, 0.1, 0.001$. What is the order of approximation ? 6

6. (a) Approximate the value of $\int_0^1 e^{-x}dx$ using the Trapezoidal rule and verify that the theoretical error bound holds for the same. 6.5

(b) State Simpson's 1/3rd rule for the evaluation of $\int_a^b f(x)dx$ and prove that it has degree of precision 3. 6.5

(c) Use Euler's method to approximate the solution of the initial value problem.

$x' = (1+x^2)/t$, $x(1) = 0$, $1 \le t \le 4$ taking 5 steps. 6.5

This question paper contains 4+1 printed pages]

Roll No. | | | | | | | | | | |

S. No. of Question Paper : **8086**

Unique Paper Code : **32357506** **J**

Name of the Paper : **Cryptography and Network Security**

Name of the Course : **B.Sc. (Hons) Mathematics : DSE-1**

Semester : **V**

Duration : 3 Hours Maximum Marks : **75**

(Write your Roll No. on the top immediately on receipt of this question paper.)

All questions are compulsory.

Attempt any *five* parts from question No. **1**, each part carries **3** marks.

Attempt any *two* parts from questions **2** to **6**, each part carries **6** marks.

1. (*a*) Use the Rail fence cipher of depth 3 to encrypt "there could be better questions." Which attack is this cipher vulnerable to ?

(*b*) Explain the term diffusion in the context of a block cipher. How does DES achieve diffusion ?

(*c*) What is the difference between a stream cipher and a block cipher ?

(*d*) Describe a trap-door-one-way function.

(*e*) Define Euler totient function ϕ. Compute ϕ (105).

(*f*) Write the order in which Compression, Encryption and Digital Signatures are applied in PGP, while achieving both Authentication and Confidentiality, clearly state the reason behind this order.

(*g*) Describe the terms Non-Repudiation and Integrity in context of Cryptography. Mention the cryptographic primitives used to achieve these.

2. (*a*) Decrypt the following message encrypted using playfair cipher with the key "HER MAJESTY'S SHIP".

LVHZ CRJE RQQO ZRTY ERGM JRRM XOJR RANF RMOW ODNM AHYN WDER NMFM.

(*b*) What does it mean to say that the one time pad is unbreakable ? If the one time pad is unconditionally secure, why is it not widely used ?

(*c*) Describe the key expansion algorithm of DES with the help of a diagram.

3. (*a*) For any positive integers a and n, show that $b \equiv c \ mod(n)$ implies $ab \equiv ac \ mod(n)$. Show that converse is not true in general. In which case converse is also true ?

(*b*) Determine the GCD of $x^4 + 2x^3 + 5x^2 + 5x + 4$ and $x^3 + 2x^2 + 3x + 6$ over GF(7).

(*c*) State Fermat's Theorem. Use Fermat's Theorem to reduce $8^{109} \pmod{37}$.

4. (*a*) Describe the general structure of the encryption process in AES with the help of a diagram. Briefly comment on the various transformations performed in each round.

(*b*) Suppose that we have the following 128-bit AES key, given in haxadecimal notation :

287E151628AED2A6ABF7158809CF4F3C

(*i*) Express the initial round key (w_0 w_1 w_2 w_3) as a State matrix.

(*ii*) Given that RC[1] = 01, S(09) = 01, S(CF) = 8A, S(4F) = 84 and S(3C) = EB, where S denotes the S-box, calculate the first four bytes (w_4) for round one.

(*c*) Define the discrete logarithm of *a* number *b* for the base *a* (*mod p*). Prove that : $dlog_{a,p}\ (xy) = [dlog_{a,p}\ (x) + dlog_{a,p}\ (y)]\ (mod\ \phi(p))$.

5. (*a*) Perform encryption and decryption using the RSA algorithm for $p = 7$, $q = 13$, $e = 5$ and $M = 8$.

(*b*) The public parameters of Alice consists of an elliptic curve $y^2 = x^3 + x + 6$ over the field GF(11) and a point G = (2, 7) on this curve. Suppose Alice's private key is $a = 2$. Bob sends the ciphertext ((8,3), (5,9)) to Alice. Find the message sent by Bob to Alice.

(*c*) For the elliptic curve $y^2 = x^3 + x + 6$ over the field GF(11) :

(*i*) Calculate P + Q, where P = (5,2), Q = (8, 3).

(*ii*) Calculate 2P, where P = (5,2).

6. (*a*) What is the maximum input size and length of output of hash function SHA-512. State the value of padding field and length fields if the message length is 1920 bits. What is the size of word (register used) in SHA-512 ?

(*b*) Alice uses Flgamal Digital signature scheme to sign a document with the parameters : A cyclic group GF(19) with generator $a = 10$ and private key $X = 16$. He generated the random $K = 5$, gcd $(K, 18) = 1$ as part of signing process. If Alice signed the document with hash value $m = 14$, claculate the signature.

(*c*) Define Digital Signatures, its parameters, input/output, and general working of signing and verification algorithms. Define three types of attacks on a Digital signature.

(This Question paper contains 4 printed pages)

Roll No.....

Sr. No. of Question Paper: 8904

Unique Paper Code :235505

Name of the Course :BSc(Hons) Mathematics

Name of the Paper : Linear Programming and Theory of Games

Semester : V

Duration: 3 Hours

Maximum Marks: 75

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. Attempt any two parts of each question.
3. All questions carry equal marks.

1.(a) If for a basic feasible solution $x_B = B^{-1}b$ to the linear programming problem:

Minimize $z = cx$

$Ax = b$

$x \geq 0$

there is some column x_j in A but not in B for which $z_j - c_j > 0$ *and* $y_{ij} \leq 0$, then prove that the problem has an unbounded solution.

(b) Let $x_1 = 2$, $x_2 = 3$, $x_3 = 1$ is a feasible solution of the system of equations

$$2x_1 + x_2 + 4x_3 = 11$$

$$3x_1 + x_2 + 5x_3 = 14$$

Reduce this feasible solution to a basic feasible solution.

(c) Solve the following LPP using Simplex method:

Max $z = 10x_1 + x_2 + 2x_3$

Subject to

$$x_1 + x_2 - 2x_3 \leq 10$$

$$4x_1 + x_2 + x_3 \leq 20$$

$x_1, x_2 \geq 0$, x_3 unrestricted.

2) (a) Solve the linear programming problem by Big M method.

Max $z = 3x_1 - x_2$

Subject to

$$2x_1 + x_2 \geq 2$$
$$x_1 + 3x_2 \leq 3$$
$$x_2 \leq 4$$
$$x_1, x_2 \geq 0.$$

(b) Use Simplex method to solve the system of equation:

$$3x_1 + 2x_2 = 5$$
$$2x_1 + x_2 = 4$$

(c) Find the dual of the following LPP

Minimize $Z = x_1 + x_2 + 2x_3$

subject to $x_1 + x_2 + x_3 \leq 9$

$$2x_1 - 3x_2 + 3x_3 \geq 1$$
$$-3x_1 + 6x_2 - 4x_3 = 3$$
$$x_1 \leq 0, x_2 \geq 0, x_3 \text{ unrestricted.}$$

3 (a) Solve the following LPP by Two Phase method.

Max $z = x_1 + 5x_2$

Subject to

$$3x_1 + 4x_2 \leq 6$$
$$x_1 + 3x_2 \geq 2$$
$$x_1, x_2 \geq 0.$$

(b) State and prove Strong Duality theorem.

(c) Apply the principle of duality to solve the linear programming problem

Minimize $x = 3x_1 + 2x_2$

Subject to $x_1 + x_2 \geq 1$

$$x_1 + x_2 \leq 7$$
$$x_1 + 2x_2 \leq 10$$

$$x_2 \leq 3$$
$$x_1, x_2 \geq 0$$

4) (a) Solve the following cost-minimizing transportation problem:

	D_1	D_2	D_3	Supply
O_1	6	8	4	14
O_2	4	9	3	12
O_3	6	10	15	5
Demand	6	10	15	

(b) Minimize the total man hours in the following assignment matrix by Hungarian method.

	I	II	III	IV	V
A	11	17	8	16	20
B	9	7	12	6	15
C	13	16	15	12	16
D	21	24	17	28	26
E	14	10	12	11	15

(c) Define saddle point of a two person zero sum game. Use the minimax criteria to find the best strategy for each player for the game having the following pay off matrix

Player II

Player I $\begin{bmatrix} 1 & -1 \\ -2 & 0 \\ 3 & 1 \end{bmatrix}$

Is it a stable game?

5) (a) Solve graphically the game whose payoff matrix is

$$\begin{bmatrix} 2 & 4 & 11 \\ 7 & 4 & 2 \end{bmatrix}$$

(b) Use the relation of dominance to solve the game whose payoff matrix is given by

$$\begin{bmatrix} 1 & 7 & 3 & 4 \\ 5 & 6 & 4 & 5 \\ 7 & 2 & 0 & 3 \end{bmatrix}$$

(c) Reduce the following game to a Linear Programming Problem and then solve by simplex method.

Shift it ← to the previous sheet.

$$\begin{bmatrix} 1 & -3 & 2 \\ -4 & 4 & -2 \end{bmatrix}$$