MCA.I/11.24.004 Reg.No. | | | | | | | | | C

MCA DEGREE FIRST SEMESTER EXAMINATION, NOVEMBER 2024

22-382-0104 SOFTWARE ENGINEERING

(Regular & Supplementary)

Write any FIVE questions.
(Each Question Carries 10 Mark)

Time-3 Hours **Maximum Marks :50**

Q.Nos		QUESTIONS	Marks	CO	BL	PI
1.	a.	Discuss the role and significance of Software Engineering ethics.	4	CO1	L2	8.2.1
	b.	A project manager selects a Software process model which ensures that every development cycle includes identifying risks, customer feedback and improvement, and developing prototypes. The product is built incrementally. Name this model. Explain the working of this model with a neatly abelled diagram. Also, mention its advantages and disadvantages.	6	CO1	L3	1.7.1
		OR				
2.		Discuss the Agile SCRUM model in detail.	10	CO1	L1	1.7.1
3.		Assume that you are preparing an SRS for an upcoming Hotel room booking software. The facilities included in-room dining and mess hall dining. The user must be able to make choices regarding dining while booking rooms. Further relevant assumptions pertaining to the system, you can make for answering this question. List the functional and non-functional requirements that must be included in the SRS. Along with each listing, please add in brackets what was the assumption/ condition behind the requirement.	10	CO2	L3	3.1.6
		OR				
4.		"Modularity, Cohesion, and Coupling are the key factors that determine the goodness of a Software Design". How? Give a suitable explanation including different types/levels of Cohesion and Coupling.	10	CO2	L2	3.1.6

5.		Draw the Use-Case diagram for a Doctor appointment system. Deployment of generalization, <<includes>> and <<extends>> is mandatory. Narrative/ User story: This system allows users to book a Doctor's appointment online. A patient can be a new patient or an existing patient. New patients need to register first and then login. Existing users can directly login and use the system. The appointment is allotted only after the fee is paid. Cancellation as well as postponement of appointments can also be done in the system. In case of cancellation, the fee paid will be refunded. The same patient can make multiple bookings in one login session.	**10**	**CO3**	**L3**	**3.6.2**
		OR				
6.		For the narrative given in Question 5 above, prepare and present the Sequence diagram.	**10**	**CO3**	**L3**	**3.6.2**
7.		Why are Software documentation and Testing documentation important? How do we implement these? Give an example of Testing documentation.	**10**	**CO4**	**L2**	**5.1.1**
		OR				
8.		What is black box testing? Explain any two black box testing techniques with examples.	**10**	**CO4**	**L1**	**1.7.1**
9.		With a neat diagram, explain the CMMI process improvement framework.	**10**	**CO5**	**L1**	**3.5.4**
		OR				
10.		Write notes on: i. Virtualisation and Containers ii. Elements of Software Quality Assurance.	**5** **5**	**CO5**	**L1**	**5.1.1**

****

MCA.I/11.24.003 Reg.No. | | | | | | | | | B

MCA DEGREE FIRST SEMESTER EXAMINATION, NOVEMBER 2024

22-382-0103 DIGITAL FUNDAMENTALS AND COMPUTER ARCHITECTURE

(Regular)

Write any FIVE questions.
(Each Question Carries 10 Mark)

Time-3 Hours **Maximum Marks :50**

Q.Nos		QUESTIONS	Marks	CO	BL	PI
1.	a.	What is K Map? Represent/Simplify the following expressions using K Map i. Σ m(0,3,4,6,7) ii. π M(1,2,5,7) iii. Y=(ABC+ ~AB+ AB~C + A~B~CD) iv. Y=(~A+B+~C).(A+~B+~C+~D).(~A+~C).(C+D)	5	CO1	L3	1.1.2
	b.	Convert the following : i. 1001.11(Bin) to Dec ii. 368. 25(Dec) to Bin iii. BF. 5 (Hex) to Oct iv. 275. 25(Oct) to Hex	5	CO1	L3	1.1.2
		OR				
2.	a.	Exemplify the scope and significance of Boolean Algebra and any three the Boolean Algebra operations. Describe the laws of Boolean Algebra with suitable Examples.	5	CO1	L3	2.2.2
	b.	Explain D Morgan's first and second law. Draw the truth table for A(B+D).	5	CO2	L2	1.1.1
3.		Explain shift operations specifying its advantages and applications.	10	CO2	L2	1.1.1
		OR				
4.		Explain the process of Encoding Machine Instructions with suitable examples.	10	CO2	L2	1.3.1

5.	a.	Describe the Memory Hierarchy exemplifying its significance with data transfer and storage capacity.	5	CO3	L2	2.4.1
	b.	Illustrate I/O Interface Techniques emphasising I.O mapped I/O and Memory Mapped I/O.	5	CO3	L2	2.4.1
		OR				
6.	a.	Exemplify different kinds of interrupts and its significance to the system.	5	CO3	L2	2.4.1
	b.	Illustrate the Instruction Set Architecture with proper examples.	5	CO3	L2	2.4.1
7.		What is the significance of 2's compliment in Computer Arithmetic? Perform the following operations in Binary using proper compliment method. i. (+5) + (+8) ii. (-7) + (+6) iii. (+4) - (+8) iv. (+7) - (-5)	10	CO4	L3	3.2.1
		OR				
8.		What is the significance of LSB and MSB in Binary Arithmetic? Perform the following operations i. 1011 * 101 ii. 1101.10 * 10.11 iii. 11010 / 101 iv. 1111 / 10	10	CO4	L3	3.2.1
9.		Describe processor organization and instruction execution with help of a proper figure.	10	CO5	L3	1.3.1
		OR				
10.		Explain Pipelining and its significance in parallel processing. Exemplify various Pipeline hazards.	10	CO5	L2	1.3.1

****

MCA.I/11.24.001 Reg.No.

MCA DEGREE FIRST SEMESTER EXAMINATION, NOVEMBER 2024
22-382-0101 MATHEMATICAL FOUNDATIONS FOR COMPUTING
(Regular)

Write any FIVE questions.
(Each Question Carries 10 Mark)

Time-3 Hours **Maximum Marks :50**

Qn No		Questions	Marks	CO	BL	PI
1	a	Which among the following sets are subspaces of R^3? Justify your answer. (i) $S=\{(x,y,z)\in R^3 : x^2+y^2=z^2\}$ (ii) $W=\{(x,y,z)\in R^3 : x=3y+2z\}$	5	CO1	L2	1.3.1
	b	Consider the following matrix A where a and b are real numbers $A=\begin{bmatrix} a & 1 & 2 \\ 0 & 2 & b \\ 1 & 3 & 6 \end{bmatrix}$ Find out the values of a and b for which the matrix A has (i) rank=1 (ii) rank=2 and (iii) rank=3	5	CO1	L3	1.1.2
		OR				
2	a	Find the complete solution for the following system of equations: $x_1+x_2-x_3+x_4+5x_5=0$ $2x_1+x_2-2x_3+4x_4=0$ $3x_1+2x_2-3x_3+5x_4+6x_5=0$	5	CO1	L1	1.3.1
	b	Find all the possible values of h and k so that the following system of equations has: (i) no solution (ii) unique solution and (iii) infinitely many solution. $\begin{bmatrix} 1 & 1 \\ -2 & h \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}=\begin{bmatrix} k \\ 1 \end{bmatrix}$	5	CO1	L3	1.1.2

3	a	Construct a 3×3 real-valued matrix A that has the eigenvalues: $\lambda_1=5$, $\lambda_2=2$ and $\lambda_3=-1$ and the corresponding eigenvectors: $v_1=[1,0,0]$, $v_2=[0,1,0]$ and $v_3=[0,0,1]$.	5	CO2	L3	1.1.2
	b	Compute the eigen values and the corresponding eigen vectors of the following matrix A in terms of k. $$A=\begin{bmatrix}1 & k\\ 2 & 1\end{bmatrix}$$	5	CO2	L3	1.1.1
		OR				
4	a	Verify Cayley-Hamilton theorem for the following matrix A. $$A=\begin{bmatrix}11 & -6i\\ 4i & 1\end{bmatrix}$$	5	CO2	L3	1.1.1
	b	Compute the Singular Value Decomposition of the following matrix A. $$A=\begin{bmatrix}1 & 1\\ 0 & 1\\ -1 & 1\end{bmatrix}$$	5	CO2	L3	1.1.1
5		There are three random variables X, Y and Z each can takes values either 0 or 1. The following table shows the joint distribution of these three random variables A, B, and C:	10	CO3	L3	1.3.1

X	*Y*	*X*	*P(X,Y,Z)*
0	0	0	0.1
0	0	1	0.2
0	1	0	0.15
0	1	1	0.05
1	0	0	0.1
1	0	1	0.2
1	1	0	0.1
1	1	1	0.1

(i) Verify whether X and Y are independent
(ii) Verify whether X and Z are independent
(iii) Verify whether Y and Z are independent

OR

6	a	In a certain college, 4% of boys and 1% of girls are taller than 1.8 meters. Furthermore, 60% of the students in the college are girls. If a student is selected at random and is found to be taller than 1.8 meters. Then, what is the probability that the selected student is a girl?	5	CO3	L3	1.3.1
	b	From the joint distribution table given in Question No.5, compute the following probability values: (i) P(X), P(Y) and P(Z) (ii) P(X=1|Y=1) (iii) P(Y=1, Z=1)	5	CO3	L3	1.3.1
7	a	A fitness coach is analysing the relationship between the daily exercise time in hours and the calories burned per week in kilocalories. The following dataset containing 8 observations were collected from individuals over a one-week period: **Daily Exercise Time / Calories Burned** 0.5 / 1200 1.0 / 1500 1.5 / 1700 2.0 / 2000 2.5 / 2200 3.0 / 2500 3.5 / 2800 4.0 / 3100 Fit a simple linear regression model to the given dataset using the method of least squares. Also, compute the Sum of the Squared Residuals (SSR) between the given observations and the fitted regression line.	6	CO4	L3	1.1.1
	b	Suppose a researcher wants to model the relationship between the weekly study hours and the test scores of students belonging to a particular class. The researcher derived the following statistical measures form the sample data: (i) Average weekly study hours = 102.30 (ii) Average test scores = 215.70 (iii) Covariance between study hours and test scores = 18.5 (iv) Standard deviation of weekly study hours = 7.40 and (v) Standard deviation of test scores = 22.80. Then, compute the slope and the y-intercept of the regression line for predicting the test scores from weekly study hours.	4	CO4	L3	1.1.2

		OR				
8	**a**	Solve the following optimization problem using Lagrange Multipliers method: $\min_{x_1,x_2,x_3} x_1^2 + x_2^2 + x_3^2 - 10x_1 - 6x_2 - 4x_3 = 0$ $subject\ to\ x_1 + x_2 + x_3 = 7$	**5**	**CO4**	**L3**	**1.1.2**
	b	Check whether the following function is convex or not. $x_1^2 + x_2^2 + x_3^2 - 10x_1 - 6x_2 - 4x_3 = 0$	**5**	**CO4**	**L3**	**1.3.1**
9		Given the following data set, use Principal Component Analysis (PCA) to reduce the dimensions from 2 to 1. x_1: 12, 15, 14, 13, 16, 10, 11 x_2: 18, 24, 22, 21, 25, 19, 20	**10**	**CO5**	**L3**	**1.1.2**
		OR				
10		A dataset contains the following measurements of two features, X_1 and X_2, across six observations: X_1=[10, 12, 14, 16, 18, 20] X_2=[25, 30, 35, 40, 45, 50]. (i) Standardize the given dataset using z-score normalization. (ii) Compute the covariance matrix of the standardized data. (iii) Interpret the diagonal and off diagonal elements of the computed covariance matrix. (iv) Compare the covariance matrix prior to normalization with the covariance matrix after normalization, and discuss the observed differences.	**10**	**CO5**	**L3**	**1.1.2**

****

MCA.I/11.24.002 Reg.No. | | | | | | | | | A

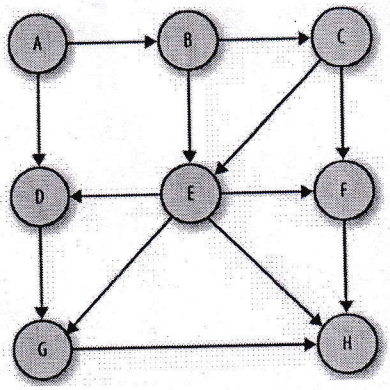
MCA DEGREE FIRST SEMESTER EXAMINATION, NOVEMBER 2024
22-382-0102 DATA STRUCTURES AND ALGORITHM USING C
(Regular)

Write any FIVE questions.
(Each Question Carries 10 Mark)

Time-3 Hours **Maximum Marks :50**

Q. No		Questions	Marks	CO	BL	PI
1.	a.	Write a menu driven C program to accept a two dimensional matrix and perform the following operations: 1. Display the transpose of the matrix. 2. Print the sum of the squares of the diagonal elements.	6	CO1	L2	1.7.1
	b.	Compare the working of *while* and *do while* looping constructs of C language with examples.	4	CO1	L2	1.7.1
		OR				
2.	a.	Write a menu driven C program to accept an integer number and perform the following operations: 1. Check whether the number is palindrome. 2. Replace the smallest digit in the number with zero.	6	CO1	L2	1.7.1
	b.	Explain the following terms in C language with examples: 1. Keywords 2. Identifiers	4	CO1	L2	1.7.1
3.	a.	Write a C program to calculate the power of a number using recursion. Input: A base x and an exponent y Output: The value of x^y.	6	CO2	L3	1.7.1
	b.	What is a pointer? Explain the relevance of pointer in dynamic memory allocation with an example.	4	CO2	L3	1.7.1
		OR				
4.	a.	Define a structure called Employee with the following members: Name (string) Age (integer) Employee ID (integer) Salary (float)	6	CO2	L2	1.7.1

		Write a C program to create an array of n employees (where n is input by the user) and display i) Average salary of employees' ii) Details of employees whose age greater than 50.				
	b.	Differentiate *call by value* and *call by reference* with examples.	4	CO2	L2	1.7.1
5.	a.	Write a C program to create a stack using linked list and to perform push, pop and display operations.	6	CO3	L3	1.7.1
	b.	Explain preorder and inorder traversal on binary tree with examples.	4	CO3	L3	1.7.1
		OR				
6.	a.	Define Binary Search Tree. Construct a Binary Search tree by inserting 26 35 38 31 43 58 46. Delete 38 and add 88 to the binary search tree and show the tree after deletion and addition.	6	CO3	L3	1.7.1
	b.	Perform the following operations on a Queue with Max_Size 4 and show the values of front and rear after each operation. Initially the Queue is empty. i) Insert A, B ii) Delete 1 elements iii) Insert C, D iv) Delete 3 elements	4	CO3	L3	1.7.1
7.	a.	Explain the difference between a Max-Heap and a Min-Heap with examples. Provide the applications of Heap.	4	CO4	L3	1.7.1
	b.	Given the following array representing a binary tree: 15, 10, 8, 7, 5, 3, 20 (i) Determine if it satisfies the properties of a Max-Heap. Justify your answer. (ii) If it does not satisfy, perform the necessary steps to convert it into a Max-Heap	6	CO4	L3	1.7.1
		OR				
8.	a.	Explain any 2 graph representation methods with examples.	4	CO4	L3	1.7.1

	b.	Find the DFS traversal of the following graph taking A as the starting vertex. Show the step by step operations.  	6	CO4	L3	1.7.1
9.		Write a C program to implement quick sort. Sort the given array elements 20, 35, 40, 100, 3, 10, 15 using quick sort and describe the step by step operations.	10	CO5	L2	1.7.1
		OR				
10	a	A hash table of size 13 uses double hashing for collision resolution. The primary hash function is h1(x) = x mod 13 and the secondary hash function is h2(x) = 1+(x mod 11). Insert the keys: 10, 22, 31, 4, 15, 28, 17. i. Show the resulting hash table ii. Show the hash table if linear probing is used for collision resolution.	6	CO5	L2	1.2.2
	b.	Define collision in hashing. Explain the Separate Chaining collision resolution method with example?	4	CO5	L2	1.2.2

****

M.Sc.(AI).III/11.24.002 Reg.No. | | | | | | | | |

A

M.Sc. COMPUTER SCIENCE WITH SPECIALIZATION IN ARTIFICIAL INTELLIGENCE THIRD SEMESTER EXAMINATION NOVEMBER 2024

23-344-0321 EXPLAINABLE ARTIFICIAL INTELLIGENCE

(Regular)

Write any FIVE questions.
(Each Question Carries 10 Mark)

Time-3 Hours **Maximum Marks :50**

Q. No		Questions	Marks	CO	BL	PI
1	a	What are some model-agnostic techniques for explainability?	5	CO1	L2	1.7.1
	b	How do post-hoc explainability methods differ from inherently interpretable models?	5	CO1	L2	1.7.1
		OR				
2	a	What are the main components of LIME, and how do they contribute to its interpretability?	5	CO1	L2	1.7.1
	b	Explain the concept of feature importance in a Random Forest model. How does feature importance in Random Forests differ from feature importance in individual decision trees?	5	CO1	L2	1.7.1
3	a	Implement a model agnostic explanation using LIME in a deep learning model.	5	CO2	L3	1.2.1
	b	How is shapley (SHAP) used in machine learning to explain classification or regression models? Write mathematical formulations for estimating shapely values for an attribute i.	5	CO2	L3	1.2.1
		OR				
4		Imagine that you are developing a predictive model for diagnosing heart disease using patient data. Your model is a black-box neural network with high accuracy but low interpretability.	10	CO2	L3	2.5.2

		a) Explain why interpretability is crucial in a healthcare application like heart disease prediction. b) Choose two XAI techniques (e.g., LIME, SHAP, or Partial Dependence Plots) and discuss how each could help make the model's predictions understandable to doctors and patients. c) Describe the ethical implications of deploying an opaque model in healthcare. How could explainability improve trust and decision-making? d) Briefly discuss the limitations of XAI techniques in this context and any potential risks of misinterpreting the explanations.				
5	**a**	Consider Wine.csv file with attributes fixed acidity, volatile acidity, citric acid, residual sugar, chlorides, free sugar dioxide, total sulphur dioxide, density, pH, sulphates, alcohol. Implement linear regression using the necessary Python library to estimate the quality of alcohol on scale of 1 to 10, the higher the better. Explain the model using linear regression.	**5**	**CO3**	**L3**	**2.5.2**
	b	Build an agnostic explanation for a black box model for classifying a set of images with VGG16 and apply augmentation in input dataset. Write a code using python with occlusion as explainability to highlight the features that are important .	**5**	**CO3**	**L3**	**1.2.1**
		OR				
6		Use Grad-CAM to analyze the model's predictions for a set of misclassified images. a) Generate Grad-CAM heatmaps for each misclassified image. b) Describe any patterns you observe in the heatmaps—are there consistent regions the model tends to focus on? c) Discuss how Grad-CAM can help diagnose why the model may be making errors	**10**	**CO3**	**L3**	**1.2.1**

		Explain how occlusion sensitivity can be used to interpret the decision-making process of a deep learning model for image classification. Provide an example of how this method can help identify biases or weaknesses in the model's predictions.	10	CO3	L3	1.7.1
		OR				
8	a	Explain the counterfactual explanation method in the context of machine learning. How can counterfactual explanations be used to increase fairness and transparency in decision-making algorithms, such as those used for loan approval or university admissions?	5	CO4	L3	1.7.1
	b	Explain loss function for generating counterfactual examples. List advantages and disadvantages for counterfactual explanation.	5	CO4	L2	1.7.1
9	a	What is the Fast Gradient Sign Method (FGSM) for generating adversarial examples? Explain how it works, and describe the formula for generating an adversarial example using FGSM.	5	CO5	L3	1.2.1
	b	Explain the creation of adversarial examples using GAN.	5	CO5	L3	1.7.1
		OR				
10	a	Discuss the challenges and potential solutions in ensuring that Explainable AI models remain robust against adversarial attacks. Provide examples of methods that can help defend against such attacks while maintaining model interpretability.	5	CO5	L3	1.2.1
	b	Explain the procedure used for generating SHAP signature to defend against adversarial attacks.	5	CO5	L3	1.7.1

****

MCA.III/11.24.002 Reg.No.

MCA DEGREE THIRD SEMESTER EXAMINATION, NOVEMBER 2024
22-382-0302 CRYPTOGRAPHY AND NETWORK SECURITY
(Regular & Supplementary)

Write any FIVE questions.
(Each Question Carries 10 Mark)

Time-3 Hours **Maximum Marks :50**

Q.No		QUESTIONS	MARKS	CO	BL	PI
1.	a.	Decrypt **"TSUTPIILRSTSOANIHAMROOICNASN"** Using the key APPLE (Hint: Keyed transposition cipher)	4	CO1	L3	1.7.1
	b.	Use the Vigenere cipher With keyword HEALTH To encipher the message "D I G I T A L W O R L D".	4	CO1	L3	1.7.1
	c.	Evaluate 49^{-1} (mod 970) if it exists.	2	CO1	L3	1.7.1
2.	a.	Encrypt the message "THE TREASURE IS HIDDEN UNDER THE OLD TREE" using ADVENTURE as key and play fair cipher.	5	CO1	L3	1.7.1
	b.	Check whether the following matrix is suitable for Hill cipher encryption? $\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix}$	5	CO1	L3	1.7.1
3.	a.	What are three variants of AES? Explain Mix Column operation in AES.	4	CO2	L3	1.7.1

	b.	Consider the plain text block with 32 hexa characters each represented by using 4 bits{00010203040506070809 0A0B0C0D0E0F} i)Display the 128 bit block as an AES state table ii) Perform Substitute byte and shift row operations using following S- BOX.	6	CO2	L3	1.7.

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

OR

4.	a.	Let m be a message consisting of 50 blocks. Alice transmits m to Bob using block mode of encryption. Due to a network error, the 24th block gets corrupted, but all other ciphertext blocks are transmitted correctly. Once Bob decrypts the cipher text, how many plaintext blocks will be affected, If using i) CFB mode of operation? ii) OFB mode of operation ?	4	CO2	L2	1.6.1
	b.	Explain operations performed within a round of DES.	6	CO2	L2	1.6.1
5.	a.	Check for primality without using a calculator i) 1009 ii) 63 (Apply suitable theorem and Show all steps)	2	CO3	L3	2.5.3

	b.	What is the key feature behind Homomorphic encryption? List 3 different types of Homomorphic encryption together with supporting operations.	4	CO3	L3	2.5.3
	c.	What is the trapdoor function behind Elgamal public key scheme? Assume p= 107, primitive root a=2 and random number d=67. Encrypt the message "C encoded to 2" with random number k= 45 using Elgamal public key cryptosystem.	4	CO3	L3	2.5.3
		OR				
6.	a.	Consider the curve $y^2 = x^3 + 4x + 7 \pmod{13}$ over the prime filed Z_{13} and Find all the points on the curve.	8	CO3	L3	2.5.3
	b.	What is the key idea behind Shamir's secret sharing scheme?	2	CO3	L3	2.5.3
7.	a.	If RSA key pairs of user Alice are given as follows Publish public key PU={7,187} and private key PR={17,11,23} Alice composed a message to Bob and calculated the MD5 hash "11". Prepare Alice's digital signature based on the above information and RSA algorithm.	4	CO4	L3	2.5.3
	b.	Consider the message with 2400 bits given as input to SHA512 algorithm, how many bits need to be added to it excluding the length.If the size of the message is 900 in bits , How many bits need to be padded if SHA1 algorithm used for digest preparation.	3	CO4	L3	2.5.3
	c.	If we have a message M of size 128 bits, whose MD5 hash H1 is exactly 128 bits is "844f85c2723bbd39381c7379a6041608" What will be the size of the hash for the message created by appending M with another copy of the same message if the hashing algorithm remains the same?	3	CO4	L3	2.5.3

		OR				
8.	**a.**	List key requirements of Cryptographic Message Authentication codes.	**4**	**CO4**	**L2**	**1.7.1**
	b.	Explain steps for preparing ECC Digital signature including Key generation , Encryption and Decryption.	**6**	**CO4**	**L2**	**1.7.1**
9.	**a.**	Which protocol is used for securing credit card transactions over unsecured networks?	**2**	**CO3**	**L2**	**1.7.1**
	b.	What is a Digital Certificate ? Explain Certificate generation process with a suitable block diagram.	**8**	**CO3**	**L2**	**1.7.1**
		OR				
10.		Compare SSL and TLS and evaluate the security of each protocol.	**10**	**CO5**	**L2**	**1.7.1**

****