STELLA MARIS COLLEGE (AUTONOMOUS), CHENNAI
COURSE PLAN June - November 2024

Department : Mathematics
Name/s of the Faculty : S Mercy Soruparani
Course Title : Number Theory and Cryptography
Course Code : 23MT/PE/NC15
Shift : I

COURSE OUTCOMES (COs)

On successful completion of the course, students will be able to

COs	Description	CL
CO1	recall the basic concepts of number theory and their applications in cryptography	K1
CO2	understand the fundamental ideas of number theory and cryptography	K2
CO3	apply the concepts of number theory and cryptography in problems	K3
CO4	analyze the analytics of residues and congruences and its relevance to cryptography	K4
CO5	evaluate and exhibit crypto models as an application of number theory and cryptography	K5

Week	Unit No.	Content	C L	Teaching Hours	COs	Teaching Learning Methodology	Assessment Methods
Jun 24 – 26, 2024 (Day Order 4 - 6)	1	**Elementary Number Theory** 1.1 Time Estimates for doing Arithmetic	K1- K5	2	CO1-5	Presentation	Questioning
Jun 27 – July 4, 2024 (Day Order 1 - 6)	1	1.1 Time Estimates for doing Arithmetic(cont.) 1.2 Divisibility and the Euclidean Algorithm	K1- K5	5	CO1-5	Problem Solving	Quiz
July 5 – 12, 2024 (Day Order 1 - 6)	1	1.3 Congruences 1.4 Some Applications to Factoring	K1- K5	5	CO1-5	Lecture	Problem Solving
July 15 – 23, 2024 (Day Order 1 - 6)	1 2	1.4 Some Applications to Factoring (cont.) **Finite Fields and Quadratic Residues** 2.1 Finite Fields	K1- K5	3 2	CO1-5	Model Problems	Group Study
July 24 – 31, 2024 (Day Order 1 - 6)	2	2.1 Finite Fields(cont.)	K1- K5	5	CO1-5	Group Discussion	Model Problems
Aug 1 – 5, 2024 (Day Order 1 - 3)	2	2.2 Quadratic Residues and Reciprocity	K1- K5	3	CO1-5	Simulation	Group Discussion
Aug 6 – 10, 2024	**C.A. Test – I (Unit 1 & Unit 2:2.1)**						
Aug 12 – 14, 2024 (Day Order 4-6)	2	2.2 Quadratic Residues and Reciprocity(cont.)	K1- K5	2	CO1-5	Lecture	Quiz
Aug 16 – 23, 2024 (Day Order 1-6)	3	**Cryptography** 3.1 Some Simple Cryptosystems	K1- K5	5	CO1-5	Model Problem	Problem Solving

Aug 27 – Sep 3, 2024 (Day Order 1-6)	3	3.2 Enciphering Matrices	K1- K5	5	CO1-5	Presentation	Field Work
Sep 4 – 11, 2024 (Day Order 1-6)	3 4	3.2 Enciphering Matrices (cont.) **Public Key** 4.1 Public Key Cryptography	K1- K5	2 3	CO1-5	Group Discussion	Field Work
Sep 12 - 20, 2024 (Day Order 1-6)	4	4.1 Public Key Cryptography(cont.)	K1- K5	5	CO1-5	Problem Solving	Test 30 Marks Unit 4
Sep 23 - 26, 2024 (Day Order 1-4)	4	4.2 RSA	K1- K5	3	CO1-5	Presentation	Seminar 20 Marks
Sep 27 – Oct 3, 2024	**C.A. Test – II (Unit 2:2.2 & Unit 3)**						
Oct 4 – 5, 2024 (Day 5 & 6)	4 5	4.2 RSA (cont.) **Primality and Factoring** 5.1 Pseudoprimes	K1- K5	1 1	CO1-5	Group Study	Presentation
Oct 7 - 15, 2024 (Day Order 1 to 6)	5	5.2 The Rho Method	K1- K5	5	CO1-5	Model Problems	Group Study
Oct 16 - 22, 2024 (Day Order 1 to 6)	5	5.3 Fermat factorization and factor bases	K1- K5	5	CO1-5	Lecture	Group Discussion
Oct 23 , 2024 (Day Order 1)	5	5.3 Fermat factorization and factor bases(cont.)	K1- K5	1	CO1-5	Problem Solving	Discussion
Oct 24 , 2024 (Day Order 2)	**REVISION**						