ST.JOSEPH'S COLLEGE FOR WOMEN (AUTONOMOUS), VISAKHAPATNAM

VII SEMESTER **MATHEMATICS** TIME: 2Hrs/Week

M 7355(2) **CRYPTOGRAPHY** Max. Marks: 50

w.e.f .20AH Batch **PRACTICAL SYLLABUS**

Course Objectives: To enable the students to

- Understand time estimates for arithmetic operations, finite fields and their properties, concept of public key cryptography.
- Explore the concepts of divisibility and the Euclidean algorithm, enciphering matrices for encryption, quadratic residues and reciprocity in number theory.
- Learn about congruences and their applications in factoring, discrete logarithms and the Knapsack algorithm. factoring methods including the rho method, Fermat factorization, factor bases, the continued fraction method, and the quadratic sieve method.
- Study some simple cryptographic systems, RSA algorithm for encryption and decryption, pseudoprimes and their properties.

Learning Outcomes:
After successful completion this course, the student will be able to

- Apply theoretical / analytical / statistical knowledge gained in various courses of B.Sc to solve numerical problems based on real life situations during practicals and draw meaningful solutions to day to day problems
- Enabling students to develop a positive attitude towards mathematics as an interesting and valuable subject of study
- Enhancing students' overall development and to equip them with mathematical abilities, problem solving skills, creative talent and power of communication necessary for various kinds of employment.
- Problem solving on Divisibility and Euclidean algorithm and congruences
- Problem solving on Enciphering matrices
- Problem solving on finite fields and quadratic residues
- understand the idea of public key cryptography
- understand psedo-primes and Fermat's factorization

UNIT-I
Elementary Number Theory

Time Estimates for doing arithmetic - Divisibility and Euclidean algorithm – Congruences - Applications to factoring.(Chapter-I of the Text Book)

UNIT-II
Cryptography

Some simple crypto systems - Enciphering matrices (Chapter-III of the Text Book)

UNIT-III
Finite Fields and quadratic Residues

Finite fields - Quadratic residues and Reciprocity (Chapter-II of the Text Book)

UNIT-IV
Public Key Cryptography

The idea of public key cryptography - RSA - Discrete log - Knapsack (Chapter-IV: Sections to IV.4 (omit sec.5) of the Text Book)

UNIT-V
Primality and Factoring

Pseudoprimes - The rho method - Fermat factorization and factor bases - The Continued fraction method - The quadratic sieve method.(Chapter-V of the Text Book)

Activities:

1. Assignments
2. Student Seminars and Guest Lecturers
3. Problem Solving Sessions

Text Book:

Neal Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, New York,2002, Second Edition.

Reference Books:

1. Niven and Zuckermann, An Introduction to Theory of Numbers (Edn. 3), Wiley EasternLtd., New Delhi, 1976.
2. David M.Burton, Elementary Number Theory, Wm C.Brown Publishers, Dubuque, Iowa,1989.
3. K.Ireland and M.Rosen, A Classical Introduction to Modern Number Theory, SpringerVerlag, 1972.