MTS 561	**Cryptography**	**4 Credits (48 hours)**

Course Outcome: To introduce the concepts and to develop working knowledge on fundamentals of Cryptography. Students will have the knowledge and skills to apply the concepts of the course in Computer Applications including Cyber security.

Course Specific Outcome: At the end of the course students will have the knowledge and skills to understand, explain in depth and apply the fundamental concepts-

- Number Theoretic Background
- Finite Fields and Quadratic Residues
- Cryptography, Public key
- Primality and Factoring

Unit I - Some Topics in Elementary Number Theory:
Time estimates for doing arithmetic, Divisibility and Euclidean Algorithm, Congruences, Some Applications to Factoring.

(8 Hours)

Unit II - Finite Fields and Quadratic Residues:
Finite Fields, Quadratic residues and Reciprocity.

(6 Hours)

Unit III - Cryptography:
Some Simple cryptosystems, Enciphering matrices.

(6 Hours)

Unit IV - Public Key:
The Idea of Public Key Cryptography, RSA, Discrete Log, Knapsack, Zero-knowledge Protocols and Oblivious Transfer.

(14 Hours)

Unit-V - Primality and Factoring:
Pseudoprimes, The rho method, Fermat Factorization and Factor Bases, The Continued Fraction Method, The Quadratic Sieve Method.

(14 Hours)

References:

[1] Neal Koblitz, *A course in Number Theory and Cryptography*, Springer Verlag, NewYork, 1987.

[2] Hans Delfs, Helmut Knebl, *Introduction to Cryptography*, Springer Verlag, 2002.

[3] William Stallings, *Cryptography and Network Security*, Prentice Hall of India, 2000.

[4] Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2000.

MTS 562	**Finite Element Method with Applications**	**4 Credits (48 hours)**

Course Outcome: This course intended to understand and develop proficiency in the application of the finite element method to realistic problems in modeling, analysis, and interpretation.

Course Specific Outcome: At the end of the course students will have the knowledge and skills to understand, explain in depth and apply the fundamental concepts-

- Weighted Residual Approximations
- Finite Elements and Finite Element Procedures
- Finite Element solution of differential equations

Unit I - Weighted Residual Approximations:
Point collocation, Galerkin and Least Squares method. Use of trial functions to the solution of differential equations.

(12 Hours)

Unit II - Finite Elements:
One dimensional and two dimensional basis functions, Lagrange and serendipity family elements for quadrilaterals and triangular shapes. Isoparametric coordinate transformation. Area coordinates standard 2- squares and unit triangles in natural coordinates.

(12 Hours)