COURSE SYLLABUS

SEMESTER-V

Course Name: Number Theory and Cryptography	**Course Code: BMA5****
No. of Lecture hours / week: 03	**CIE Marks: 50**
No. of Tutorial hours / week: 0	**SEE Marks: 50**
Total No. of Lecture Hours + Tutorial hours: 40+0=40	**SEE Duration: 03 hrs**
L: T: P: 3:0:0	**Credits: 03**

COURSE PREREQUISITES: To understand Number Theory and Cryptography, the students should have strong basics in number system and basic algebra.

COURSE OVERVIEW:

Number Theory and Cryptography is a course which provides strong basic knowledge of number theory which is very useful to understand the algorithms of cryptography. The course majorly focuses on Divisibility, Congruence, Modular Arithmetic, Primitive Roots and Quadratic Congruences, Introduction to Cryptography and Elliptic curves. The purpose of this course is to provide the skills and knowledge required to perform fundamental Mathematical procedures and processes for solution of engineering problems, particularly to use Modular Arithmetic, Primitive Roots and Quadratic Congruences. The course aims at exploring the relevance of Mathematics to Cryptography.

COURSE LEARNING OBJECTIVES (CLO):

The objective is to enable the students to apply the knowledge of Mathematics in various fields of engineering by the following means:

a) Explain the concept of Divisibility and Congruence, Modular Arithmetic, Primitive Roots and Quadratic Congruences, Introduction to Cryptography and Elliptic curves to apply appropriately in solving Engineering problems.

b) Explain how to analyse the system in various Engineering domain using Divisibility and Congruence, Modular Arithmetic, Primitive Roots and Quadratic Congruences, Introduction to Cryptography and Elliptic curves.

Module-I: Divisibility and Congruence

Introduction-Divisibility-Greatest common divisor -Prime numbers - Fundamental theorem of arithmetic (no proof), Euclidean algorithm.

CONGRUENCES: Congruence and basic properties of congruence - Residue classes. Linear congruence, Linear Diophantine Equations and the Chinese Remainder Theorem (no proof).

Module-II: Modular Arithmetic

Euler's Phi function, Properties, Fermat's Theorem, Euler's Theorem, Wilson's Theorem (no proof) and Fermat Numbers, Successive squaring, Finite Fields of order 2^n .

Module-III: Primitive Roots and Quadratic Congruences (I-C)

Primitive Roots: Introduction, definition and properties of primitive roots, existence of primitive roots, Indices.

Quadratic Congruences: Quadratic Congruences, Euler's Criterion (with proof), Quadratic residues, the Legendre Symbol, quadratic Reciprocity (only statement).

Module-IV: Introduction to Cryptography (I-C)

Introduction to Caesar Cipher, Affine Cipher, Hill Ciphers, Robin-Miller Primality test.

Public Key Cryptography: The Diffie Hellman key exchange system, Elgamal encryption, RSA Cryptosystem, Discrete logs.

Module-V: Elliptic Curves

Basic facts of Elliptic curves, Elliptic curve cryptosystems, Elliptic Curve Primality test.

Textbooks:

1. Neal Koblitz, A course in Number Theory and Cryptography, Springer, 1994.
2. Kenneth Ireland and Michel Rosen, A Classical Introduction to Modern Number Theory, Springer, 2013
3. Douglas R. Stinson, Cryptography: Theory and Practice, CRC Press, Third Edition, 2005.
4. David M. Burton, Elementary Number Theory, McGraw Hill Education, Seventh edition, 2014

Reference Books:

1. Lawrence C. Washington, Elliptic Curves Number Theory and Cryptography, Chapman & Hall/CRCTaylor & Francis Group, 2008
2. Menezes, A, et.al. Handbook of Applied Cryptography, CRC Press, 1996
3. Thomas Koshy, Elementary Number Theory with applications, Elsevier India, 2005.

Course Outcomes:

CO1	**Understand** the basic concepts of divisibility and congruence, Number theoretic function, Primitive Roots and Quadratic Congruences, Cryptography and Elliptic Curve
CO2	**Apply** the elementary number theory to cryptography.
CO3	**Analize** the concepts of theoretical basis of number theory and identify how number theory is related and used in cryptography.

SEE - Course Assessment Plan

CO	Marks Distribution					Total Marks	Weightage (%)
	Module-1	Module-2	Module-3	Module-4	Module-5		
CO1	--	6	6	--	6	18	18
CO2	20	7	14	6	14	61	61
CO3	--	7	--	14	--	21	21
	20	20	20	20	20	100	100%

Intra-Module Choice for Answering of Questions	
Module - 3	**Module - 4**
In other modules there will be no choice for answering	