BAPATLA ENGINEERING COLLEGE::BAPATLA

(Autonomous)

MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY

II B. Tech. IV Semester 20CB401/MA05

Lectures	:	2 Hours/Week	Tutorial	:	1 Hour/Week	Practical	:	0
CIE Marks	:	30	SEE Marks	:	70	Credits	:	3

Pre-Requisite: None

Course Objectives: Students will learn how to

➢	Use Euclidean and extended Euclidean algorithms to find GCDof polynomials.
➢	Apply various number theory concepts in solving congruences.
➢	Learn how codes in mathematics are used for error correction and data transmission.
➢	Constructsubstitution ciphers and transposition ciphers.

Course Outcomes: After studying this course, the students will be able to

CO-1	Apply Euclidean algorithm and extended Euclidean algorithm to find GCDof polynomials.
CO-2	Apply various number theory concepts in solving congruences.
CO-3	Utilize linear block codes for error detection and correction.
CO-4	Constructsubstitution ciphers and transposition ciphers.

Mapping of Course Learning Outcomes with Program Outcomes & Program Specific Outcomes

	PO's												**PSO's**		
CO	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**	**3**
CO-1	3	3	2	-	-	-	-	-	-	-	-	3	-	3	-
CO-2	3	3	2	-	-	-	-	-	-	-	-	3	-	3	-
CO-3	3	3	2	-	-	-	-	-	-	-	-	3	-	3	-
CO-4	2	3	2	-	-		-	-	-	-	-	3	-	3	-

UNIT-1

(12 Hours)

Basic Concepts In Number Theory and Finite Fields: Divisibility and The Division Algorithm, The Euclidean Algorithm, Modular Arithmetic, Groups, Rings and Fields, Finite Fields of the form GF(p), Polynomial Arithmetic, Finite Fields of the form GF(2^n)

(**Sections 1 to 7 of Chapter 3 in Textbook 1**)

UNIT-2

(12 Hours)

More on Number Theory: Prime Numbers, Fermat's and Euler's Theorem- Fermat's Theorem, Euler's Totient Function, Euler's Theorem, Testing for Primality- Miller-Rabin Algorithm, A Deterministic Primality Algorithm, Distribution of Primes, The Chinese Remainder Theorem, Discrete Logarithms- The Powers of an Integer, Modulo n, Logarithms for Modular Arithmetic, Calculation of Discrete Logarithms.

(**Sections 1 to 5 of Chapter 7 in Textbook 1**)

UNIT-3	(12 Hours)

Coding Theory:

Introduction to error correcting codes, Basic definitions, Matrix description of Linear Block Codes, Equivalent Codes, Parity Check Matrix, Decoding of a Liner Block Code, Syndrome Decoding,Error Probability after Coding, Perfect Codes, Hamming Codes, Optimal Linear Codes, Maximum Distance Separable codes.

(**Sections 3.1 to 3.12 of Chapter 3 in Textbook 2**)

UNIT-4	(12 Hours)

Cryptography Basics:

Traditional Symmetric – Key Ciphers: Introduction, Substitution ciphers, Transposition ciphers.

(**Sections: 3.1, 3.2, 3.3 of Text Book 3**)

Text Books :	Miller & Freund's "Probability and Statistics for Engineers", Richard A. Johnson, 8th Edition, PHI.
References :	1. Cryptography and Network Security, William Stallings, Pearson, 6th Edition, 2014 2. Information Theory Coding And Cryptography, Ranjan Bose, Tata McGraw-Hill, 4th Edition, 2005. 3. Cryptography & Network Security, Behrouz A. Forouzan, Tata McGraw-Hill, 2010.