MATHEMATICAL FOUNDATION FOR CYBER SECURITY

III Semester: CSE(CS)								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
ACCC01	**Core**	**L**	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
		3	1	0	4	30	70	100
Contact Classes: 45	**Tutorial Classes: 15**	**Practical Classes: Nil**				**Total Classes: 60**		
Prerequisites: **There are no prerequisites to take this course.**								

I. COURSE OVERVIEW:

This course introduces different mathematical concepts in cyber security. The cryptographic algorithms designed by some mathematical algorithms, to use the different keys. Number theory, coding theory are well versed areas in the cyber security. Essentially, coding theory is associated with error correcting codes. This course studies with strong math background to improve Strong analytics and statistical analysis skills that needed.

II. COURSE OBJECTIVES:

The students will try to learn:

I. The basics of mathematical models used in information security.
II. The general understanding of cyber security relationship with numbers
III. The security model and analyze them before being used in many commercial, industrial as well as web application.

III. COURSE OUTCOMES:

After successful completion of the course, students should be able to:

CO 1	**Utilize** the concept of Number theory algorithms to understand and find the GCD of numbers?	Apply
CO 2	**Apply** all the Algebraic properties (CAII) to satisfy the algebraic relations and algebraic congruence’s?	Apply
CO 3	**Explain** the concept of probability that to understand the axioms ofprobability?	Understand
CO 4	**Analyze** the concept of coding theory to implement mathematic formulations in the cryptography?	Analyze
CO 5	**Utilize** the concept of Generator matrix that to implements a way togenerate different codes?	Apply
CO 6	**Explain** the concept of Pseudo random bit generation to implement and achieve error correcting mechanism?	understand

IV. SYLLABUS:

MODULE – I: INTRODUCTION TO NUMBER THEORY (09)

Definition - Divisibility - Greatest common divisor - Prime numbers - Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers - Euclidean algorithm - Fermat’s theorem - Euler totient function - Euler’s theorem. Congruences: Definition - Basic properties of congruences - Residue classes - Chinese remainder theorem.

MODULE – II: ALGEBRAIC STRUCTURE (09)

Algebraic Structures: Groups – Cyclic groups, Cosets, Modulo groups - Primitive roots - Discrete logarithms. Rings – Sub rings, ideals and quotient rings, Integral domains. Fields – Finite fields – GF(pn), GF(2n) - Classification - Structure of finite fields. Lattice, Lattice as Algebraic system, sub lattices, some special lattices.

MODULE – III: PROBABILITY THEORY (09)

Introduction – Concepts of Probability - Conditional Probability - Baye’s Theorem - Random Variables – discrete and continuous- central Limit Theorem-Stochastic ProcessMarkov Chain

Bayesian methods of estimation. Random Processes: general concepts, power spectrum, discrete-time processes, random walks and other applications, Markov chains, transition probabilities.

MODULE - IV: CODING THEORY (09)

Coding Theory: Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Linear codes - Generator matrices and parity-check matrices - Syndrome decoding – Hamming codes - Hadamard Code - Goppa codes.

MODULE - V: PSEUDORANDOM NUMBER GENERATION (09)

Introduction and examples - Indistinguishability of Probability Distributions - Next Bit Predictors - The Blum-Blum-Shub Generator – Security of the BBS Generator.

V. TEXT BOOKS:

1. D. S. Malik, J. Mordeson, M. K. Sen, “Fundamentals of Abstract Algebra, Tata McGraw Hill.
2. P. K. Saikia, “Linear Algebra”, Pearson Education, 2009.
3. Niven, H.S. Zuckerman and H. L. Montgomery, “An Introduction to the Theory of Numbers”, John Wiley and Sons, 2004.
4. D P Bersekas and J N Tsitsiklis, “Introduction to Probability”, Athena Scientific, 2008.
5. C.L. Liu, ‘Elements of Discrete mathematics’, McGraw Hill, 2008.

VI. REFERENCE BOOKS:

1. Douglas Stinson, ‘Cryptography – Theory and Practice’, CRC Press, 2006.
2. Sheldon M Ross, “Introduction to Probability Models”, Academic Press, 2003.
3. Leigh Metcalf, William Casey, “Cybersecurity and Applied Mathematics”, Syngress Publisher(s): Released in June 2016.
4. Chuck Easttom, “Modern Cryptography: Applied Mathematics for Encryption and Information Security”, 1st Edition 2006.

VII. WEB REFERENCES:

1. https://www.amrita.edu/course/mathematical-foundations-cyber-security-systems
2. https://www.oreilly.com/library/view/cybersecurity-and-applied/9780128044995/?code=msdeal
3. https://cybersecurityguide.org/resources/math-in-cybersecurity/