Name of Faculty	:	Faculty of Engineering & Technology
Name of Program	:	Master of Technology (M.Tech.) – Cyber Security
Course Code	:	1MCS01
Course Title	:	Mathematical Foundations of Cyber Security
Type of Course	:	Professional Core
Year of Introduction	:	2023-24

Prerequisite	:	Basic knowledge of Computer Network and Basic mathematics
Course Objective	:	Master Number Theory, Probability, Algebraic Structures, and Coding for versatile mathematical problem-solving.
Course Outcomes	:	At the end of this course, students will be able to:
	CO1	To learn about Number theory including Divisibility, Greatest common divisor and prime numbers
	CO2	To understand and apply Euclidean algorithm, Fermat's theorem and Euler's theorem
	CO3	To understand the concept of Algebraic structure including Groups, Rings, Fields and Classifications.
	CO4	To calculate probability based on Baye's theorem.
	CO5	To calculate probability for discrete random variables and continuous random variables.
	CO6	To apply the concept of Coding.
	CO7	To use Pseudorandom number generation for Next Bit Predictors and Blum-Blum-Shub Generator

Teaching and Examination Scheme

Teaching Scheme (Contact Hours)			Credits	Examination Marks				
				Theory Marks		Practical Marks		Total Marks
L	**T**	**P**	**C**	**SEE**	**CIA**	**SEE**	**CIA**	
4	2	0	5	70	30	30	20	150

*Legends: **L**-Lecture; **T**–Tutorial/Teacher Guided Theory Practice; **P** – Practical, **C** – Credit, **SEE** – Semester End Examination, **CIA** - Continuous Internal Assessment (It consists ofAssignments/Seminars/Presentations/MCQ Tests, etc.))*

Course Content

Unit No.	Topics	Teaching Hours	Weightage	Mapping with CO
1	**Introduction to Number Theory:** Introduction – Divisibility – Greatest common divisor –Primes – Primes numbers – Cardinality	08	20%	CO1

	of Primes, Fundamental theorem of arithmetic – Mersenne primes, Fermat numbers, Fermat's and Euler's Theorem, Testing for Primality, Factorization, The Chinese Reminder Theorem, Quadratic Congruence, Exponentiation and Logarithms, Discrete Logarithms			
2	**Algebraic Structures and Finite Fields:** Groups, cyclic groups, Co sets, Modulo groups, Primitive roots, Discrete logarithms The Euclidean Algorithm, Modular Arithmetic, Algebraic Structures Groups, Rings and Fields, Future Fields of the Form GF(2"), Polynomial Arithmetic, Finite Fields of the Form Gf(2^n)	06	15%	CO2
3	**Pseudorandom Number Generation and Stream Ciphers:** Principles of Pseudorandom Number Generation, Principles of Pseudorandom Number Generation using Block Cipher, Stream Ciphers, RC4, True Random Number Generators	05	15%	CO7
4	**Discrete Mathematics for Cryptography:** Cryptography and Modular Arithmetic, Inverses & GCDs, The RSA Cryptosystems, Mathematical Induction, Recursion, Recurrences and Induction, Recurrences and Selection	04	10%	CO5
5	**Coding Theory**: Introduction, basic concepts: codes, minimum distance, equivalence of codes, Linear codes, Generator matrices and parity check matrices, Syndrome decoding, Hamming codes, Handamard Code, Goppa codes	05	15%	CO6
6	**Probability Theory:** Introduction, concepts of probability, conditional probability, Baye's theorem, random variables, discrete and continuous, central Limit Theorem, Stochastic Process, Markov Chain	04	15%	CO4
7	**Cryptographic Hash Functions:** Application of Cryptographic Hash functions, Two simple hash functions, Requirements and security, Hash functions based on cipher block chaining, secure hash functions, SHA-512	04	10%	CO5

Suggested Distribution of Theory Marks Using Bloom's Taxonomy						
Level	Remembrance	Understanding	Application	Analyse	Evaluate	Create
Weightage	**20**	**30**	**30**	**20**	**0**	**0**

NOTE: This specification table shall be treated as a general guideline for the students and the teachers. Theactual distribution of marks in the question paper may vary slightly from above table.

Suggested List of Experiments/Tutorials

Sr. No.	Name of Experiment/Tutorial	Teaching Hours
1	Find greatest common divisor for following: 1. gcd(2,4), 2. gcd(6,9), 3. gcd(124,72) 4. gcd(748, 2024)	04
2	Find x,y,€ Z such that ax + by = gcd(a,b)?	04
3	Explain Fundamental theorem of arithmetic.	04
4	Find integer x,y such that 5*x + 7*y = 1	04
5	Find integer x,y such that 27*x + 42*y = gcd(27,42)	04
6	Using CRT to Simplify Modulo Computations calculate 3299 mod 24	04
7	Using CRT to simplify modulo computation calculation 12345*12345 mod 35	04
8	Using Fermat's little theorem solve 11^{17} mod 3	04
9	Explain Properties of Group	04
10	Which integers belongs to z?	04
11	Explain Conditional probability	04
12	What is expected outcomes of rolling a dice?	04
13	Rolling a fair dice, what is the expectation of the square of the outcomes?	04
14	What is the expected output about rolling a dice Twice?	04
15	What are the application of Cryptographic Hash Functions?	04

Suggested Learning Websites

Sr. No.	Name of Website
1	https://www.coursera.org/learn/mathematical-foundations-cryptography
2	https://cybersecurityguide.org/resources/math-in-cybersecurity/

Reference Books

Sr. No.	Name of Reference Books
1	Introduction to Probability Models by Sheldom M Ross, Academic Press
2	Contemporary Abstract Algebra by Joseph A Gallian – Narosa
3	Cryptography and Network security by William Stallings 5^{th} edition of pearson education