SCHEME OF COURSE WORK

Course Details:

Course Title	**: COMPUTATIONAL NUMBER THEORY**		
Course Code	**:13CS2204**	**L T P C**	**:4 0 0 3**
Program:	**: M.Tech.**		
Specialization:	**: Cyber Security**		
Semester	**:Ist Semester**		
Prerequisites	**:Number theory basics,Security issues.**		
Courses to which it is a prerequisite	**:Number theory basics,Security issues.**		

Course Outcomes (COs):

1	Develop the mathematical skills to solve number theory problems and to develop the mathematical skills of divisions, congruences, and number functions.
2	Learn the history of number theory and its solved and unsolved problems.
3	Investigate applications of number theory and the use of computers in a Number theory.
4	Estimate the time and space complexities of various Secure Algorithms.
5	Learn various factorization and logarithmic methods.

Program Outcomes (POs):

A graduate of Cyber Security Specialization will be able to

1	Understand what are the common threats faced today.
2	The foundational theory behind Cyber security
3	The basic principles and techniques when designing a secure system,
4	How to think adversarial, how today's attacks and defenses work in practice, how to assess threats for their significance, and how to gauge the protections and limitations provided by today's technology
5	The basic principles and techniques in ethical hacking and overcome various hackers
6	Learn various security methodologies to enhance the security of web.
7	Basic principles of cyber laws and security policies
8	Various scripting languages to develop programs for security mechanisms.
9	Various tools and methodologies to analyze the various cyber crimes
10	Secure protocols inner mechanisms and their practical implementation
11	Various Forensic technologies and methodologies for security measurements analyzation.
12	.Intrusion detection techniques and image model security aspects in Android application developments.

Course Outcome versus **Program Outcomes:**

COs	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
CO-1			S			S						
CO-2	M	M	S							S		M
CO-3			M							S		M
CO-4		S		S								
CO-5												S

S - Strongly correlated, *M - Moderately* correlated, *Blank - No correlation*

Assessment Methods:	Assignment / Quiz / Seminar / Case Study / Mid-Test / End Exam

Teaching-Learning and Evaluation

Week	TOPIC / CONTENTS	Course Outcomes	Sample questions	TEACHING-LEARNING STRATEGY	Assessment Method & Schedule
1	Topics in elementary number theory: O and Ω notations – time estimates for doing arithmetic – divisibility and the Euclidean algorithm – Congruence‟s: Definitions and properties .	CO-1	1.EXplain Ω and O notations. 2.Describe the Euclidean algorithms.	▫ Lecture ▫ Demonstration	Assignment (Week 3 - 4)
2	linear congruences , residue classes, Euler‟s phi function.	CO-1	1.explain linear congruence.	▫ Lecture / Discussion ▫ Programs implentation	Mid-Test 1 (Week 9)
3	Fermats Little Theorem – Chinese Remainder Theorem – Applications to factoring – finite fields	CO-2	1.explain fermat's little theorem.	▫ Lecture ▫ Programs implementation	Seminar (Week 3 - 6)
4	quadratic residues and reciprocity: Quadratic residues – Legendre symbol – Jacobi symbol. Enciphering Matrices – Encryption Schemes – Symmetric and Asymmetric Cryptosystems	CO-3,CO-4	1.explain symmetric and asymmetric cryptosystems.		
5	Cryptanalysis – Block ciphers –Use of Block Ciphers.	CO-3	1. Explain the uses of block ciphers		
6	Multiple Encryption – Stream Ciphers –Affine cipher – Vigenere, Hill, and Permutation Cipher – Secure Cryptosystem.	CO-3,CO-4	1.Explain stream ciphers.		
7	Public Key Cryptosystems: The idea of public key cryptography – The Diffie–Hellman Key Agreement Protocol	C0-4	1explain Diffie Hellman key agreement protocol. **2014**		
8	RSA Cryptosystem – Bit security of RSA – ElGamal Encryption	CO-4	1.Explain ElGamal Encryption process		
9	**Mid-Test 1**	CO-1,CO-2			
10	Discrete Logarithm – Knapsack problem – Zero-Knowledge Protocols	CO-3	1.describe Discrete logarithm.	▫ Lecture ▫ Discussion	Mid-Test 2 (Week 18)
11	From Cryptography to Communication Security - Oblivious Transfer.	CO-3	1.Write down the description about cryptography to communication security.		Seminar (Week 10 - 15)
12	Primality and Factoring: Pseudo primes – the rho (γ) method – Format factorization and factor bases	CO-3	1.explain the rho method format factorization		
13	The continued fraction method – the quadratic sieve method.	CO-3	1.explain quadratic sieve method with example		
14	Number Theory and Algebraic	CO-5	1.Describe the basic Elliptic curves		

	Geometry: Elliptic curves – basic facts				
15	elliptic curve cryptosystems	CO-5	1.explain the Elliptic curve cryptosystems		
16	elliptic curve primality test	CO-5	1.Define primality test in elliptic curve		
17	elliptic curve factorization.	CO-5	1.decribe factorization in elliptic curve .		
18	**Mid-Test 2**				
19/20	**END EXAM**				