Course Type	Course Code	Name of Course	L	T	P	Credit
DE	NCSD515	**Number Theory and Cryptography**	3	0	0	3

Course Objective
To understand the basics of Number Theories related to the underlying mathematics of Cryptographic techniques namely message Confidentiality, Integrity, Availability (CIA) etc. along with the further research in these areas.
Learning Outcomes
To understand the applications of number theory in cryptographic aspects and cyber security protections. It also helps in developing new cryptographic techniques for better security of our applications.

Unit No	Topics to be Covered	Lecture Hours	Learning Outcome
1	Fundamentals: Basic Algebraic Structures, Divisibility Theory, Arithmetic Functions, Congruence Theory, Primitive roots, Elliptic Curves.	7	Understanding the basics of mathematics and algebraic structures used in cryptography
2	Primes and Primality Testing: Primes- The Euclidean Algorithm, Primes and factorization, Distribution of primes, Prime number theorem. Primality Testing- Basic Tests, Fermat & Euler Tests, Miller-Rabin Test, Elliptic Curve Tests, AKS Test.	6	Understanding the different primes, modular arithmetic and congruence relation.
3	Integer Factorization: Basic Concepts, Trial Divisions Factoring, ρ and ρ-1 methods, Elliptic Curve method, Continued Fraction method, Quadratic Sieve, Number Field Sieve.	5	Understanding basics of integer factorization
4	Discrete Logarithms: Basic concepts, Baby-Step Giant-step method, Pohlig-Hellman method, index calculus, Elliptic Curve Discrete Logarithms.	5	Understanding the basic concept of discrete logarithm and its related algorithms.
5	Integer Factorization based Cryptography: RSA Cryptography, Cryptanalysis of RSA, Rabin Cryptography, Residuosity based Cryptography, Zero-Knowledge Proof.	6	Understanding the cryptographic techniques based on integer factorization.
6	Discrete Logarithm based Cryptography: Diffie-Hellman_Merkle Key exchange Protocol, ElGamal Cryptography, Massey-Omura Cryptography, DLP-Based Digital Signatures, Blind Signature	6	Understanding the cryptographic techniques based on discrete logarithm.
7	Elliptic Curve Discrete Logarithm based Cryptography: Basic Ideas, Elliptic Curve Diffie-Hellman-Merkle Key Exchange Scheme, Elliptic Curve Massey-Omura Cryptography, Elliptic Curve ElGamal Cryptography, Elliptic Curve RSA Cryptosystem, Menezes-Vanstone Elliptic Curve Cryptography, Elliptic Curve DSA.	7	Understanding the cryptographic techniques based on elliptic curve discrete logarithm.
	Total	42	

Text Books:

1. A Course in Number Theory and Cryptography By Neil Koblitz
2. Computational Number Theory and Modern Cryptography By Song Y. Yan
3. Lecture notes Number Theory and Cryptography Matt Kerr

Reference Books:

1. W. Trappe and L. Washington, "Introduction to Cryptography with Coding Theory", Pearson Prentice Hall.
2. B. Forouzan and D. Mukhopadhyay, "Cryptography and Network Security", McGraw Hill Education.
3. D. Stinson, "Cryptography: Theory and Practice", Chapman and Hall/CRC.