Course Type	Course Code	Name of Course	L	T	P	Credit
DC (Hons)	**NCSH401**	**NUMBER THEORY AND CRYPTOGRAPHY**	3	1	0	4

Course Objective

To understand basics of Number Theory and Cryptography and to learn how to maintain the Confidentiality, Integrity, and Availability (CIA) of the data along with modern algorithms in number theory.

Learning Outcomes

To understand both theoretical and practical knowledge in cryptographic aspects. To do research in the new emerging areas of number theory and cryptography while implementing the related security protocols.

Unit No.	Topics to be Covered	Lecture+ Tutorial	Learning Outcome
1	Fundamentals: Basic Algebraic Structures, Divisibility Theory, Arithmetic Functions, Congruence Theory, Primitive roots, Elliptic Curves.	6+2	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+2	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+2	Understanding basics of integer factorization
4	Discrete Logarithms: Basic concepts, Baby-Step Giant-step method, Pohlig-Hellman method, index calculus, Elliptic Curve Discrete Logarithms.	6+2	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+2	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.	6+2	Understanding the cryptographic techniques based on discrete logarithms.
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+2	Understanding the cryptographic techniques based on elliptic curve discrete logarithm.
			Total: 42 (L) + 14 (T)

Text Books:

1. Neil Koblitz, “A Course in Number Theory and Cryptography”, Springer
2. Song Y. Yan, “Computational Number Theory and Modern Cryptography”, Wiley

Reference Books:

1. Matt Kerr, “Lecture notes Number Theory and Cryptography”, Online Available