Course Type	Course Code	Name of Course	L	T	P	Credit
DC (Hons)	**NCSH402**	**NUMBER THEORY AND CRYPTOGRAPHY LABORATORY**	0	0	3	1.5

Course Objective

To provide hands-on experience in implementing cryptographic algorithms, understanding their mathematical foundations, and analyzing security protocols based on number theory.

Learning Outcomes

Upon successful completion of this lab, students will:

- Gain practical knowledge in implementing cryptographic algorithms.
- Understand the computational aspects of number theory in cryptography.
- Learn to analyze and compare different cryptographic techniques.
- Develop proficiency in using cryptographic libraries and tools.

Unit No.	Topics to be Covered	Practical Hours	Learning Outcome
1	**Fundamentals of Number Theory:** Implementing arithmetic functions, modular arithmetic, congruences, and primitive roots.	3	Understanding algebraic structures and modular computations.
2	**Primes and Primality Testing:** Implementation of Euclidean Algorithm, Primality Tests: Fermat, Miller-Rabin, AKS	6	Understanding prime number testing methods and their security implications.
3	**Integer Factorization Techniques:** Implementing Trial Division, Pollard's ρ-method, and Quadratic Sieve.	6	Understanding how integer factorization techniques apply to cryptanalysis.
4	**Cryptographic Protocols Based on Integer Factorization:** Implementing RSA Cryptosystem, Various attacks on RSA, Rabin Cryptosystem, ZKP protocols.	6	Understanding the security of Rabin and RSA, ZKP protocols.
5	**Cryptographic Protocols Based on Discrete Logarithm:** Implementing Diffie-Hellman Key Exchange, ElGamal Cryptosystem, El Gamal Cryptosystem, Massey-Omura cryptosystem.	9	Understanding the security of cryptosystems based on discrete logarithms.
6	**Elliptic Curve Cryptography (ECC):** Implementing Diffie-Hellman-Merkle Key exchange, Massey-Omura cryptosystem, ElGamal cryptosystem, RSA Cryptosystem, DSA, Menezes-Vanstone cryptosystem.	12	Understanding the security of cryptosystems based on Elliptic Curve.
			Total: 42

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