CourseType	Course Code	Name of Course	L	T	P	Credit
DE	**NMCD501**	Cryptography	3	0	0	3

Course Objective
• To understand the classical and modern cryptosystems for secure encryption and decryption.
Learning Outcomes
• The students will be able to understand the basic idea of encryption and decryption schemes.

Unit No.	Topicsto be Covered	Contact Hours	Learning Outcome
1	Brief introduction to number theory, Euclidean algorithm, Euler’s totient function, Fermat’s theorem and Euler’s generalization, Chinese Remainder Theorem, primitive roots and discrete logarithms, Quadratic residues, Legendre and Jacobi symbols.	9	Students will learn the basics of number theory.
2	Cryptography and cryptanalysis, classical cryptosystems, concept of block and stream ciphers, private and public key cryptography. Encryption standard: DES and differential and linear cryptanalysis, Advanced encryption standards.	9	Students will be able to understand classical and public key encryption and decryption techniques.
3	RSA public key cryptosystems: RSA system, primality testing. Diffe-Hellman key exchange system. Massey-Omura cryptosystem for message transmission	6	Students will learn RSA cryptosystems and Massey-Omura cryptosystem for message transmission.
4	Other public key cryptosystems: El Gamal public key cryptosystem, algorithms for discrete log problem, Knapsack public key cryptosystems.	6	Students will learn El Gamal and Knapsack cryptosystems and discrete log problem.
5	Digital signature and hash functions: El Gamal signature scheme, digital signature standard, onetime undeniable and fail-stop signatures, computationally collision-free hash functions, extending hash functions, examples of hash functions. Introduction to elliptic curves, basic facts, elliptic curve cryptosystems.	12	The students will be able to understand different signature schemes and properties of hash functions and their applications. Students will be able to understand basics of elliptic curves and their applications in designing cryptosystems
Total		**42**	

Text Book:

1. N. Koblitz, A Course in Number Theory and Cryptography, 2nd Edition, 1994

Reference Books:

1. J. Hoffstein, J. Pipher, J. H. Silverman, An Introduction to Mathematical Cryptography, Springer, 2008.
2. J. Buchmann, Introduction to Cryptography, 2nd Edition, Springer, 2012.