APPENDIX - X

Course Type	Course Code	Name of Course	L	T	P	Credit
DC10	MCC301	Number Theory and Cryptography	3	0	0	9

Course Objective
To understand (i) the basics of number theory and (ii) classical and modern cryptosystems for secure encryption and decryption.
Learning Outcomes
Upon successful completion of this course, students will: 1. be able to understands basics of number theory and their different applications. 2. be able to understand the basic idea of encryption and decryption schemes.

Unit No.	Topics to be Covered	Lecture Hours	Learning Outcome
1	Time estimates, Divisibility and the Euclidean algorithm	5	Students will be able to compute to time complexity of an algorithm. This unit will also help students to understands basics of number theory
	Congruences, Fermat's Little Theorem, Euler's Theorem, Chinese Remainder Theorem, Some applications to factoring	6	
2	Finite fields	3	This unit will help students to understand the basic idea of finite fields, quadratic residues and primality testing.
	Quadratic residues and reciprocity, Primality Testing	5	
3	Some simple cryptosystems, Enciphering matrices, DES, AES	7	Students will be able to understand classical and private key encryption and decryption techniques.
4	The idea of public key cryptography, Classical versus public key, RSA	4	This unit will help students to understand public key cryptosytem, cryptosystems based on discrete log and digital signature schemes.
	Discrete log, Diffie-Hellmann key exchange system, Massey-Omura cryptosystem for message transmission, ElGamal cryptosystem	5	
	Hash functions, RSA signature schemes, ElGamal digital signature scheme, Digital signature standard. Knapsack problems.	3	
5	Introduction to elliptic curves, Elliptic curve cryptosystems, Elliptic curve primality test.	4	Students will be able to understand basics of elliptic curves and their applications in designing cryptosystems and primality testing,

Text Books:

1. Neal Koblitz, A Course in Number Theory and Cryptography (Second edition), Springer, 1994.

Reference Books:

1. D. M. Burton, Elementary Number Theory (Seventh edition), McGraw Hill Education, 2017.
2. **J. Hoffstein**, J. **Pipher**, J.H. **Silverman**, An Introduction to Mathematical Cryptography (First edition), Springer, 2008.