INDIANINSTITUTE OF INFORMATION TECHNOLOGY
DESIGN AND MANUFACTURING (IIITDM) KANCHEEPURAM

INTRODUCTION OF NEW COURSE

Course Title	**An introduction to Cryptography**	Course No	MAT503			
Specialization	CSE/ECE/MEC/PHY/MAT	Structure (LTPC)	3	0	0	3
To be offered for	UG/PG	Status	Core ☐		Elective ■	
Faculty Proposing the course	M. Subramani	Type	New ■		Modification ☐	
Date of DAC		Members Present in DAC				
		External Member:				
Pre-requisite	Engineering Mathematics	Submitted for approval	44th Senate			
Learning Objectives	This course will be an introduction to cryptography and cryptanalysis.					
Learning Outcomes	Will be able to implement various cryptosystems and digital signature schemes, and understand their basic decryption and security pitfalls, including for RSA and El Gamal public key systems.					
Contents of the course *(With approximate break-up of hours)*	Modular arithmetic, Euclidean algorithm and its generalizations, quadratic residues laws, primality testing, integer factorization, finite fields [10] Introduction to simple cryptosystems, cryptanalysis, Public key cryptography, Hash function, RSA cryptosystem, Pseudo primes, Pollard's p-1 method, the Rho method [10] The ElGamal cryptosystem, Diffee-Hellman key exchange system, discrete logarithm problem- Shank's algorithm, The Pollard Rho algorithm, The Pohlig-Hellman Algorithm, ElGamal systems, The ElGamal signature scheme [10] Introduction Elliptic curve, Elliptic curve cryptography, Elliptic curve primality test, Elliptic curve factorization [12]					
Text Books	1. Cryptography : theory and practice, Stinson, Douglas R, Paterson, Maura B, Fourth edition, CRC Press, Taylor & Francis Group, 2018.					
Reference Books	1. An introduction to Mathematical cryptography, Jeffery Hoffstein, Jill Pipher, J.H. Silverman, First edition, Springer, 2008. 2. A course in Number Theory and Cryptography, Neal Koblitz, Second edition, Springer, 1994.					