Devi Ahilya University, Indore, India Institute of Engineering & Technology				MSc – II Year (Applied Mathematics) with Specialization in Computing & Informatics Semester- IV			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
AM4EM3: Number Theory/ Cryptography	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
	3	**1**	**-**	**3**	**1**	**-**	**4**
Duration of Theory Paper: 3 Hours							

Learning Objectives:

- The course aims to give elementary ideas from number theory which will have applications in cryptology.
- Identify and apply various properties of and relating to the integers including the Well-Ordering Principle, primes, unique factorization, the division algorithm, understand the concept of a congruence,
- To impart the knowledge of encryption and decryption techniques and their applications in managing the security of data.

Prerequisites: Set theory, algebra of functions.

COURSE OF CONTENTS

UNIT I

Divisibility and Euclidean algorithm, congruences, applications to factoring.

UNIT II

Finite fields, Legendre symbol and quadratic reciprocity, Jacobi symbol.

UNIT III

Cryptosystems, diagraph transformations and enciphering matrices, Symmetric key cryptosystem, traditional techniques, Key range and size, Deffie-Hellman key exchange, various types of attacks, algorithm types and modes, various symmetric key algorithms (DES, IDEA, RC5, Blowfish)

UNIT IV

Asymmetric key cryptography,concept, RSA algorithm, digital envelope, concept of message digest, MD5 algorithm, Authentication requirements, Digital signatures, message authentic codes, Knapsack algorithm.

UNIT V

Primality and Factoring, Pseudoprimes, Carmichael number, Primality tests, Strong Pseudoprimes, Monte Carlo method, Fermat factorization, Factor base, Implication for RSA, Continued fraction method. Elliptic curves - basic facts, Elliptic curve cryptosystems.

Learning Outcomes:

Upon completing the course, students will be able to:

- Solve problems in elementary number theory.
- Apply elementary number theory to cryptography.
- Develop a deeper conceptual understanding of the theoretical basis of number theory and identify how number theory is related to and used in cryptography.

BOOKS REOMMENDED:

[1] Neal Koblitz, A Course in Number Theory and Cryptology, Graduate Texts in Mathematics, Springer, 1994.
[2] Williams Stallings, Cryptography & Network Security, Pearson Education 3rd edition, 2004.
[3] Atul Kahate, Cryptography & Network Security, Tata McGraw Hill, New Delhi, 2005.
[4] Thomas Koshy, Elementary Number Theory with Applications, Academic Press, 2007.