Devi Ahilya University, Indore, India Institute of Engineering & Technology				IV Year B.E. Information Technology (Full Time)			
Subject Code & Name **ITR8E4** **Cryptography and Computational number theory**	**Instructions Hours per Week**			**Credits**			
	L	**T**	**P**	**L**	**T**	**P**	**Total**
	3	**1**	**1**	**3**	**1**	**1**	**5**
Duration of Theory Paper: **3 Hours**							

Learning Objectives: To learn the application of number theory in the design of cryptographic algorithm.

Prerequisite: Knowledge of Algorithms and Discrete mathematics.

UNIT – I

Notion of algorithms, types of algorithms, Analysis – Best case, worst case, average case. Performance issues – Time and space complexity, Asymptotic notations, Mathematical preliminaries, functions and their growth rates, Recurrence relations and their solving methods,

UNIT – II

Elementary of number theory, GCD computations, Euclids algorithms, finite groups, subgroups, primitive roots, generator computation, modular arithmetic, solving modular linear equations, modular exponentation, remainder theorem, Discrete Logarithmic problem, quadratic residues.

UNIT – III

Key Exchange, Diffie Hellman key exchange, Cryptosystems based on discrete log, public key Cryptosystems and RSA, choice of the public key, attacks on RSA and remedies, rabin Cryptosystems.

UNIT – IV

Factorization, current state of the art, large prime variant, Dixon's factorization method, quadratic sieve factoring, pollard-Rho method, pollard-Rho analysis, Primality Testing, Fermat Primality Test, AKS Primality Tes.

UNIT – V

Eliptic curves cryptography, Eliptic curves and finite fields, Eliptic curve encryption and decryption, ECDLP, Zero knowledge proof, cryptographic Hash function, Digital signature, authentication protocols,vproxy signature, Elgamal Digital signature scheme, Blind and prony signature, video data cippers

Recommended Books:

1. Introduction to Algorithms: T. H. Cormen, C. E. Leiserson, R. Rivest and C. Stein Prentice Hall India, 2 nd Edition, 2002.
2. Cryptography and Network security: Principles and Practice, William Stallings, Pearson Education, 2002.

3. Cryptography: Theory and Practice, Douglas R. Stinson, CRC Press.

Learning Outcomes:

Upon completing the course, students will be:

- Familiar with Basics of number theory and its application in cryptography.
- Able to apply skills for writing programs for cryptography algorithms.

List of Assignments:

1. Implementation of various symmetric key algorithms in detail and study of their complexities.
2. Implementation of various asymmetric key algorithms in detail and study of their complexities.
3. Implementation of digital certificates using any programming language
4. Implementation of various open source security tools