SEMESTER S8

COMPUTATIONAL NUMBER THEORY

(Common to CS/CM)

Course Code	**PECST869**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:0:0:0	**ESE Marks**	60
Credits	3	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	PCCST205 PCCST303 PCCST502	**Course Type**	Theory

Course Objectives:

1. To develop proficiency in key algorithms for number-theoretic operations, including primality testing, integer factorization, and modular exponentiation and to analyze and implement these algorithms efficiently to solve problems in number theory and cryptography.
2. To apply advanced computational techniques, such as elliptic curve cryptography and lattice-based methods, to address complex problems in cryptographic systems and gain practical skills to implement and evaluate these techniques within real-world security applications.

SYLLABUS

Module No.	Syllabus Description	Contact Hours
1	Introduction to Number Theory - Basic concepts and definitions, Greatest common divisor (GCD) and Euclidean algorithm; Modular Arithmetic - Congruences and modular arithmetic, Applications of modular arithmetic; Integer Factorization - Prime numbers and factorization, Algorithms for integer factorization; Basic Algorithms - Algorithms for modular arithmetic, Fast exponentiation techniques	**9**
2	Advanced Factorization Algorithms - Pollard's rho algorithm, Elliptic curve factorization; Public-Key Cryptography - RSA algorithm, Security analysis of RSA; Elliptic Curve Cryptography - Introduction to elliptic curves, Algorithms for elliptic curve cryptosystems	**9**
3	Public Key Cryptography - RSA algorithm and its implementation, Security aspects and cryptanalysis; Elliptic Curve Cryptography - Basics of elliptic curves, Elliptic curve cryptosystems; Cryptographic Protocols - Key	**9**

	exchange protocols, Digital signatures and authentication	
4	Algebraic Number Theory - Algebraic integers and number fields, Factorization in number fields; Computational Methods - Algorithms for solving Diophantine equations, Applications in computational algebra; Recent Developments and Applications - Applications in modern cryptography and coding theory	**9**

Course Assessment Method
(CIE: 40 marks, ESE: 60 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	**15**	**10**	**10**	**40**

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24 marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 subdivisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Understand basic number theory concepts and algorithms.	**K2**
CO2	Apply factorization algorithms to solve computational problems.	**K3**
CO3	Analyze and evaluate cryptographic systems based on number theory.	**K4**
CO4	Synthesize algebraic number theory concepts into computational methods.	**K4**
CO5	Create and present a project on recent advances and applications in computational number theory.	**K4**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	3									2
CO2	3	3	3									2
CO3	3	3	3	3	3							2
CO4	3	3	3	3	3					2	2	2
CO5	3	3	3									2

Note: *1: Slight (Low), 2: Moderate (Medium), 3: Substantial (High), -: No Correlation*

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	A Computational Introduction to Number Theory and Algebra	Victor Shoup	Cambridge University Press	2/e, 2008

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Computational Number Theory and Modern Cryptography	Song Y. Yan	John Wiley & Sons	1/e, 2013
2	A course in computational algebraic number theory	Henri Cohen	Springer-Verlag	4/e, 2000
3	Computational Number Theory	Abhijit Das	CRC	1/e, 2013
4	Modern Computer Algebra	Joachim von zur Gathen and Jürgen Gerhard	Cambridge University Press	4/e, 2013
5	An Introduction to the Theory of Numbers	G. H. Hardy, Edward M. Wright, Roger Heath- Brown and Joseph Silverman	Oxford University Press	6/e, 2008

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://archive.nptel.ac.in/courses/111/104/111104138/ https://archive.nptel.ac.in/courses/106/103/106103015/
2	https://archive.nptel.ac.in/courses/111/104/111104138/ https://archive.nptel.ac.in/courses/106/103/106103015/
3	https://archive.nptel.ac.in/courses/111/104/111104138/ https://archive.nptel.ac.in/courses/106/103/106103015/
4	https://archive.nptel.ac.in/courses/111/104/111104138/ https://archive.nptel.ac.in/courses/106/103/106103015/