GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Post Graduate Diploma

Level: PG Diploma

Branch: Cyber Security

Subject Code : PI01001041

Subject Name : Computational Number Theory and Cryptography

w. e. f. Academic Year:	2025-26
Semester:	1
Category of the Course:	Core Course

Course Outcome:

After Completion of the Course, Student will able to:

No	Course Outcomes
CO-1	To learn about Number theory including Divisibility, Greatest common divisor and Prime numbers.
CO-2	To understand and apply Euclidean algorithm, Fermat's theorem and Euler's theorem.
CO-3	To calculate probability for discrete random variables and continuous random variables.
CO-4	To apply the concept of Coding.
CO-5	To use pseudorandom number generation for Next Bit Predictors and Blum Blum-Shub Generator.

Teaching and Examination Scheme:

Teaching Scheme (in Hours)			Total Credits L+T+ (PR/2)	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial / Practical		
L	T	PR	C	ESE (E)	PA / CA (M)	PA/CA (I)	ESE (V)	
4	0	2	5	70	30	20	30	150

Course Content:

Sr. No.	Content	Teaching Hours	Module Weightage (%)
1	**Introduction to Number Theory:** Introduction-Divisibility-Greatest common divisor - Primes- Prime numbers - Cardinality of Primes, Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers, Fermat's and Euler's Theorem, Testing for Primality, Factorization, , Chinese Reminder Theorem, Quadratic Congruence, Exponentiation and Logarithms, Discrete logarithms.	**10**	**20**

2	**Pseudorandom Number Generation and Stream Ciphers :** Principles of Pseudorandom Number Generation, Principles of Pseudorandom Number Generation using a Block Cipher, Stream Ciphers, RC4 , True Random Number Generators	**08**	**15**
3	**Discrete Mathematics for Cryptography:** Cryptography and Modular Arithmetic, Inverses & GCDs, The RSA Cryptosystems, Mathematical Induction, Recursion, Recurrences and Induction, Recurrences and Selection	**05**	**10**
4	**Coding Theory:** Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes, Generator matrices and parity-check metrics - syndrome decoding- Hamming codes - Hadamard Code - Goppa codes	**08**	**15**
5	**Cryptographic Hash Functions:** Application of Cryptographic Hash Functions, Two Simple Hash functions , Requirements and Security, Hash Functions Based on Cipher Block Chaining, Secure Hash Functions (SHA), SHA-512	**05**	**10**
6	**Probability Theory:** Introduction - Concepts of Probability - Conditional Probability -Baye's Theorem - Random Variables - discrete and continuous- central Limit Theorem-Stochastic Process- Markov Chain.	**07**	**15**

References/Suggested Learning Resources:

(a) Books:

1. Sheldon M Ross, "Introduction to Probability Models, Academic Press, 2003.
2. Joseph A. Gallian, "Contemporary Abstract Algebra', Narosa, 1998.
3. Cryptography and Network Security by William Stallings 5th Edition Pearson Education.
4. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, 'An introduction to the theory of numbers', John Wiley and Sons 2004.
5. C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.
6. Cryptography and Network Security by Behrouz A. Forouzan TMH Publication

****