Engineering Mathematics - IV
(Number Theory and Cryptography)

Course Code	19BS1403	**Year**	II	**Semester**	II
Course Category	Basic Sciences	**Branch**	CSE	**Course Type**	Theory
Credits	3	**L-T-P**	3-0-0	**Prerequisites**	Mathematics, Algebra
Continuous Internal Evaluation :	30	**Semester End Evaluation:**	70	**Total Marks:**	100

Course Outcomes		
Upon successful completion of the course, the student will be able to:		
CO1	Understand the fundamental concepts of number theory and cryptography	**L2**
CO2	Apply substitution/transposition techniques to design classical encryption ciphers	**L3**
CO3	Apply appropriate cryptographic algorithm for a given scenario and make an effective report	**L3**
CO4	Apply cryptographic hash functions for message authentication.	**L3**

Contribution of Course Outcomes towards achievement of Program Outcomes & Strength of correlations (3:Substantial, 2: Moderate, 1:Slight)

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	3													
CO2	3													
CO3	3								3	3				
CO4	3													

Course Content		
UNIT-1	**Basic Concepts in Number Theory:** Divisibility and the Division Algorithm, The Euclidean Algorithm, Modular arithmetic, Prime numbers, Fermat's Theorem and Euler's Theorems (without proofs), Testing for Primality, The Chinese Remainder Theorem (without proofs), Discrete Logarithms.	**CO1**
UNIT-2	**Classical Encryption Techniques :** Symmetric Cipher Model, Substitution Techniques-Caesar Cipher, Monoalphabetic Cipher: Playfair, Hill Ciphers, Polyalphabetic Ciphers, Onetime Pad, Transposition Techniques.	**CO1,CO2**
UNIT-3	**Block Ciphers:** Traditional Block Cipher Structure, The Data Encryption Standard, Advanced Encryption Standard, Block Cipher modes of operations.	**CO1,CO3**
UNIT-4	**Public Key Cryptography**: Principles of Public-Key Cryptosystems, The RSA Algorithm, Diffie-Hellman Key Exchange- The Algorithm, Key Exchange Protocols, Man-in-the-Middle Attack.	**CO1,CO3**
UNIT-5	**Cryptographic Hash Functions**: Applications of Cryptographic Hash Functions, Two Simple Hash Functions, Message Authentication Requirements, Message Authentication Functions, MACs based on Hash functions: HMAC	**CO1,CO4**

Learning Resources

Text books

1. Cryptography and Network Security- Principles and Practice, William Stallings, Sixth Edition, 2014, Pearson.

References

1. An Introduction to the Theory of Numbers, Ivan Niven, Herbert S. Zukerman, Hugh L. Montgomery, Fifth Edition, 2008, Wiley.
2. Cryptography: Theory and Practice, Stinson. D, Third Edition, 2012, Chapman & Hall/CRC.

e-Resources and other Digital Material

1. https://nptel.ac.in/courses/106/105/106105162/
2. https://nptel.ac.in/courses/106/103/106103015/
3. https://nptel.ac.in/courses/106/105/106105031/https://www.coursera.org/learn/number-theory-cryptography