UNIT – III: Fluid Mechanics **(18 hours)**

Classification of fluids, Continuum model, Eulerian and Lagrangian approach of description, Differentiation following the fluid motion, Velocity of a fluid particle, Irrotational flow, Velocity potential, Equipotential surfaces, Streamlines and Pathlines, Mass flux density, Conservation of mass leading to equation of continuity, Boundary surface; Forces in fluid flows, Conservation of linear momentum and its mathematical formulation (Euler's equation of motion), Bernoulli's equation, Axi-symmetric flows and motion of sphere; Two-dimensional flows, Motion of cylinder, Stream function, Complex potential, Line sources and line sinks, Line doublet, Milne-Thomson circle theorem; Viscous flow, Stress components in a real fluid, Stress and strain analysis, Navier-Stokes equations of motion and its applications.

Essential Readings

1. Chorlton, F. (2005). Textbook of Fluid Dynamics. CBS Publishers, Delhi. Reprint 2018.
2. Synge, J. L. and Griffith, B. A. (2017). Principles of Mechanics (3rd ed.). McGraw-Hill Education. Indian Reprint.

Suggestive Readings

- Gantmacher, F. (1975). Lectures in Analytic Mechanics. MIR publisher, Moscow.
- Goldstein, H., Poole, C.P. and Safco, J.L. (2002). Classical Mechanics. (3rd ed.). Addison Wesley.
- Kundu, Piyush K. and Cohen, Ira M., Dowling, David R. (2016). Fluid Mechanics (6th ed.). Academic Press.
- Mitchell, John W. (2020). Fox and McDonald's Introduction to Fluid Mechanics. (10th ed.). John Wiley & Sons.
- Taylor, John R. (2005). Classical Mechanics. University Science Books.

DISCIPLINE SPECIFIC ELECTIVE COURSE – 6(ii): CRYPTOGRAPHY

CREDIT DISTRIBUTION, ELIGIBILITY AND PRE-REQUISITES OF THE COURSE

Course title & Code	Credits	Credit distribution of the course			Eligibility criteria	Pre-requisite of the course (if any)
		Lecture	Tutorial	Practical/ Practice		
Cryptography	4	3	1	0	Class XII pass with Mathematics	Group Theory, Linear Algebra

Learning Objectives: Primary objective of this course is to:

- Learn challenges and types of attacks on the security of cryptographic protocols.
- Understand concept of confusion and diffusion, that is central to the security of symmetric key cryptography.
- Learn mathematical hard problems, which can be used to build various public key cryptosystems.
- Gain knowledge of post quantum cryptography that resist quantum attacks.

Learning Outcomes: This course will enable the students to:

- Learn classical cryptosystems Caesar cipher, Monoalphabetic cipher, Hill cipher, Vigenère cipher and their security analysis.
- Understand Feistel cipher structure to achieve confusion and diffusion in case of Data Encryption Standard (DES).
- Understand Advanced Encryption Standard (AES) structure and its operations along with key generation.
- Learn key sharing protocol – Diffie Hellman key exchange, Public-key cryptosystems – RSA, Elgamal, and Elliptic curve cryptography.
- Learn Lagrange interpolation secret sharing scheme.
- Learn hash functions and their applications, digital signatures scheme.
- Gain knowledge of code-based cryptography – McEliece cryptosystem.

SYLLABUS OF DSE-6(ii)

UNIT–I: Classical Cryptosystems and Review of Finite Fields (15 hours)

Overview of Cryptography, Symmetric key and Public-key cryptography, Security attacks, Relation between key length and security, Objectives and applications of cryptography primitives, Types of attacks from cryptanalyst view, Kerckhoff's principle; Substitution techniques - Caesar cipher, Monoalphabetic cipher, Hill cipher, Vigenère cipher, One-time pad; Euclidean Algorithm, Modular Arithmetic, Statement of Fermat's, Euler's and Chinese Remainder theorems, Discrete logarithm, Finite fields of the form GF(p) and GF(2^n), Binary and ASCII representation, Pseudo-random bit generation.

UNIT – II: Modern Block Ciphers (12 hours)

Introduction to stream and block ciphers, Diffusion and Confusion, The Feistel cipher Structure, Data Encryption Standard (DES); Advanced Encryption Standard (AES) Structure, AES transformation functions, Key expansion, AES Example.

UNIT – III: Public-key Cryptography, Hash Functions, Digital Signatures and Post Quantum Cryptography (18 hours)

Introduction to Public key cryptography, RSA cryptosystem, Diffie Hellman key exchange, Man in the middle attack, Elgamal cryptosystem, Elliptic curve arithmetic, Elliptic curve cryptography, Secret sharing; Hash functions, Applications of hash functions – MAC and digital signature, Simple Hash functions, Security requirements of Hash functions, Properties of SHA family of hash functions; Digital signatures, Elgamal and Schnorr digital signature scheme; Introduction to post quantum cryptography, Linear codes, Generating matrix, Parity check matrix, McEliece cryptosystem.

Essential Readings

1. Stallings, William (2023). Cryptography and Network Security, Principles and Practice (8th ed.). Pearson Education Limited. Global Edition.
2. Stinson, Douglas R. and Paterson, Maura, B. (2019). Cryptography: Theory and Practice (4th ed.). CRC Press.
3. Trappe, Wade and Washington, Lawrence C. (2020). Introduction to Cryptography with Coding Theory (3rd ed.). Pearson Education International.

Suggestive Readings

- Hoffstein, Jeffrey. Pipher, Jill & Silverman, Joseph H. (2014). An Introduction to Mathematical Cryptography (2nd ed.). Springer New York.
- Goldreich O. (2005). Foundations of Cryptography: Basic tools - Vol.1, Cambridge University Press.
- Goldreich O. (2009). Foundations of Cryptography: Vol.2, Basic applications, Cambridge University Press.

DISCIPLINE SPECIFIC ELECTIVE COURSE – 6(iii): INDUSTRIAL MATHEMATICS

CREDIT DISTRIBUTION, ELIGIBILITY AND PRE-REQUISITES OF THE COURSE

Course title & Code	Credits	Credit distribution of the course			Eligibility criteria	Pre-requisite of the course (if any)
		Lecture	Tutorial	Practical/ Practice		
Industrial Mathematics	4	3	0	1	Class XII pass with Mathematics	Calculus, Real Analysis, Linear Algebra, Ordinary and Partial Differential Equations

Learning Objectives: The main objective of this course is to:

- Orient the learners to understand nature and working of industrial systems and their models.
- Familiarize the learners with control and maneuvering of industrial processes through sample case-studies and encourage design-thinking and understanding.

Learning Outcomes: This course will enable the students to:

- Determine the controllability, stability, and observability of a system from the model description.
- Comprehend the signal processing landscape and analyse signals using real and spatial domain representations.
- Model/analyse an industrial system from its description and use mathematical formulations to investigate and manipulate the system for specific objectives.

SYLLABUS OF DSE-6(iii)

UNIT – I: Understanding Systems from their Mathematical Description (15 hours)

Continuous-time linear systems, Laplace transform, Transfer function and analogous systems, State-space models, Block-diagram algebra, Signal flow graph, Order of a system and reduced-order models; Discrete-time systems, Z-transform and its inverse, Feedback systems, Stability: Routh-Hurwitz criterion, Root locus method, Controllability and Observability.

UNIT – II: Mathematical Tools for Signals (15 hours)

Signal-to-noise ratio, Analog and digital messages, Channel bandwidth and rate of communication, Modulation, Randomness and redundancy; Signal energy and power, Period and aperiodic signals, Signal operations, Unit impulse function, Vector representation of signals, Orthogonality, Correlation of signals, Signal representation by orthogonal signal sets.