# Foundation of Modern Cryptography and its Application

| Code: CS31212CS | Course Type: Core | Semester: II |
|---|---|---|
| Evolution Scheme (TA-MSE-ESE): 20-30-100 | Total Marks: 150 | L-T-P (Credits): 3-0-0 (3) |

**Pre-Requisites:** Basics of Number Theory, Probability, and Abstract Algebra.

**Course Objective:** To understand modern cryptographic paradigms, formal security definitions, and construction principles of essential cryptographic primitives for secure communication systems.

**Course Outcomes:** At the end of the course, the student will be able to

| | |
|---|---|
| CO-1 | Understand the fundamentals of cryptography including classical and modern ciphers. |
| CO-2 | Apply concepts of computational and semantic security to analyze the symmetric-key cryptographic primitives |
| CO-3 | Analyze the number theoretic hard assumptions to evaluate the security of asymmetric-key cryptographic primitives for Chosen plaintext and chosen ciphertext attacks. |
| CO-4 | Understand cryptographic hash functions and their properties, and random oracle model to evaluate the security of cryptographic primitives in the random oracle model and describe advanced applications of Modern Cryptography. |

**Course Articulation Matrix:**

| PO | PEO-1 | PEO-2 | PEO-3 | PEO-4 | PEO-5 |
|---|---|---|---|---|---|
| CO-1 | 3 | 2 | 1 | - | - |
| CO-2 | 3 | 2 | 1 | - | 1 |
| CO-3 | 3 | 2 | - | - | 3 |
| CO-4 | 3 | 2 | 1 | 1 | - |

**1 - Slightly; 2 - Moderately; 3 – Substantially**

**Syllabus:**

**Unit-1: Introduction to Modern Cryptography**

Classical Cryptography V/s Modern Cryptography, Cryptographic Primitives, Kerckhoff's Principle, Deterministic V/s Randomized Algorithms, Challenges in FormalizingConfidentiality, Attack Models, Historical Ciphers, Basic Principles of Modern Cryptography, Notion for Perfectly Secret Cipher, One-Time Pad (Vernam's Cipher), Limitations of Perfect Secrecy.

**Unit-2: Symmetric-Key Cryptographic Primitives**

Introduction to Computational Security, Semantic Security, Pseudo-random Generators (PRGs), Stream Ciphers, Provably Secure Instantiation and practical Instantiations of PRG, CPA-security, Pseudo-random Functions (PRFs), Modes of Operations of Block Ciphers, Theoretical and Practical Constructions of Block Ciphers, Message Authentication Codes.

**Unit-3: Asymmetric-Key Cryptographic Primitives**

Introduction to Asymmetric-Key Cipher System, Key Exchange Protocol, RSA Cipher with CPA and CCA Security, Discrete Logarithm Assumption, El Gamal Cipher with CPA and CCA Security, RSA and El Gamal Digital Signature, Elliptic-Curve Based Cipher System.

**Unit-4: Cryptographic Primitives in Random Oracle Model with Advanced Cryptographic Applications**

Cryptographic Hash Function, Random Oracle Model, Optimal Asymmetric Encryption Padding (OAEP), Hybrid Asymmetric-Key Cipher, Signcryption, Advanced Applications of Cryptography; Cryptocurrency with the property of physical cash, Preventing Single point of failure, Zero-knowledge protocol, Outsourced computation, Distributed Consensus Protocol, Holy Grail problem.

**Learning Resources:**

**Text Books:**

1. Introduction to Modern Cryptography Book by Jonathan Katz and Yehuda Lindell
2.Cryptography: Theory and Practice by Douglas Stinson
3.Cryptography: An Introduction by Nigel Smart
4.A Graduate Course in Applied Cryptography by Dan Boneh and Victor-Shoup
5. Handbook of Applied Cryptography by Alfred Menezes, Paul van Oorschot, and Scott Vanstone