# Elective-2

# CRYPTOGRAPHY AND NETWORK SECURITY

| | | | |
|---|---|---|---|
| **Subject Code:** CS35221CS | **Subject Type:** DE (Elective-2) | **Evaluation Scheme:** MSE (30), TA (20), ESE (50) | **L-T-P:** 3-0-0 (3) |

**Pre-Requisites:** Mathematics, Computer Networks

**Course Objective:** To understand securing computer network protocols based on cryptography techniques. To understand various protocols for network security to protect against the threats in the networks. To get an insight into the working of different existing cryptographic algorithms.

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

| CO | Course Outcomes |
|---|---|
| CO1 | Students will be able to understand classical and modern symmetric cryptographic techniques. |
| CO2 | Students will be able to apply number theory and algebraic concepts in cryptography. |
| CO3 | Students will be able to analyse and implement public-key cryptographic algorithms. |
| CO4 | Students will be able to evaluate advanced cryptographic systems and security protocols. |

## Syllabus:

### Unit-I: Introduction to Cryptography with Public-Key Cryptosystems

Introduction to Cryptography, Classical Cryptosystem, Cryptanalysis on Substitution Cipher (Frequency Analysis), Play Fair Cipher, Block Cipher, Data Encryption Standard (DES), Triple DES and Modes of Operation, Stream Cipher, Pseudorandom Sequence, LFSR Based Stream Cipher.

### Unit-II: Elementary Number Theory

Abstract Algebra: Group, Ring, Field, Number Theory: Modular Arithmetic: Addition, Subtraction, Multiplication, Exponentiations, Prime Numbers, Preliminaries and Basic Group Theory: Cyclic Group, Greatest Common Divisor (GCD): Properties of GCD, Euclidean and Extended Euclidean Algorithm, Multiplicative Inverse, Linear Congruence, Solving Systems of Linear Congruence using Chinese Remainder Theorem, Fermat's Little Theorem: Application in Primality Testing and Carmichael Numbers, Euler's theorem, Quadratic Residue, Polynomial Arithmetic, Advanced Encryption Standard (AES).

### Unit-III: Introduction to Public-Key Cryptosystems and Primality Testing

Introduction to Public Key Cryptosystem, Discrete Logarithm Problem (DLP), Diffie-Hellman Key Exchange, Knapsack Cryptosystem, RSA Cryptosystem, Primarily Testing, ElGamal Cryptosystem, Elliptic Curve over the Reals, Elliptic curve Modulo a Prime, Generalised ElGamal Public Key Cryptosystem, Rabin Cryptosystem, Legendre and Jacobi Symbols, Message Authentication, Digital Signature.

### Unit-IV: Key Management, Hashing, Cryptanalysis, and Network Security Protocols

Key Management, Key Exchange, Hash Function, Universal hashing, Cryptographic Hash Function, Secure Hash Algorithm, Digital Signature Standard, Key Exchange Protocols, Cryptanalysis: Memory Trade off Attack, Differential Cryptanalysis, Linear Cryptanalysis, Cryptanalysis and Stream Cipher, Shamir Secret Sharing, Identity Based Encryption (IBE), Attribute Based Encryption, Functional Encryption, Implementation Attacks, The Secure Sockets Layer (SSL), Pretty Good Privacy (PGP).

## Learning Resources:

**Text Books:**


1. Introduction to Modern Cryptography 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.