15MAME305 Number Theory and Cryptography (3-1-0)

Course Objectives:

1. To learn about representation of finite fields.
2. To identify how number theory is related to and used in cryptography.
3. To classify the symmetric encryption techniques.
4. To illustrate various Public key cryptographic techniques

Prerequisites: Set of integers. Permutation & Combination.Programming language.

Syllabus

Module-I(15Hrs)

Euclidean GCD Algorithm, Extended GCD Algorithm, Congruences and Modular Arithmetic: Modular Exponentiation, Fast Modular Exponentiation, Linear Congruences: Chinese Remainder Theorem, Polynomial Congruences: Hensel Lifting, Quadratic Congruences: Quadratic Residues and Non Residues, Legendre Symbol, Jacobi Symbol, Multiplicative Orders: Primitive Roots, Computing Orders, Prime Number Theorem and Riemann Hypothesis

Polynomial-Basis Representation, Fermat's Little Theorem for Finite Fields, Multiplicative Orders of Elements in Finite Fields, Normal Elements, Minimal Polynomials,

Application to cryptography: The Shift Cipher, The Substitution Cipher, The Affine Cipher, The Vigenere Cipher, The Hill Cipher, The Permutation Cipher, Stream Ciphers.

Module-II(15Hrs)

Primality Testing: Fermat Test, Solovay-Strassen Test, Miller-Rabin Test, AKS Test, Integer Factorization: Trial Division, Pollard's Rho Method, Floyd's Variant, Block GCD Calculation, Brent's Variant, Pollard's p-1 Method: Large Prime Variation, Quadratic Sieve Method: Sieving, Incomplete Sieving, Large Prime Variation, Multiple- Polynomial Quadratic Sieve Method

The RSA Cryptosystem: Introduction to Public-key Cryptography, Implementing RSA Cryptosystem, Other Attacks on RSA: Computing $\phi(n)$, The Decryption Exponent, Wiener's Low Decryption Exponent Attack, Cryptographic Hash Functions: Hash Functions and Data Integrity, Security of Hash Functions : The Random Oracle Model, Algorithms in the Random Oracle Model, Comparison of Security Criteria, Discrete Logarithms: The ElGamal Cryptosystem, Algorithms for the Discrete Logarithm Problem: Shank's Algorithm , The Pollard Rho Discrete Logarithm Algorithm, Security of ElGamal Systems.

Module-III (10Hrs)

Elliptic Curves: Elliptic Curves over the Reals, Elliptic Curves Modulo a Prime, Properties of Elliptic Curves, Point Compression and the ECIES, Computing Point Multiples on Elliptic Curves. Signature Schemes: Introduction, Security Requirements for Signature Schemes, Signatures and Hash Functions, The ElGamal Signature Schemes, Security of the ElGamal Signature Scheme, Variants of the ElGamal Signature Schemes: The Schnorr Signature Scheme, The Digital Signature Algorithm, The Elliptic Curve DSA, Elliptic Curve Primality Test.

Text Books:

1. Computational Number Theory-Abhijit Das, CRC Press (First Indian Reprint,2015) Chapter 1(1.2-1.7, 1.9), Chapter 2 (2.2.1,2.4.1,2.4.2, 2.4.3, 2.4.4), Chapter 5 (5.2.1,5.2.2, 5.2.3, 5.3.2), Chapter 6(6.1-6.6, 6.8).
2. Cryptography Theory and Practice- Douglas R. Stinson, Chapman & Hall/ CRC (Third Edition) Chapter 1, Chapter 4 (4.1 ,4.2), Chapter 5(5.1,5.3,5.7), Chapter 6 (6.1,6.2,6.5,6.7), Chapter 7(7.1-7.4)

Reference Books:

1. Neal Koblitz: A Course in number theory and Cryptography, Springer Veriag, Chapter 6(section 3)

Course Outcomes: After successful completion of the course, students will be able to:

1. solve problems in elementary number theory,
2. develop a deeper conceptual understanding of the theoretical basis of number theory and cryptography.
3. apply elementary number theory to cryptography,
4. work effectively as part of a group to solve challenging problems in Number Theory and Cryptography.