MTH381:NUMBER THEORY AND CRYPTOGRAPHY

L:3 T:0 P:0 Credits:3

Course Outcomes: Through this course students should be able to

CO1 :: understand and apply division algorithms, modular arithmetic, and integer representations for efficient data processing and problem-solving.

CO2 :: understand different classical cryptography techniques, ciphers, and cryptosystems for secure communications and data protection.

CO3 :: compute GCD, LCM, and prime decompositions for key generation and protection of sensitive information.

CO4 :: compute the solutions of linear congruences by apply the various number theory theorem.

CO5 :: use public key cryptography techniques, including Diffie-Hellman, RSA, and ElGamal, for secure key exchange, encryption, and decryption.

CO6 :: apply cryptographic protocols, including hash functions, MACs, and digital signatures, to ensure data authenticity and secure communication.

Unit I

Number Theory-I : division, the division algorithm, modular arithmetic, arithmetic modulo m, representations of integers, binary expansions, octal and hexadecimal expansions, conversion between binary, octal, and hexadecimal expansions, algorithms for integer operations, addition algorithm, multiplication algorithm,

Unit II

Number Theory-II : primes, the fundamental theorem of arithmetic, trial division, the sieve of Eratosthenes, the prime number theorem, greatest common divisors and least common multiples, the Euclidean algorithm, greatest common divisors as linear combinations

Unit III

Number Theory-III : linear congruences, The Chinese remainder theorem, computer arithmetic with large integers, Fermat's little theorem, applications of congruences

Unit IV

Cryptography : introduction, history and overview of cryptography, classical cryptography, shift cipher, affine cipher, substitution cipher, vigenere cipher, Hill cipher, permutation cipher, cryptosystems

Unit V

Public Key Cryptography : introduction to public-key cryptography, Diffie-Hellman key exchange, the RSA cryptosystem, ElGamal cryptosystem, RSA encryption, RSA decryption

Unit VI

Cryptographic Protocols : hash functions and data integrity, security of hash functions, message authentication codes, digital signatures, security requirements for signature schemes

Text Books:

1. DISCRETE MATHEMATICS AND ITS APPLICATIONS by KENNETH H ROSEN, Tata McGraw Hill, India

References:

1. CRYPTOGRAPHY AND NETWORK SECURITY by BEHROUZ A FOROUZAN DEBDEEP MUKHOPADHYAY, MC GRAW HILL