CSE515:NETWORK SECURITY AND CRYPTOGRAPHY LABORATORY

L:0 T:0 P:3 Credits:2

Course Outcomes: Through this course students should be able to

CO1 :: Demonstrate the working of transposition cipher and substitution cipher method in crypotography

CO2 :: Describe the importance of symmetric key encryption method to encrypt and decrypt electronic data

CO3 :: Recall public key encryption algorithms for secure data transmission

CO4 :: Illustrate the working of extended euclidean algorithm for public key and private key encryption

CO5 :: Apply diffie-hellman key exchange method for secure digital communication

CO6 :: Explore the use of digital signatures in cryptography to validate the authenticity and integrity of a digital document

List of Practicals / Experiments:

Transposition cipher Method

- Rail fence technique- encryption and decryption
- Column Transposition- encryption and decryption

Euclid Algorithm

- Apply the Extended Euclidean algorithm to find the GCD
- Apply the Euclidean Algorithm to generate the GCD
- Apply the Extended Euclidean algorithm to find the GCD and multiplicative inverse.

Substitution Cipher method

- Caesar Cipher and modified Caesar- encryption and decryption, Monoalphabetic Cipher - encryption and decryption, Polyalphabetic Cipher - encryption and decryption, Playfair Cipher - encryption and decryption, Hill Cipher - encryption and decryption One-Time Pad - encryption and decryption, Vignere and Auto Key methods

Symmetric Key Encryption Method

- Apply the encryption and decryption of 8-bit data using Simplified DES AlgorithmConvert 64 bit key to 56 bit using Permuted choice 1 table and do a left circular shift after splitting to 28 bit left and right. Apply 64 bit user input plaintext fed to Initial Permutation (IP) table. Split into 32 bit L and R. R bit fed to Expansion/permutation (E table) to convert into 48 bitXORed 48 bit inputs to S-box to make 32 bit output which again input to Permutation Function (P) table

Public Key Encryption algorithm

- RSA algorithm - Encryption and decryption

Key Management

- Diffie-Hellman method of exchanging cryptographic keys

Digital Signatures

- Elgamal and Schnorr schemes , RSA digital signature

Text Books:

1. CRYPTOGRAPHY AND NETWORK SECURITY: PRINCIPLES AND PRACTICE, 6/E by WILLIAM STALLINGS, PEARSON

References:

1. CRYPTOGRAPHY & NETWORK SECURITY 3/E by BEHROUZ A. FOROUZAN, MCGRAW HILL EDUCATION