CSE403:NETWORK SECURITY AND CRYPTOGRAPHY

L:3 T:0 P:2 Credits:4

Course Outcomes: Through this course students should be able to

CO1 :: Understand the concepts of conventional cryptography, classical ciphers, and attacks on wireless ad hoc networks

CO2 :: Describe the working principles of modern symmetric-key cryptographic algorithms

CO3 :: Demonstrate the working of various public-key cryptography algorithms

CO4 :: Illustrate hashing techniques and digital signature algorithms used for message integrity

CO5 :: Evaluate digital signature schemes and cryptographic key distribution techniques

CO6 :: Analyze cryptographic protocols and security mechanisms to secure communication across different layers of the TCP/IP model

Unit I

Introduction and mathematics of cryptography : Security Goals, Cryptographic Attacks, Services and Mechanism, Extended Euclidean Algorithm and Modular Arithmetic

Classification of attacks for wireless adhoc and VANET : Attacks at the Physical, MAC and Network Layer, Attacks at the Transport, Application Layer and on VANET

Traditional symmetric-key cipher : Symmetric key cipher, cryptanalysis, Substitution and Transposition cipher

Unit II

Modern Symmetric-key Encipherment : GF(2^n) Fields, DES - Structure, Analysis and Security of DES, AES - Introduction, Transformations, Key Expansion and Ciphers, Use of modern block ciphers

Unit III

Assymetric-key Encipherment : Mathematics of Asymmetric cryptography - Prime and Primality Testing, Factorization and Chinese Remainder Theorem, Difference of Symmetric and Assymetric Cryptosystems, RSA Cryptosystem, ElGamal Cryptosystem, Rabin Cryptosystem, Diffie-Hellman cryptosystem

Unit IV

Message integrity and Hash function : Message Integrity, Message Authentication, Iterated Hash Function, Whirlpool, SHA512, Description of MD Hash family

Unit V

Digital Signature and Key management : Comparison, Process and Attack on digital signature, RSA and Elgamal Digital signature scheme, Schnoor Digital signature scheme and Digital signature standards, Symmetric key distribution, Symmetric key agreement, Public-key Distribution

Unit VI

Network Security : Security at Application Layer - Email System and PGP, Security service at transport layer and SSL architecture, Four SSL protocols, Transport layer security, IP Security (IPSec) and modes of IPSec, AH and ESP security protocols, security associations and security policy

List of Practicals / Experiments:

Substitution Cipher Basic

- Caesar Cipher
- Modified Caesar
- Monoalphabetic Cipher: encryption & decryption
- Polyalphabetic Cipher: vigenere & auto key

Substitution Cipher Advanced

- Polyalphabetic Cipher: One-Time-Pad
- Playfair Cipher
- Hill Cipher

Transposition cipher Method Euclid Algorithm

- Column Transposition and Rail Fence
- Apply and implement Euclid algorithm to generate the GCD and to compute multiplicative inverse ofa number.
- Apply and implement Extended Euclidean algorithm to find the GCD.

Symmetric Key Encryption Method - DES

- Convert 64 bit key to 56 bit using Permuted choice 1 table and do a left circular shift after splitting to 28 bit left & right
- 64 bit user input plaintext fed to Initial Permutation (IP) table which is split into 32 bit L and R where R bit is fed to Expansion/permutation (E table) to convert into 48 bit
- XORed 48 bit inputs to S-box to make 32 bit output which again input to Permutation Function (P) table

Public Key Encryption and Key Management Method

- RSA algorithm
- Diffie-Hellman method of exchanging cryptographic keys

Digital Signature

- Elgmal and Schnorr digital signature generation algorithm

Text Books:

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

References:

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