Approval: 1st Convocation adhoc

Course Name: Introduction to Cryptography
Course Code: CS 241
Credit: 3-0-0-3
Category:
Prerequisites: None

Objectives: This course uncovers the foundations of Cryptography: the art and science of keeping and breaking secrets. The course aims to provide theory, algorithms and applications of cryptographic techniques. The course will introduce the concepts of public-key cryptography, symmetric-key cryptography, digital signatures and message authentication schemes, with applications to real-world problems. This course is an elective for all third-semester students.

Course contents:

Module 1: Overview of Cryptography

Introduction, Information Security and Cryptography, Background on Functions, Basic Terminology and Concepts, Symmetric Key Encryption, Digital Signatures, Authentication and Identification, Public Key Cryptography, Hash Functions, Protocols and Mechanisms, Classes of Attacks and Security Models

Module 2: Classical Cryptography

Introduction to Some Simple Cryptosystems, The Shift Cipher, The Substitution Cipher, The Affine Cipher ,The Vigenere Cipher, The Hill Cipher, The Permutation Cipher, Stream Ciphers

Cryptanalysis, Cryptanalysis of the Affine Cipher, Cryptanalysis of the Substitution Cipher, Cryptanalysis of the Vigenere Cipher, A Known Plaintext Attack on the Hill Cipher

Public Key Cryptography, Introduction to public key cryptography, Number theory, Algebra, RSA, DHP and Discrete Log assumptions, Diffie Hellman key exchange, RSA public key system, ElGamal encryption, Pseudo-random bit generators

Digital Signatures, Digital signatures: definitions and applications, How to sign using RSA, Overview of signatures based on discrete-log

Module 3: Basic Symmetric Key Encryption

One time pad and stream ciphers, Shannon's Theory, Block Ciphers, Case studies: Feistel networks, DES, 3DES, and AES, Basic modes of operation: CBC and counter mode

Attacks on Block Ciphers, exhaustive search, time-space tradeoffs, differential & linear cryptanalysis, meet in the middle, side channels

Message Integrity, Message integrity: definition and applications, Collision resistant hashing, Merkle-Damgard and Davies-Meyer. MACs from collision resistance, Case studies: SHA and HMAC

Text Books:

1. Public-Key Cryptography: Theory and Practice: Abhijit Das and C. E. VeniMadhavan. Pearson Education
2. An Introduction to the Theory of Numbers by Ivan Niven, Herbert S. Zuckerman and Hugh L. Montgomery. Wiley-India
3. Topics in Algebra by I. N. Herstein, Second Edition, Wiley India