Assignment
on
ICE 4222: Fundamental of Cryptography Lab

Objective: The learning objective of this cryptography lab is to get familiar with the concepts of symmetric and asymmetric encryption and decryption algorithm implementation. After finishing the lab, students should be able to gain an experience on encryption algorithms, encryption modes and padding.

List of the Experiments

Day	Exp. #	Problem Statements
22/04/2025	Exp. 01	Write a program to implement the Caesar Cipher, • Encryption and Decryption • Study the Brute-Force cryptanalysis of Caesar Cipher
29/04/2025	Exp. 02	Write a program to implement the Mono-alphabetic cipher. • Encryption, Decryption • Relative frequency analysis and break the substitution cipher.
06/05/2025	Exp. 03	Implement the RSA algorithm to encrypt and decrypt a given message. • Public and Privet key generation with the help of Extended Euclidean Algorithm. • Encryption and Decryption.
13/05/2025	Exp. 04	Write a program to implement the Playfair ciphering.
20/05/2025	Exp. 05	Write a program to implement the Hill ciphering.
27/05/2025	Exp. 06	Write a program to implement the Diffie-Hellman Key Exchange Algorithm.
17/06/2025	**CA-1**	**Examination-1**
24/06/2025	Exp. 07	Perform the following block Cipher Modes of operation: • Electronic Codebook (ECB) • Cipher Block Chaining (CBC) • Cipher Feedback (CFB) • Output Feedback (OFB) • Counter (CTR)
01/07/2025	Exp. 08	Investigate the Applications of Elliptic Curve Arithmetic (ECC) in cryptography: • Key exchange and • Encryption and Decryption
TBC	**CA-2**	**Examination-2 (CA-2) and Quiz** Mono, Hill, ECC, Block Cipher
TBC		**LAB Final Examination**

Evaluation and Marks Distribution:
Total Marks: 37.5

Class Attendance	Continuous Assessments	Final LAB Examinations
(10%) = 3.75	(20%) = 7.5	(70%) = 26.25

SECTION-A SECTION-B