Rust Project Proposal

File Encryption Tool

01286120 Elementary Systems Programming

Software Engineering Program,

Department of Computer Engineering,

School of Engineering, KMITL

By

67011158 Kyi Thant Sin

67011118 Hsu Myat Shwe Sin

File Encryption Tool

Project Description

The File Encryption Tool is a Rust application that securely encrypts and decrypts files using the ChaCha20 and AES algorithms. It features a user-friendly graphical user interface (GUI) built with the ICED framework, allowing users to easily select files and configure encryption settings. The tool emphasizes efficient file handling for reading and writing encrypted data, ensuring the protection of sensitive information during storage and transmission.

Key Features

- **File Selection:** Users can browse and select files they wish to encrypt or decrypt.
- **Encryption Settings:** Options to configure encryption algorithms.
- **Secure Encryption/Decryption:** Utilizes the ChaCha20 algorithm for fast and secure file encryption and decryption.
- **File Handling:** Efficiently reads and writes data, maintaining the integrity of the original files while securely managing encrypted content.
- **User-Friendly GUI:** Intuitive interface that simplifies the encryption/decryption process for users of all experience levels.

Usages

1. Encrypting Files
- Open the application and select the file to be encrypted.
- Configure the desired encryption settings (e.g. ChaCha20 or AES).
- Click the “Encrypt” button to securely encrypt the selected file, generating a new encrypted file.

2. Decrypting Files
- Open the application and choose the encrypted file to decrypt.
- Enter the required decryption parameters.
- Click the “Decrypt” button to restore the original file from its encrypted state.

Algorithms

1. ChaCha20 Algorithm
It is a fast stream cipher that encrypts data by XOR-ing it with a key-stream generated from a key and nonce.
2. AES (Advanced Encryption Standard)
AES is a block cipher that encrypts data in fixed-size blocks using a series of transformations, providing strong security and benefiting from hardware acceleration.

Library

- ICED Framework
- chacha20
- aes