CS 428

Drew Ridley, Jack Lee

4 April 2024

Rust-Based Implementation of the Advanced Encryption Standard

This project will be an implementation of the Advanced Encryption Standard (AES) using the Rust programming language. The group will consist of Jack Lee and Drew Ridley. The following table details the tasks to be split between each group member:

|  |  |
| --- | --- |
| Drew | Jack |
| Research AES algorithm details | Research required libraries |
| Implement key expansion logic | Optimize key expansion |
| Develop initial round for encryption | Develop initial round for decryption |
| Code main rounds for encryption | Code main rounds for decryption |
| Finalize encryption process | Finalize decryption process |
| Unit tests for encryption | Unit tests for decryption |
| Document encryption methods | Document decryption methods |

The project will cover AES with 128-bit key length, implemented for all platforms the rust language supports. Because AES is a block cipher, input may need to be padded with random bits. Core functionalities including key expansion, initial round, main rounds, and the final rounds for both encryption and decryption will be implemented for this project. Rust was elected as the programming language due to its emphasis on safety and performance, both of which are important in a cryptographically secure context. Furthermore, both group members are familiar with and enjoy writing programs using Rust. Below is a timeline of the project corresponding to the task division chart above. The deadline for this project is April 29, and the authors aim to complete the program before then to save time for making a video presentation.

**Project Timeline:**

April 8-12: Initial planning and development stage (Initialize git repository, perform research), implement and optimize key expansion.

April 15-19: Develop initial rounds for encryption/decryption, start coding main rounds for encryption and decryption.

April 22-26: Finalize cipher code, start writing and validating code with unit tests. Document encryption and decryption methods.

April 27-19: Plan and record video, submit project.