## Team Members

| Name | ID | Signature |
|---|---|---|
| Tanjim Tajwar Arnab | 22701066 | |
| Hafiz Hasnat Sifat Jami | 22701068 | |
| Muznabin Ahmed | 22701069 | |
| Saikat Ahmed | 22701076 | |
| Nafisa Tasnim Momo | 21701046 | |
| Kamrul Arafin | 22701016 | |

# Parallel File Encryptor

## Introduction

Parallel File Encryptor is a high-performance encryption tool designed to securely encrypt and decrypt files using multi-threaded processing in Java. This project ensures efficient file handling by leveraging parallel processing techniques, providing faster encryption without compromising security.

## Objectives

- Implement parallel encryption and decryption for large files.
- Ensure data integrity and security using AES-256 or ChaCha20.
- Optimize file handling using Java NIO for high-speed I/O operations.
- Provide robust error handling and recovery mechanisms.

## Key Features

- Multi-threaded encryption and decryption for improved speed.
- High-speed file handling using Java NIO.
- Secure key storage and metadata embedding.
- Fault tolerance with error recovery and resume capabilities.
- Supports encryption of multiple files and folders.

## Workflow

- Files are divided into chunks and encrypted in parallel.
- Metadata, including IV and chunk size, is stored securely.
- Decryption reverses the process to reconstruct original files.
- Ensures data integrity using SHA-256 verification.

## Technologies Used

- **Programming:** Java, Java NIO, Executors, ForkJoinPool.
- **Encryption:** Java Cryptography Architecture (JCA), Bouncy Castle.
- **Logging:** Log4j for tracking processes and errors.

## Testing & Optimization

- Functional testing with varying file sizes.
- Performance benchmarking for single-threaded vs multi-threaded execution.
- Security validation using SHA-256 hash verification.

## Conclusion

Parallel File Encryptor provides an efficient and secure way to encrypt large files using parallel processing. With its robust architecture, optimized performance, and strong encryption mechanisms, it ensures data confidentiality while reducing encryption time. The tool is well-suited for both personal and enterprise-level security applications.