Image Encryption and Decryption Tool

Overview

This project involves creating a tool for encrypting and decrypting JPEG images using AES-128 CBC mode. The tool is implemented in C++ and leverages the OpenSSL library for encryption, decryption, and certificate generation. It features an interactive command-line interface (CLI) to guide users through the encryption and decryption processes.

Features

Image Encryption and Decryption

- **Encrypts and decrypts images (JPEG format)**
- **Uses AES-128 in CBC mode for secure image data handling**

Interactive Command-Line Interface (CLI)

- **User-friendly menu with options for encryption, decryption, and program exit**

Certificate Generation

- **Generates X.509 certificates using OpenSSL**
- **Adds security and authenticity verification capabilities**

User-Provided Key and IV Input

- **Requires user input for encryption key and initialization vector (IV) during decryption**
- **Enhances security by emphasizing cryptographic key management**

Use of mbedTLS/OpenSSL Libraries

- **Leverages industry-standard cryptographic libraries for robust and reliable encryption**
- **Ensures compatibility and adherence to cryptographic best practices**

End-to-End Workflow

- **Complete workflow from loading an image, encrypting it, saving the encrypted data, decrypting it, and saving the decrypted image**

Technology Used

- **Programming Language**: C++
- **Libraries**: OpenSSL for cryptographic operations and certificate generation
- **File Handling**: Standard C++ libraries for file input/output

Unique Idea

Our cryptography simulation tool stands out with its specialization in image encryption and decryption, specifically using AES-128 CBC mode. Unlike generic encryption tools, our project is designed exclusively for securing JPEG images, ensuring data integrity and confidentiality. The user-friendly command-line interface (CLI) guides users through the process, making it accessible even to those with minimal cryptographic knowledge.

A distinctive feature of our tool is the integration of certificate generation using OpenSSL. By producing X.509 certificates, the tool adds an extra layer of security and authenticity, a feature often absent in basic encryption utilities. Additionally, the tool requires users to provide encryption keys and initialization vectors (IVs) during decryption, reinforcing essential cryptographic principles and enhancing security.