Project Report on

Cryptography Simulation with mbedTLS/OpenSSL Library Usage and User Interaction

By

Om Hedau

Ojas Hedau

Sahil Patil

DEPARTMENT OF COMPUTER ENGINEERING

SHAH AND ANCHOR KUTCHHI ENGINEERING COLLEGE

CHEMBUR, MUMBAI – 400088.

University of Mumbai

(AY 2024-25)

Abstract

The project aims to develop an interactive cryptography simulation tool using C programming and mbedTLS/OpenSSL libraries. This tool is designed to facilitate hands-on learning and experimentation with various cryptographic techniques. It will feature a user-friendly graphical user interface (GUI) that allows users to explore encryption, decryption, key generation, and cryptographic algorithms such as RSA, AES, DES, and SHA. The tool will also include educational content on security concepts and interactive elements for users to experiment with different encryption parameters. The primary objective is to create a valuable educational resource for students and professionals in cybersecurity, enhancing their understanding of how cryptography secures digital communication and data. The project involves implementing cryptographic algorithms, developing an intuitive GUI, and creating detailed educational documentation to ensure a comprehensive learning experience. The collaborative efforts of the team members are expected to result in a robust and engaging tool that promotes practical cryptography knowledge and secure communication awareness.

Introduction:

Cryptography is a critical field in cybersecurity, providing the foundational techniques that secure digital communication and data. With the increasing importance of data security in today's digital world, it is essential for students and professionals to understand the principles and practices of cryptography. However, learning cryptography can be challenging due to its complex mathematical and theoretical underpinnings.

To address this challenge, we propose the development of an interactive cryptography simulation tool using C programming and mbedTLS/OpenSSL libraries. This tool aims to offer a practical and engaging way to explore cryptographic techniques such as encryption, decryption, key generation, and various algorithms like RSA, AES, DES, and SHA. By providing a user-friendly graphical user interface (GUI) and educational content, the tool will enable users to experiment with cryptographic processes and gain a deeper understanding of their functionality and significance.

The interactive nature of the simulation tool will allow users to input data, select encryption methods, and observe the results of encryption and decryption processes in real-time. Additionally, the educational content will cover fundamental security concepts, enhancing users' theoretical knowledge alongside their practical skills. This project aims to create a valuable educational resource that bridges the gap between theoretical cryptography and its practical applications, ultimately contributing to the development of a more secure digital landscape.

Problem Statement:

The growing importance of cybersecurity in protecting digital communications and data necessitates a deep understanding of cryptographic techniques among students and professionals. However, the complexity of cryptographic algorithms and their theoretical foundations often makes learning these techniques challenging. Traditional educational resources may not provide the interactive and practical experience needed to fully grasp the intricacies of cryptography.

To address this educational gap, we aim to develop an interactive simulation tool using C programming and mbedTLS/OpenSSL libraries. This tool will facilitate hands-on learning and experimentation with various cryptographic techniques, including encryption, decryption, key generation, and algorithms such as RSA, AES, DES, and SHA. The simulation will feature a user-friendly graphical user interface (GUI) that allows users to input text or data, select encryption methods, view encrypted results, and decrypt data back to its original form. Additionally, it will include educational content on security concepts and interactive elements for experimenting with different encryption parameters.

The objective is to create a comprehensive educational resource that enhances the understanding of how cryptography secures digital communication and data. By making cryptographic concepts more accessible and engaging, this tool will help bridge the gap between theoretical knowledge and practical application, ultimately contributing to better-prepared cybersecurity professionals.

Objectives:

1. Develop an Interactive Simulation Tool:
   - Create a desktop application with a graphical user interface (GUI) using C programming and mbedTLS/OpenSSL libraries to simulate cryptographic techniques.

2. Facilitate Hands-on Learning:
   - Provide users with the ability to experiment with encryption, decryption, and key generation processes.
   - Implement support for various cryptographic algorithms including RSA, AES, DES, and SHA.

3. Enhance Understanding of Cryptography:
   - Include educational content that explains fundamental security concepts and cryptographic techniques.
   - Offer interactive elements that allow users to adjust encryption parameters and observe the effects.

4. Provide a User-Friendly Interface:
   - Design an intuitive GUI that makes it easy for users to input text or data, select encryption methods, and view results.
   - Ensure the interface provides visual feedback on encryption and decryption processes.

5. Create a Valuable Educational Resource:
   - Develop a tool that serves as a comprehensive learning platform for students and professionals in cybersecurity.
   - Enhance users' practical skills and theoretical knowledge of how cryptography secures digital communication and data.

6. Promote Experimentation and Exploration:
   - Allow users to explore different cryptographic algorithms and parameters to understand their applications and limitations.
   - Encourage interactive experimentation to foster a deeper appreciation of cryptographic principles.

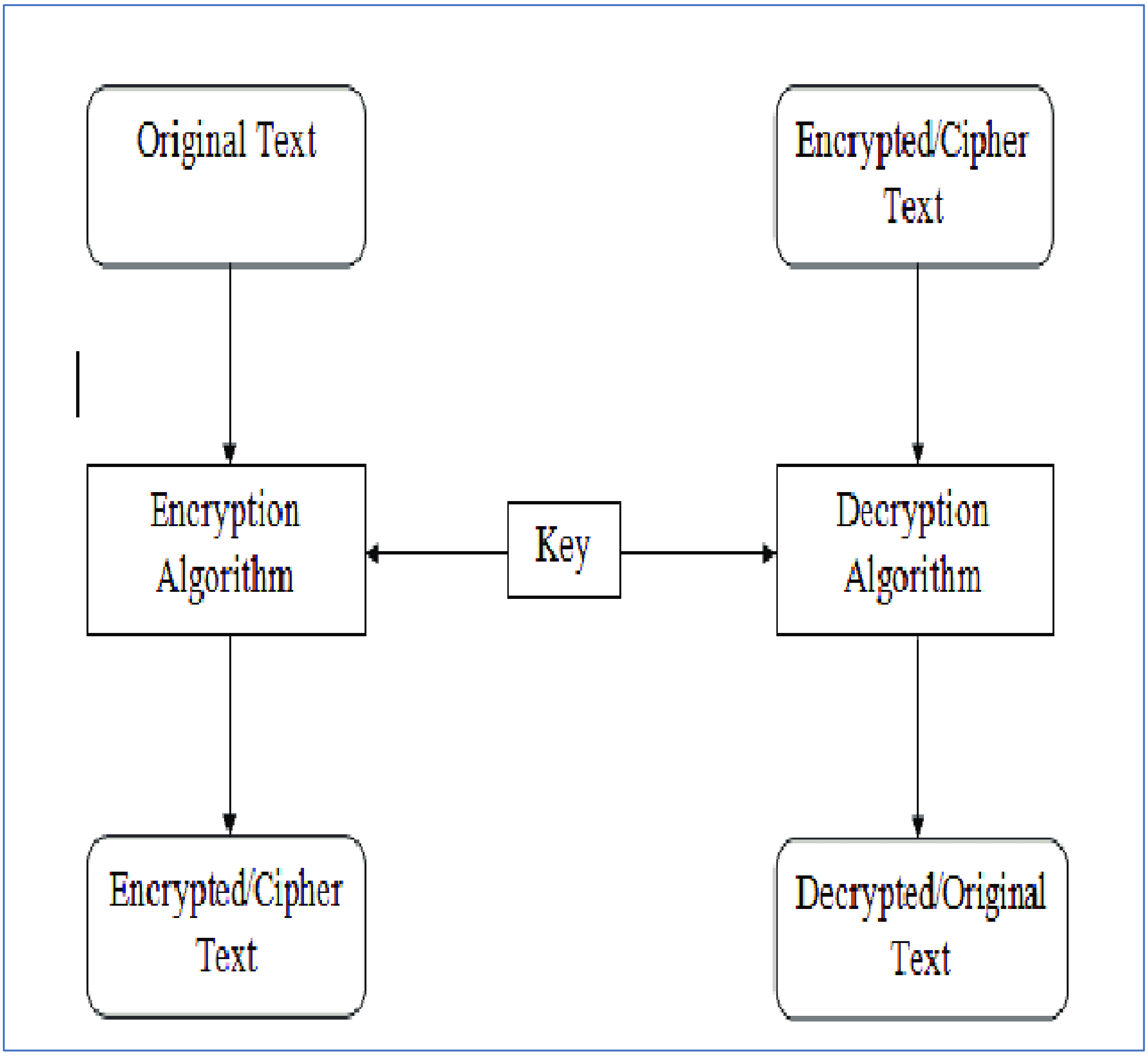
7. Ensure Comprehensive Documentation:
   - Provide detailed documentation on the cryptographic algorithms used, their implementation, and educational content to support learning.
   - Include user guides and tutorials to help users navigate and make the most of the simulation tool.

By achieving these objectives, the project aims to create a robust and engaging tool that not only educates users on cryptographic techniques but also fosters a deeper understanding and appreciation for the importance of secure communication in the digital world.

Scope:

The project will implement widely used cryptographic algorithms such as RSA, AES, DES, and SHA, providing both encryption and decryption functionality. It will feature key generation capabilities and an intuitive graphical user interface (GUI) for user interaction, allowing input of text or data, selection of encryption methods, and visualization of encryption and decryption processes. Educational content on cryptographic and security concepts will be integrated, including tutorials and guides. The tool will use C programming and mbedTLS/OpenSSL libraries, developed in environments like Visual Studio Code, with version control via Git. Comprehensive documentation will be provided, catering to students and professionals in cybersecurity. The project will undergo thorough testing to ensure accuracy and reliability, with potential future enhancements outlined for expanding the tool's capabilities.

Block Diagram:



Technologies Used:

1. Programming Language:
    - C: Utilized for implementing cryptographic algorithms and managing encryption/decryption processes.

2. Libraries:
    - mbedTLS/OpenSSL: Used for cryptographic functions including RSA, AES, DES, and SHA implementations.

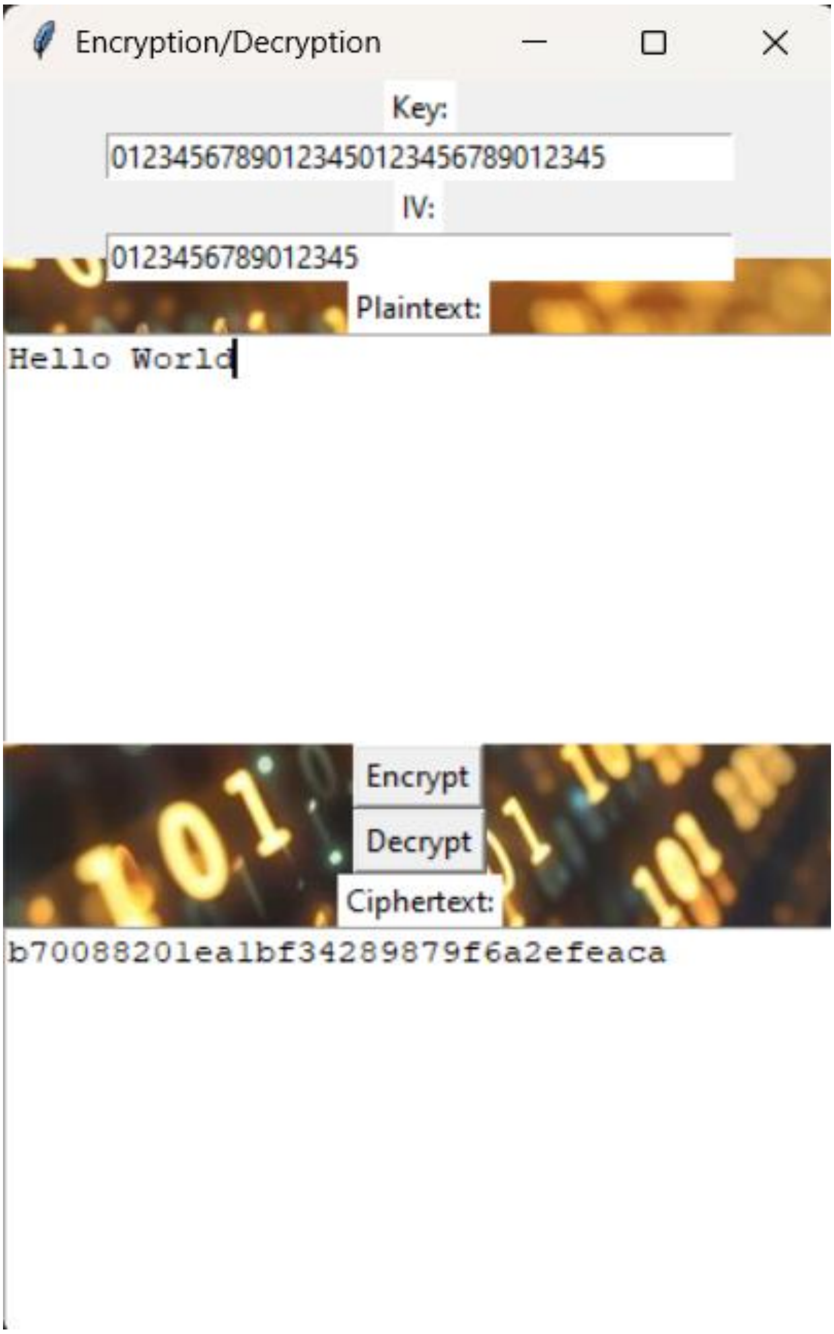
3. User Interface:
    - Graphical User Interface (GUI): Provides an interactive platform for users to input data, select encryption/decryption options, and visualize results.

4. Development Tools:
    - Integrated Development Environment (IDE): Such as Visual Studio Code, for coding, debugging, and testing the application.

5. Version Control:
    - Git: Employed for version control and collaboration on the project codebase, ensuring efficient project management and team collaboration.

These technologies collectively facilitate the development of a robust and user-friendly cryptography simulation tool, enhancing the learning experience for users.

Result:



Key: 01234567890123450123456789012345

IV: 0123456789012345

Plaintext:

```
Hello World
```

Ciphertext:

```
b70088201ea1bf34289879f6a2efeaca
```

Summary:

This project focuses on developing an interactive cryptography simulation tool using C programming and mbedTLS/OpenSSL libraries. The tool aims to provide a practical and engaging way for users to explore encryption, decryption, key generation, and various cryptographic algorithms like RSA, AES, DES, and SHA. It features a user-friendly graphical user interface (GUI) that allows users to input data, select encryption methods, view encrypted results, and decrypt data back to its original form. Additionally, the tool includes educational content on cryptographic concepts and interactive elements for experimenting with encryption parameters. By leveraging technologies such as Visual Studio Code for development and Git for version control, the project aims to create a valuable educational resource for students and professionals in cybersecurity, enhancing their understanding and practical skills in cryptography.