Green University of Bangladesh

Department of Computer Science and Engineering (CSE)
Semester: (Fall, Year: 2024), B.Sc. in CSE (Day)

AnasTamanna SecureFileCrypt Algorithm

Course Title: Computer and Cyber Security
Course Code: CSE 323
Section: 211-D1

Students Details

Name	ID
Md.Anas Khan	201902037
Nura Anha Tamanna	202902002

Submission Date: 12.01.24
Course Teacher's Name: Md. Jahidul Islam

[For teachers use only: Don't write anything inside this box]

Project Report Status	
Marks:	**Signature:**
Comments:	**Date:**

Contents

Chapter 1

Introduction

1.1 Overview

Data security is a major issue that we are facing today in this digital world of communication. As we know that today hackers are almost at every corner in search of our useful data which can be hacked by them for different purposes. Even the risk gets doubled when comes to the data of any country's government. So, a system or terminology is required to make that data safe forever by any means during communication.Data protection can be accomplished by changing the original data by any means to some other unuseful data so that if someone gets that data then also it must remain in unuseful bits. This process can be achieved by Encrypting that data by some means of algorithms which are known to the sender and the similar Decryption algorithms to be known to only the desired receiver so that it can convert that encrypted data back to the user understandable form. Today as it is a need to develop such kind of applications that performs the specified task but along with it should be very much userfriendly so that no special skills need to be required to learn in order to use that application or project.

The AnasTamanna Security Suite is a comprehensive file encryption and decryption tool designed to provide users with a secure and user-friendly solution for protecting their sensitive data. The suite combines various encryption techniques, including transposition ciphers, substitution ciphers, and XOR operations, to ensure robust and multi-layered security.

1.2 Motivation

- The project was chosen due to its comprehensive approach to file encryption. By integrating various encryption techniques such as transposition ciphers, substitution ciphers, and XOR operations, the AnasTamanna Security Suite offers a well-rounded and multi-layered security solution. This appealed to the goal of developing a tool that goes beyond basic encryption methods, providing enhanced protection for diverse types of data.

- The utilization of advanced encryption techniques, such as transposition ciphers and XOR operations, played a pivotal role in the decision to choose this project. These techniques enhance the overall security posture, making it more challenging for unauthorized entities to compromise the encrypted data.

- The project's focus on secure file transmission aligns with the modern necessity of sharing information across networks without compromising data integrity. This feature addresses a critical aspect of data security, influencing the decision to choose the AnasTamanna Security Suite.
- The increasing frequency of data breaches and cyber threats underscores the need for robust data protection solutions. SecureFileCrypt aims to empower users with a reliable tool to encrypt their files, ensuring confidentiality and privacy.
- The motivation behind the AnasTamanna Security Suite arises from the growing need for individuals and organizations to protect their confidential data from unauthorized access. With the increasing prevalence of cyber threats, having a reliable and easy-to-use encryption tool becomes crucial for ensuring privacy and security.

1.3 Problem Definition

1.3.1 Problem Statement

1. Ensuring that the application is user-friendly for individuals with varying technical expertise.
2. Coordinating and seamlessly integrating multiple encryption techniques (transposition ciphers, substitution ciphers, XOR operations) for a comprehensive and effective security solution.
3. Balancing the need for robust encryption with the potential performance impact on the application.

1.3.2 Complex Engineering Problem

The following Table 1.1 is completed according to our above discussion.

Table 1.1: Summary of the attributes touched by the mentioned projects

Name of the P Attributess	**Explain how to address**
P1: Depth of knowledge required	A comprehensive understanding of encryption techniques, including transposition ciphers, substitution ciphers, and XOR operations, is essential. Address by providing in-depth training sessions, detailed documentation, and resources explaining each encryption method.
P2: Range of conflicting requirements	Balancing conflicting requirements, such as strong encryption and minimal performance impact, is crucial. Address by conducting thorough requirement analysis sessions with stakeholders. Develop a clear understanding of trade-offs and priorities.
P3: Depth of analysis required	Implement a comprehensive testing strategy, including unit testing and integration testing, to validate the effectiveness of the encryption techniques. Utilize analytical tools and simulations for performance assessment.
P4: Familiarity of issues	User familiarity with encryption processes may vary. Address by designing an intuitive user interface with clear instructions and tooltips.
P5: Extent of applicable codes	The project involves developing complex encryption algorithms and file handling procedures. Address by establishing coding standards and conducting code reviews to ensure consistency and quality. Create a codebase that allows collaboration, facilitating the reuse of applicable code snippets and libraries.
P6: Extent of stakeholder involvement and conflicting requirements	Stakeholders, including end-users, administrators, and decision-makers, will be involved in understanding project goals, providing feedback during implementation.
P7: Interdependence	Various components, such as encryption techniques, key management, and secure file transmission, are interdependent. Address by creating a comprehensive project plan with clear dependencies and milestones.

1.4 Design Goals/Objectives

The objectives of this project are as follows:

- Implement strong encryption techniques to safeguard sensitive information.
- Create an intuitive interface for users to easily encrypt and decrypt files.
- Allow users to set encryption parameters, such as the number of iterations and passphrase.
- Support different types of ciphers to provide flexibility in choosing encryption methods.

1.5 Application

1. Users can encrypt personal files and documents to prevent unauthorized access.
2. Facilitates the secure transfer of sensitive information over networks.
3. Enhances the security of communication by encrypting files and messages.

Chapter 2

Design/Development/Implementation of the Project

2.1 Introduction

The SecureFileCrypt project is a robust and secure file encryption and decryption application. It aims to provide users with a reliable tool to encrypt sensitive files, ensuring data confidentiality during transmission and storage. This project addresses the growing need for secure data handling in various domains, including personal, professional, and organizational settings

2.2 FlowChart

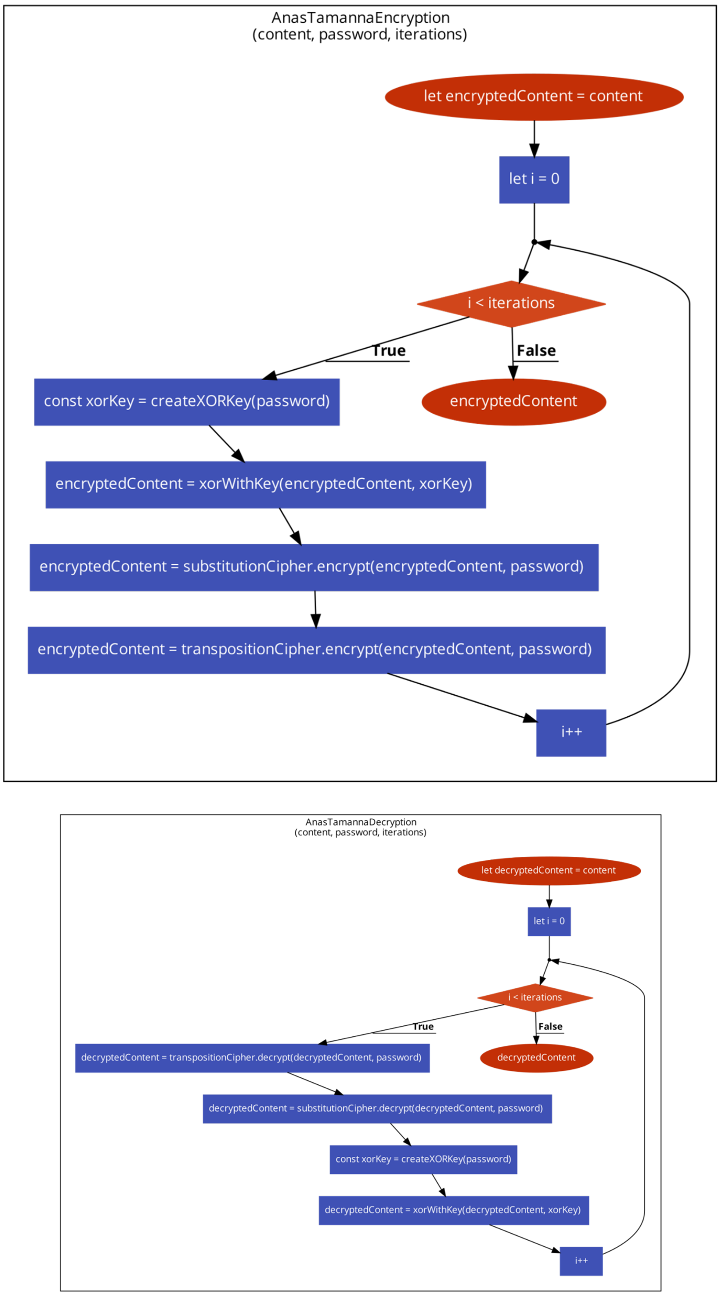

AnasTamannaEncryption
(content, password, iterations)
let encryptedContent = content
let i = 0
i < iterations
True
False
const xorKey = createXORKey(password)
encryptedContent
encryptedContent = xorWithKey(encryptedContent, xorKey)
encryptedContent = substitutionCipher.encrypt(encryptedContent, password)
encryptedContent = transpositionCipher.encrypt(encryptedContent, password)
i++
AnasTamannaDecryption
(content, password, iterations)
let decryptedContent = content
let i = 0
i < iterations
True
False
decryptedContent = transpositionCipher.decrypt(decryptedContent, password)
decryptedContent
decryptedContent = substitutionCipher.decrypt(decryptedContent, password)
const xorKey = createXORKey(password)
decryptedContent = xorWithKey(decryptedContent, xorKey)
i++

Figure 2.1: Encryption Process

2.3 Implementation

Here's an overview of our project:

1. **Transposition Cipher:** Utilizes a matrix-based approach for encryption and decryption. Allows customization of the key for increased security.

2. **Substitution Cipher:** Uses a substitution map to replace characters in the text. Key-based shuffling of the substitution map enhances encryption strength.

3. **XOR Operations:** Employs XOR operations with a dynamically created key based on the user's passphrase. Adds an additional layer of encryption to the overall process.

4. **Special Features:**

   (a) Multi-layered encryption using Combines transposition, substitution, and XOR operations for enhanced security.

   (b) Users can set the number of encryption iterations and passphrase for personalized security.

   (c) Simplifies the file selection process with an intuitive drag-and-drop feature.

   (d) key generation mechanism.

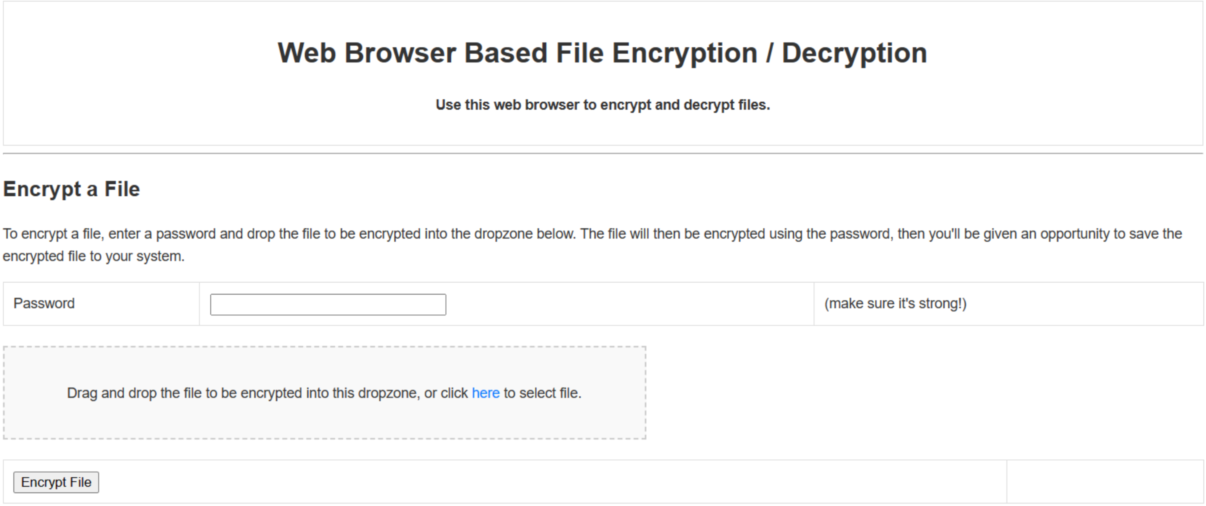
Chapter 3

Performance Evaluation

3.1 Simulation Environment/ Simulation Procedure

1. **Environment**: Set up an integrated development environment (IDE) that facilitates code development, debugging, and testing. Such as Visual Studio Code, PyCharm, Eclipse, or any IDE.

3.2 Results Analysis/Testing



Web Browser Based File Encryption / Decryption

Use this web browser to encrypt and decrypt files.

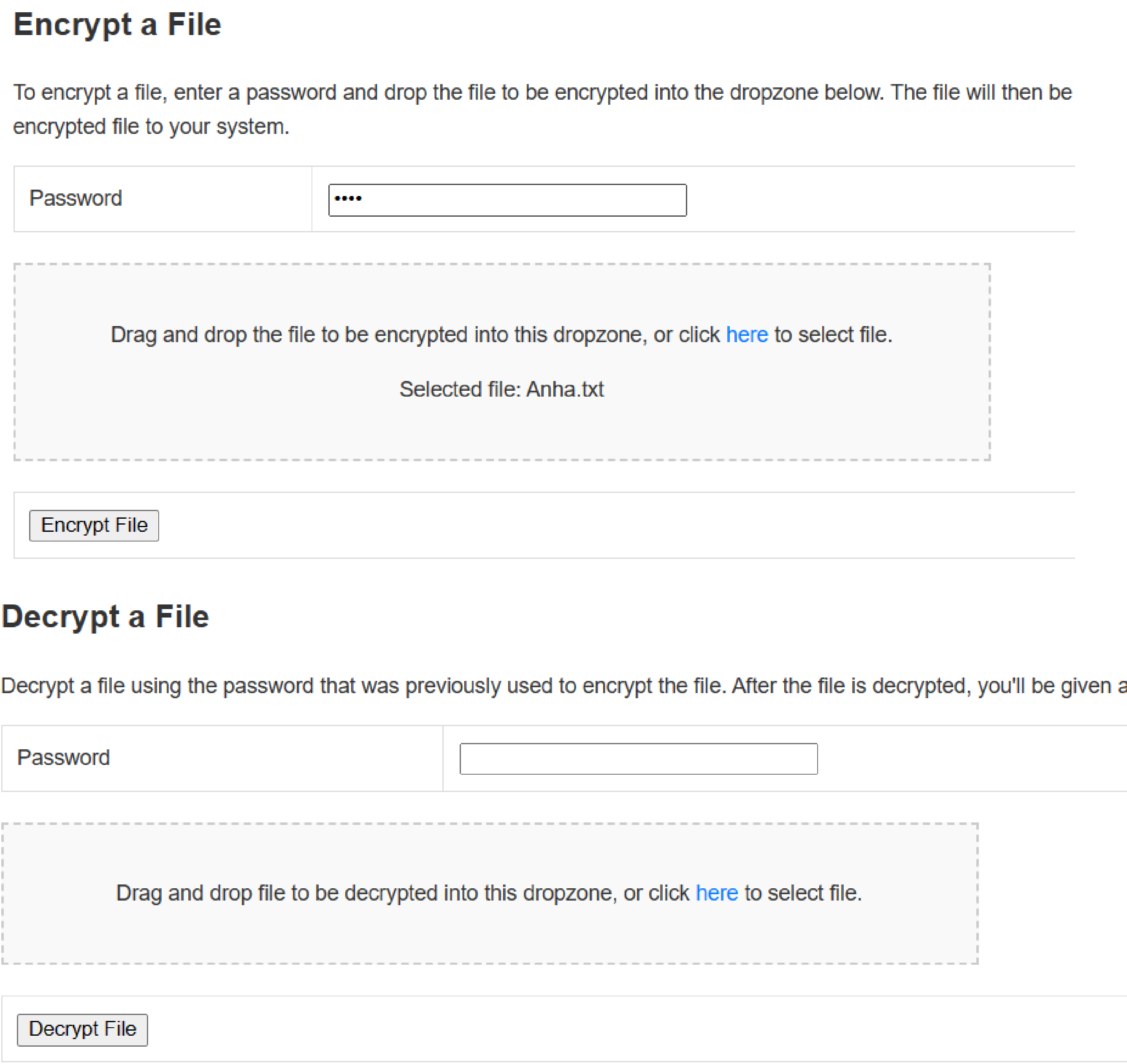
Encrypt a File

To encrypt a file, enter a password and drop the file to be encrypted into the dropzone below. The file will then be encrypted using the password, then you'll be given an opportunity to save the encrypted file to your system.

Password		(make sure it's strong!)

Drag and drop the file to be encrypted into this dropzone, or click here to select file.

Figure 3.1: Interface



Encrypt a File

To encrypt a file, enter a password and drop the file to be encrypted into the dropzone below. The file will then be encrypted file to your system.

Password	••••

Drag and drop the file to be encrypted into this dropzone, or click here to select file.

Selected file: Anha.txt

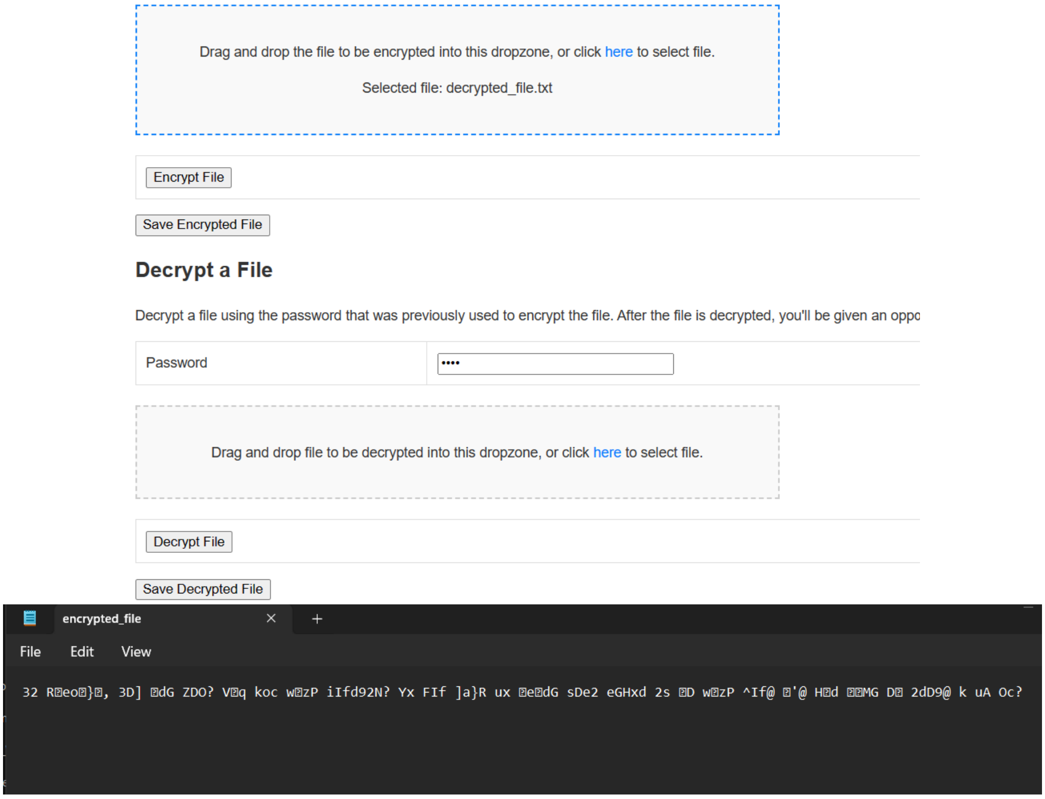
Decrypt a File

Decrypt a file using the password that was previously used to encrypt the file. After the file is decrypted, you'll be given a

Password	

Drag and drop file to be decrypted into this dropzone, or click here to select file.

Figure 3.2: File Encrypt, Decrypt



Drag and drop the file to be encrypted into this dropzone, or click here to select file.

Selected file: decrypted_file.txt

Decrypt a File

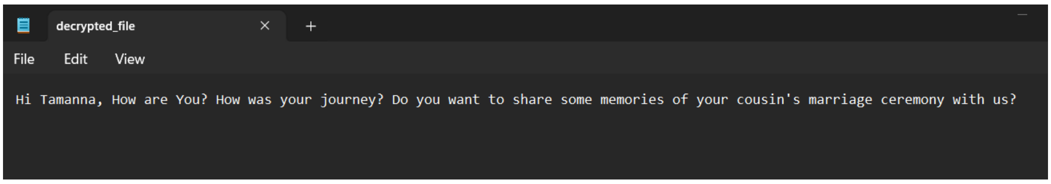
Decrypt a file using the password that was previously used to encrypt the file. After the file is decrypted, you'll be given an oppo

Password: ••••

Drag and drop file to be decrypted into this dropzone, or click here to select file.

```
32 R▯eo▯}▯, 3D] ▯dG ZDO? V▯q koc w▯zP iIfd92N? Yx FIf ]a}R ux ▯e▯dG sDe2 eGHxd 2s ▯D w▯zP ^If@ ▯'@ H▯d ▯▯MG D▯ 2dD9@ k uA Oc?
```

Figure 3.3: Save file and Encrypted file



```
Hi Tamanna, How are You? How was your journey? Do you want to share some memories of your cousin's marriage ceremony with us?
```

Figure 3.4: Decrypted File

Chapter 4

Conclusion

4.1 Discussion

In conclusion, the SecureFileCrypt project stands as a robust solution to the pressing need for secure file encryption and decryption. By combining multiple encryption techniques and adhering to high-level security standards, this application provides users with a reliable tool to protect their sensitive data. Ongoing efforts will focus on refining the application, addressing user feedback, and exploring new avenues for data security in the digital age.

4.2 Scope of Future Work

Several properties for future work can further enrich and extend the project's capabilities:

- Implementation of additional encryption algorithms.
- Allow users to encrypt and decrypt files directly from cloud storage services.
- Development of a mobile application for on-the-go encryption.

By achieving these properties future work on this project will be enriched successfully. Iterative development cycles, focused on user satisfaction and engagement, will contribute to the sustained success and growth of this project.

Bibliography

[1] *An Analysis of Encryption and Decryption Application by using One Time Pad Algorithm*. DRam, Bhupendra Pundir, Manisha. (2023). 10.21203/rs.3.rs-3242122/v1.

[2] *An Analysis of Encryption and Decryption Application by using One Time Pad Algorithm*. Multimedia Tools and Applications