Green University of Bangladesh

Department of Computer Science and Engineering (CSE)
Semester: (Spring, Year: 2023), B.Sc. in CSE (Day)

File encryption and decryption

Course Title: Cyber Security
Course Code: CSE-323
Section: 203-D1

Students Details

Name	ID
Tanha Taranum	203002061
Md. Hasinur Rahman	203002014
Sajed Khan Abir	203002008

Submission Date: 11 - 12 - 2023
Course Teacher's Name: Md. Riad Hassan

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

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

Contents

1 Introduction **2**

1.1 Overview 2

1.2 Motivation 2

1.3 Problem Definition 3

1.3.1 Complex Engineering Problem 3

1.4 Design Goals/Objectives 3

1.5 Application 3

Chapter 1

Introduction

1.1 Overview

In the evolving world of data and information transfer, the security of the file contents remains to be one of the greatest concerns for companies. Some information can be password protected (emails, logins) while other information being transferred via emails or FTP lacks efficiency if protected by some keyword. This is where file encryption plays a big role and provides the security and convenience sought by parties engaged in file transfers. Encryption is a process of converting information into some form of code to hide its true content. The only way to access the file information then is to decrypt it. The process of encryption/decryption is called cryptography.

1.2 Motivation

In an age dominated by digital connectivity and information exchange, the security of our data is more critical than ever. The motivation behind this file encryption and decryption project stems from a deep commitment to addressing the escalating concerns surrounding data privacy and unauthorized access to sensitive information.

As technology advances, so do the methods employed by malicious actors seeking to exploit vulnerabilities in digital systems. Our project is driven by the conviction that everyone has the right to protect their personal and confidential data from unauthorized access. Whether it's individuals safeguarding their personal files or organizations securing proprietary information, the need for a robust and user-friendly file encryption and decryption system has never been more apparent.

This project aims not only to contribute a technical solution but also to empower users with a tool that is accessible, reliable, and effective. By designing a system that goes beyond the conventional and bridges the gap between security and usability, we aspire to make a tangible impact on the way individuals and organizations safeguard their digital assets.

1.3 Problem Definition

1.3.1 Complex Engineering Problem

The following Table 1.1 was completed according to our above discussion in detail.

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	In-depth knowledge regarding existing tools and Crypto analysis such as encryption as well as decryption
P2: Range of conflicting requirements	If there is any kind of conflicting then that must be ignored
P3: Depth of analysis required	Analysis of controlling system is must be high
P4: Familiarity of issues	None
P5: Extent of applicable codes	None
P6: Extent of stakeholder involvement and conflicting requirements	Extensive thinking of the system to the users,as well as to developers are required
P7: Interdependence	none

1.4 Design Goals/Objectives

These are some important objectives of this project :

- Design and implement a robust encryption algorithm to ensure the confidentiality of data.
- Create an effective mechanism for generating and managing cryptographic keys, ensuring the security of the key exchange process.
- Implement a reliable file decryption process, ensuring that only authorized users can access the original content.
- Optimize the algorithm and system performance to provide efficient encryption and decryption without compromising security.
- Design the system to work seamlessly across different devices and platforms, enhancing its practicality and usability.

1.5 Application

The file encryption and decryption project has numerous practical applications across various domains due to the growing need for data security.

1. **Data Privacy for Individuals**: Individuals can use the file encryption system to protect personal documents, such as financial records, medical information, and private correspondence, ensuring that sensitive data remains confidential.

2. **Corporate Data Protection:** Businesses can employ the file encryption system to safeguard proprietary information, intellectual property, and confidential business documents from unauthorized access or data breaches.

3. **Communication:** Integration of the encryption system into messaging or email applications ensures that communication remains confidential, especially in environments where privacy is crucial, such as legal, healthcare, or financial sectors.

4. **Government and Defense**: Military and government agencies can use the encryption system to secure classified documents and communications, protecting national security interests. confidential.