

**Custom Encryption**

**and**

**Decryption Software**

Software Requirements Specification (SRS) Document

Sprint 2 Implementation

Project Timeline: **02.01.2023** to **11.01.2023**

**CONTENTS**

1. Introduction

* 1. Purpose
  2. Intended Audience
  3. Project scope

1.4 Project Objective

2. Overview

2.1 Assumptions and Dependency

3. System Features and Requirements

3.1 Functional Requirements

3.2 Technical Requirements

3.2 System Requirements

3.3 System Features

4. Reference

**1.INTRODUCTION**

       Encryption is a process by which a readable message is converted to an unreadable form to prevent unauthorized parties from reading it.

       Decryption is the process of converting an encrypted message back to its original format. The original message is called plaintext message.

* 1. **Purpose:**

The main purpose of our project is to save the files data in secured format.

If a file is entered, it will encrypt and decrypt the data that will be save in the file. And in decryption we compare a file, if comparison is possible then file will be opened, otherwise, it will display error messages.

**1.2 Intended Audience:**

* Developers Team
* Managers Team
* Client and Server

**1.3 Project Scope:**

Encryption and Decryption is mostly used to handle transactions over insecure channels of communication, such as the internet. These are used for communicating between a client program and a server.

By encrypting and decrypting other types of files, users can ensure there is no file tampering. For example, they can password-protect the file on their machine or encrypt the file before sending it over the internet for another used to decrypt.

**1.4 Project Objectives:**

It is one of the most effective approaches to achieve data security and privacy. The main objective is to secure or protect data from unauthorised access in term of viewing or modifying the data

**2.OVERVIEW**

The overview of our project is to save the data files in secured format.

The process of Encryption or Decryption takes place then the Data will be saved in the file and in Decryption process the file will be compared, if the original file matches with the decrypted file, then it will be considered as Decrypted.

**2.1 Assumptions and Dependency**

* System should have any flavour of Linux installed
* System should have either 4GB or more RAM.
* The service is used preferably on a desktop or laptop.

**3.System Features and Requirements**

**3.1 Functional Requirements:**

G1\_FR01: The application should display a main menu to select       option whether to perform encryption or decryption on the data

G1\_FR02: It should validate submenu options to select the type of encryption function and decryption function

G1\_FR03:  It should validate menu options at each level and if any    incorrect option occurs it should display an error. If it gives an invalid option, then the error should be handled by displaying few messages like “Invalid option”

G1\_FR04: The data on which encryption should be stored in a separate file and the after encrypted data should be stored in two different files

G1\_FR05: The data on which decryption should be stored in a separate file and the after decrypted data should be stored in two different files

G1\_FR06: The compare option compares normal file and the        equivalent decrypted file and checks if they are same or not

G1\_FR08:  Error handling should be done when encrypted    trying to decrypt the file in a different algorithm

G1\_FR09: It displays the statistics about the applications like Encrypted file size and Decrypted file size

G1\_FR010: It should log on to different logging             mechanisms like debug, info, error, etc...

**3.2 Technical Requirements:**

G1\_TR01:

**Process Synchronization:**

It is the task of coordinating the execution of processes in a way that no two processes can have access to the same shared data and resources. It is specially needed in a multi-process system when multiple processes are running together, and more than one processes try to gain access to the same shared resource or data at the same time.

G1\_TR02:

**Socket Programming in C – TCP:**

A socket is a communications connection point (endpoint) that you can name and address in network. Socket programming shows how to use socket APIs to establish communication links between remote and local processes

**3.3 System Requirements**

* Tools to be used:

* Val grind

**3.4 System Features:**

* Supportability: The system is easy to use.

* Reliability: It is reliable that can be trusted or believed

because we can gain the knowledge.

* Performance: The system will work on the user’s terminal.

* Availability: User can access anywhere at any time.
* Security: It provides security and privacy to data

**4.Reference**

<https://www.geeksforgeeks.org/socket-programming-cc/>

<https://www.geeksforgeeks.org/introduction-of-process-synchronization/>