**SECURE SHARE**

<DEVESH DHOBLE><0873CS181016>

<devesh.dhoble2018@sait.ac.in>

<SHUBHAM SINGH CHOUHAN><0873CS181066>

<shubham.chouchan2018@sait.ac.in>

<ADITYA SAXENA><0873CS181007>

<aditya.saxena2018@sait.ac.in>

<GAURAV KUMAR TRIPATHI><0873CS181019>

<gaurav.tripathi2018@sait.ac.in>

DR.NITIKA VATS DOOHAN

<HOD of CSE>

**Abstract**

This document is meant for describing all the features and procedures that were followed while developing the project. This document specially mentions the details of the project how it was developed, the primary requirement as well as various features and functionalities of the project and the procedures followed in achieving the objectives. Secure share is a Program to secure files (files of all extensions) and folder with user desired password as well as for sharing files over the network (peer to peer network), using cryptography.

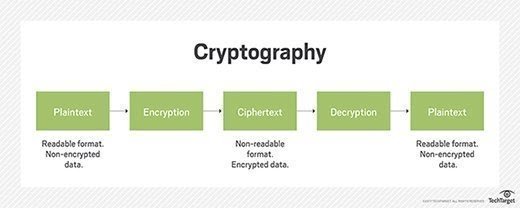
**Keywords**:

1. **INTRODUCTION** -

Secure share is a program to secure files (files of all extensions) and folder with user desired password as well as provides you to security with your friends, employs etc also includes sharing files over and within the network (peer to peer network), using cryptography. The Program will work in windows operating system as well as Linux operating system.

Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it.

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. The prefix "crypt-" means "hidden" or "vault" -- and the suffix "-graphy" stands for "writing."



2. **PROBLEM DOMAIN -**

Sometimes user share system with another person in that case if user don’t want that another person could view or access his data from the drives, files or any particular folder in that case we are providing user to encrypt those files/ folder with his preferred password and file is only visible to him whenever user decrypt it with the same password.

Since there are various softwares already available in the market which store user’s file in an encrypted manner. But users are not always sure that is there data ( images, audio, video etc) is really secured over the server or transferred in encrypted form.

3. **SOLUTION DOMAIN** -

Software development that is the technologies used in the making of project is PYTHON3 and knowledge of NETWORKING.

Since the project is all developed in python3 there is no other language or technology is required for networking. We have used various libraries for accessing system files, for encryption and decryption, for hashing passwords, and for transferring the data

whether it’s a file or simply a text message.

Some of libraries include:

os. pathlib

crypto.cipher crypto.hash crypto.Publickey crypto.random socket

threading tkinter

The design of the application is simple and user friendly which is designed with the help of tkinter.

4. **SYSTEM DOMAIN**

The project will be built on Python3 and it would be web-based application. The project has some future aspects too.

**Hardware and Software requirements:**

A computer or a laptop with windows or Linux operating system installed.

Now to secure files/folder over the system, there is no requirement of hardware or software but for transferring files to other user.

You must consider the cryptographic hardware that exists at the site that will decrypt the data. Not all types of RSA private keys are supported by all types of cryptographic hardware If you plan to use the RSA option with DFSMSdss to encrypt the data-encrypting key.

Summarizes the RSA private tokens and required cryptographic hardware for decryption.

| RSA private key token (internal) | Required cryptographic hardware |
| --- | --- |
| RSA private key token 1024 — Modulus-Exponent Internal form | One of the following:   1. Cryptographic Coprocessor feature 2. PCI X Cryptographic Coprocessor 3. Crypto Express2 Coprocessor. |
| RSA private key token 1024 — Chinese Remainder Theorem Internal form | One of the following:   1. PCI Cryptographic Coprocessor 2. PCI X Cryptographic Coprocessor 3. Crypto Express2 Coprocessor. |
| RSA private key token 2048 — Chinese Remainder Theorem Internal form | One of the following:   1. PCI Cryptographic Coprocessor with LIC January 2005 or later, and z/OS® ICSF HCR770B or later 2. PCI X Cryptographic Coprocessor 3. Crypto Express2 Coprocessor. |
| Table 1. RSA private tokens and required cryptographic hardware for decryption | |

**5. Summary**

The program is very useful in securing your assets/data (file/folder) over the system. For Company or institute where there is tire division the program is very useful.

Example: Suppose within a company if HR wants to send crucial information to his/her employee he/she can use this program and transfer files directly to each other without passing to any other employee within the company primises.Same for college if HODs want to communicate with particular faculty or any other in the staff.

One can also share files and folder over the network to anyone.

**6. Proto Type**

