ENCRYPTION-DECRYPTION SYSTEM

A

MAJOR PROJECT-I REPORT

Submitted in partial fulfillment of the requirements

for the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

GROUP NO. 12

Ambika Sadh: 0187CS181021

Under the guidance of

Prof. Umesh Kumar Sahu

(Assistant Professor)

December-2021

Department of COMPUTER SCIENCE & ENGINEERING
Sagar Institute of Science & Technology (SISTec)
Bhopal (M.P.)

Approved by AICTE, New Delhi & Govt. of M.P.
Affiliated to Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal (M.P.)

Sagar Institute of Science & Technology (SISTec), Bhopal
Department of COMPUTER SCIENCE & ENGINEERING
Bhopal (M.P.)

December-2021

CERTIFICATE

I hereby certify that the work which is being presented in the B.Tech. Major Project-I Report entitled **Encryption-Decryption System,** in partial fulfillment of the requirements for the award of the degree of *Bachelor of Technology* in *Computer Science & Engineering* and submitted to the Department of Computer Science & Engineering, *Sagar Institute of Science & Technology (SISTec),* Bhopal (M.P.) is an authentic record of my own work carried out during the period from Jul-2021 to Dec-2021 under the supervision of **Prof. Umesh Kumar Sahu (Assistant Professor).**

The content presented in this project has not been submitted by me for the award of any other degree elsewhere.

Signature

Ambika Sadh
0187cs181021

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Date: 22 November 2021

Project Guide	*HOD*	*Principal*
Prof. Umesh Kumar Sahu	*Prof. Bhavana Gupta*	*Dr. Keshavendra Choudhary*

ABSTRACT

My project title is "Encryption-Decryption System" which is GUI based application. The major functionality of my project is that the project **aims** to develop **encryption-decryption app** that would help the people to **secure their data**.

Encryption is the process of converting normal message (plaintext) into meaningless message (Cipher text). **Decryption** is the process of converting meaningless message (Cipher text) into its original form (Plaintext).

In this app there are three features. First is **text encryption-decryption** which is used to encrypt and decrypt the text, second is **image encryption decryption** which is used to encrypt and decrypt image files, third is **file encryption- decryption** which is used to encrypt and decrypt word files, excel files and text based files.

It is a **GUI based application** in which I have used waterfall model methodology.

In this application we have basically 2 modules. The first one is a 'normal user' module and the second one is 'admin module'. The normal users have to register to use this app services.

This project is the output of planning, schedule, programming skills and hard work, and this report reflects my steps taken at various levels of programming skill and I have learnt a lot during this project.

ACKNOWLEDGEMENT

Presentation inspiration and motivation have always played a key role in the success of any venture. We express our sincere thanks to **Prof. Umesh Kumar Sahu** of **Computer Science & Engineering Department**, for their invaluable guidance during the course of this project work of Sagar Institute of Science & Technology Bhopal.

We are also thankful to **Prof. Bhavana Gupta, Head of Department of Computer Science & Engineering** for cooperation and support to complete this work. We would also like to express thanks to **Dr. Swati Saxena (Vice-Principal, SISTec**) for their continuous support.

We are pleased to acknowledge **Dr. Keshavendra Choudhary (Principal SISTec)** for their invaluable guidance during the course of this project work. We extend our sincere thanks to teachers who continuously helped us throughout the project and without their guidance; this project would have been an uphill task.

Last but not least, our parents are also an important inspiration for us. So with due regards, we express our gratitude to them.

Ambika Sadh

0187cs181021

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ACRONYM	FULL FORM
SDLC	Software Development Life Cycle
SQL	Structured Query Language
HTML	Hyper Text Markup Language
UML	Unified Modeling Language

LIST OF FIGURES

Chapter 1
Introduction

CHAPTER-1
INTRODUCTION

1.1 ABOUT PROJECT

Encryption-Decryption system is a GUI based application, which is developed for making secure message by using cryptography encryption decryption algorithms.

This is GUI based application made in python language with the use of python EEL. This project is used for the people who want to secure their data by using encryption method and share data securely over the network.

Encryption is the process of converting normal message (plaintext) into meaningless message (Cipher text).**Decryption** is the process of converting meaningless message (Cipher text) into its original form (Plaintext).

1.2 PROJECT OBJECTIVE

The project aim is to create a system that can **protect electronic data** (secret information) which Consist of encryption and decryption process and to fully design an encryption and decryption algorithm.

The objectives of this project is to understand how the Encryption and Decryption process and to make secure message by using encryption.

Encryption-Decryption system is the process by which information can't be detect by the unauthorized person. The information can't be recognizing by the national foe because this system is using the process to encrypt data and decrypt data.

1.3 PROJECT DESCRIPTION

Encryption -Decryption System is GUI app which can be used in desktop. This app helps user to convert their data into secure format by using cryptography AES encryption (symmetric encryption) algorithm.

After registration users can login by using their username and password.

Registered users can use these services: 1. Text Encryption-Decryption, 2. Image Encryption- Decryption, 3. File Encryption- Decryption.

1.3.1 TEXT ENCRYPTION-DECRYPTION: In this, I have used AES (Advance Encryption Standard) Algorithm to encrypt and decrypt the text. User can convert the text into cipher text format.
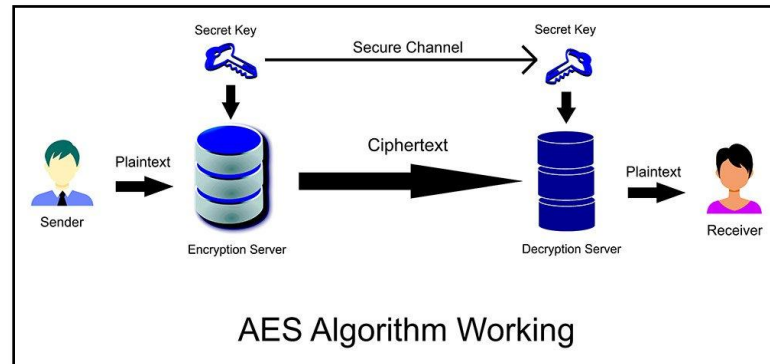

Fig 1.1 – Text Encryption-Decryption

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES

1.3.2 FILE ENCRYPTION-DECRYPTION: In this section user can encrypt and decrypt their ms word, ms excel files. In this section I have implemented encryption and decryption of an files using the XOR operator.

1.3.3 IMAGE ENCRYPTION-DECRYPTION: In this section user can encrypt and decrypt their image files. In this section I have implemented encryption and decryption of an image using the XOR operator.
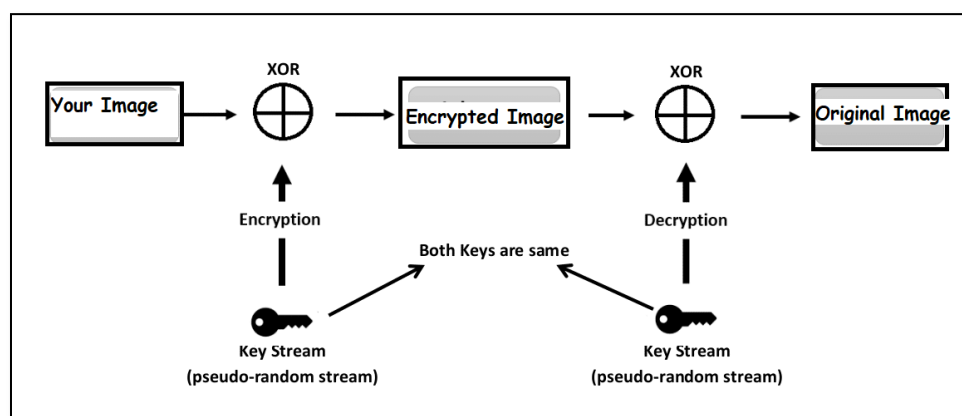

Fig. 1.2 – Image Encryption-Decryption

1.4 FUTURE SCOPE

In today's world sensitive data is increasingly used in communication over the internet. Thus security of data is the biggest concern of internet users. Millions of people are using messaging apps like whatsapp, facebook etc. To make secure communication among people, there we can use cryptography algorithms of encryption decryption.

Encryption and decryption is particularly impacted in the field of military communications and reliable security data to protection for transmitting.

This cipher text is used in the military is to send information such as direction, strategy, secret codes and other information that can't be know by the national foe during the war.

Chapter 2

Software & Hardware Requirements

CHAPTER-2
<u>SOFTWARE & HARDWARE REQUIREMENTS</u>

2.1 HARDWARE REQUIREMENTS

- Processor: Minimum 1 GHz; Recommended 2GHz or more

- Internet connection OR a wireless adapter (Wi-Fi)

- Hard Drive: Minimum 32 GB; Recommended 64 GB or more

- Memory (RAM): Recommended 4 GB or above

2.2 SOFTWARE REQUIREMENTS:

- Operating System: Windows 7 or above.

- Coding Language: Python

- Tool Kit: Python EEL

- IDE: Visual Studio Code

2.3 TOOLS & TECHNOLOGY USED:

2.3.1 PYTHON LANGUAGE: Python is an easy to learn, powerful programming language. It has efficient high-level data structures and a simple but effective approach to object-oriented programming.

2.3.2 PYTHON EEL: Eel is a **Python library for making simple offline HTML/JS GUI apps**, with full access to Python capabilities and libraries. Eel hosts a local webserver, then lets you annotate functions in Python so that they can be called from Javascript, and vice versa.

2.3.3 HTML,CSS, JAVASCRIPT: HTML provides the basic structure of sites, which is enhanced and modified by other technologies like CSS and JavaScript. CSS is **used to control presentation, formatting, and layout**. JavaScript is used to control the behavior of different elements.

2.3.4 **MYSQL DATABASE:** MySQL is a relational database management system based on the Structured Query Language, which is the popular language for accessing and managing the records in the database. MySQL is open-source and free software under the GNU license. It is supported by **Oracle Company**.

2.3.5 **VISUAL STUDIO CODE IDE:** Visual Studio Code is a **streamlined code editor** with support for development operations like debugging, task running, and version control.

Chapter 3
Problem Description

CHAPTER-3
PROBLEM DESCRIPTION

Internet communication is playing the important role to transfer large amount of data in various fields. Some of data might be transmitted through insecure channel from sender to receiver. Different techniques and methods have been using by private and public sectors to protect sensitive data from intruders because of the security of electronic data is crucial issue.

Cryptography is one of the most significant and popular techniques to secure the data from attackers by using two vital processes that are encryption and decryption.

Encryption is the process of encoding data to prevent it from intruders to read the original data easily. This stage has the ability to convert the original data (Plaintext) into unreadable format known as Cipher text. The next process that has to carry out by the authorized person is Decryption.

Decryption is contrary of encryption. It is the process to convert cipher text into plain text without missing any words in the original text. To perform these process cryptography relies on mathematical calculations along with some substitutions and permutations with or without a key.

Chapter 4
Literature Survey

CHAPTER-4
LITERATURE SURVEY

In today's digital world, encryption is emerging as a disintegrable part of all communication networks and information processing systems, for protecting both stored and in transit data world .Security has become an increasingly important feature with the growth of complex electronic communication. The AES also known as the Rijndael algorithm was selected as a Standard by National Institute of Standards and Technology (NIST). Advanced Encryption Standard (Rijndael Block Cipher) became the new US Federal Information Processing Standard on November 26, 2001[1,23] in order to replace the Data Encryption Standard (DES) which was used for more than 20 years as a common key block cipher for FIPS. Encryption is the transformation of plain data (known as plaintext) into unintelligible data (known as cipher text) through an algorithm referred to as cipher. Encryption is the transformation of data into a form that is as close to impossible as possible to read without the appropriate knowledge (a key). Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended, even those who have access to the encrypted data.

Xinmiao Zhang et al (2002) have presented various approaches for efficient hardware implementation of the Advanced Encryption Standard algorithm. They optimization methods can be divided into two classes: architectural optimization and algorithmic optimization. Architectural optimization exploits the strength of pipelining, loop unrolling and sub-pipelining. Speed is increased by processing multiple rounds simultaneously at the cost of increased area. Architectural optimization is not an effective solution in feed-back mode.

Encryption and decryption is particularly impacted in the field of military communications and reliable security data to protection for transmitting.

This cipher text is used in the military is to send information such as direction, strategy, secret codes and other information that can't be know by the national foe during the war

Chapter 5
Software Requirement Specification

CHAPTER-5
SOFTWARE REQUIREMENT SPECIFICATION

5.1 INCREMENTEAL MODEL: Incremental Model is a process of software development where requirements are broken down into multiple standalone modules of software development cycle. Incremental development is done in steps from analysis design, implementation, testing/verification, maintenance. Each iteration passes through the requirements, design, coding and testing phases. And each subsequent release of the system adds function to the previous release until all designed functionality has been implemented**.**

Phase 1: Requirement analysis

Phase 2: Design & Development
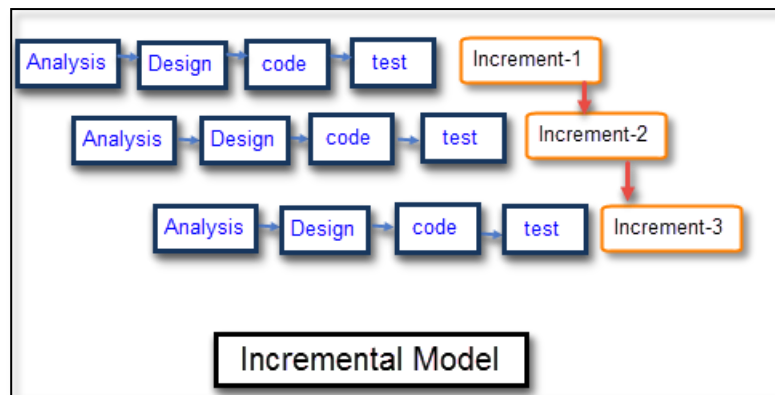
Phase 3: Testing

Phase 4: Implementation

Fig. 5.1 – Incremental Model

5.2   FUNCTIONAL REQUIREMENTS: Functional requirements define the specific functions that the system performs, along with the data operated on by the functions. The functional requirements are presented in scenarios that depict an operational system from the perspective of its end users. Included are one or more examples of all system features and an enumeration of all the specific requirements associated with these features:

The system has login mechanism to authenticate its users.The system shall verify and validate all user input and should notify in case of error detection and should help the user

in error correction.

5.2.1 ACTORS: There are two actors in this project.

- Admin
- User

5.2.1.1 Admin: The functional requirements of Admin are
as follows after "Admin Login":

- Add User
- View User Details

5.2.1.2 User: The functional requirements of user are as follows:

- Create Account
- Login
- Text Encryption
- File Encryption
- Image Encryption
- Logout

5.2.2 ADMIN: Functional requirements of Admin as follows:

R.1 Add User:

Input: Name, EmailID, Password

Output : Message –"User created successfully".

Description: Admin can registered many user by using this functionality, so that
these user can access the app services.

R.2 View all user details:

Input: Select "user_details".

Output: Display the list of all users with their details like name, phone
number, city, state etc.

Description: By using this functionality admin can view the details of all registered users.

5.2.2 USER: Functional Requirements of User as follows:

R.1: Create Account:

Input:

- Select "Get Started" button

- Enter Name

- Enter password & confirm password

- Enter Email Id

- Click on Signup button

Output: Display Message "User created successfully".

Exceptions: If username and email id already exist then generate error. Message: "User already exists". If email is not in format then generate error. Message: "Please enter valid format of email Id".

Description: Create Account function will do registration of user with their details. After creating account user can login into app.

R.2: Login

Input:

- Click on login button

- Enter Username

- Enter Password

Output: message- "Login successful" and user will redirect to welcome Page.

Exception: If username and password is invalid then generate message. Message: "Username name and password is wrong".

Description: By using login, user can login into the account and view app services.

R.3: Text Encryption

Input:

- Enter Text

- Enter Key

- Click on Encrypt Button or Decrypt Button

Output: message – "Encryption done successfully" or "Decryption done successfully!".

Description: This is used to encrypt and decrypt text.

R.4: Image Encryption

Input:

- Open Image using button
- Enter Image Path
- Enter Key
- Click on Encrypt Button or Decrypt Button

Output: message – "Encryption done successfully" or "Decryption done successfully!".

Description: This is used to encrypt and decrypt image.

R.5: File Encryption

Input:

- Enter file path
- Enter Key
- Click on Encrypt Button or Decrypt Button

Output: message – "Encryption done successfully" or "Decryption done successfully!".

Description: This is used to encrypt and decrypt file.

R.5: Logout

Input: Select "Logout" tab in navigation bar

Output: System generate message – "Logout successfully" then user will redirect to login page.

Description: This module wills logout the user account form app.

5.3 NON – FUNCTIONAL REQUIREMENTS

Non-functional requirements address aspects of the system other than the specific functions it performs. These aspects include system performance, costs, and such general system characteristics as reliability, security, and portability. The non-functional requirements also address aspects of the system development process and operational personnel. It include following.

5.3.1 AVAILABLITY: The system provides the easy app service for the users and it is online system so any person across the world, having internet can access this service. Internet network using 10 mbps or higher speed network required.

5.3.2 EFFICIENCY: Efficient usable interfaces will allow the users to navigate easily for doing meditation and exercise.

5.3.3 RELIABLE: Because of the user is preregister, and then user will have a reliable to access anytime.

5.3.4 SECURITY: A secure system protects your data. This software is secure, we provide login information of user and admin, so only by using correct login id password user or admin can use this system.

5.3.5 ACCURACY: The system is user friendly and accurate.

5.3.6 ROBUSTNESS: We follow incremental model and divide the project in small modules and testing, so the project becomes robust.

5.3.7 USABILITY: Our app can be used by kids, adults and teenagers, means any kind of user can use app services.

Chapter 6
Software Design

CHAPTER-6

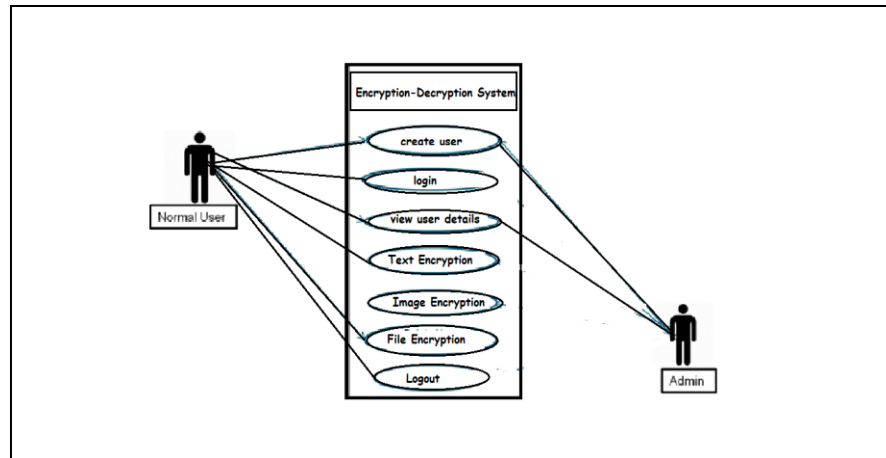# SOFTWARE DESIGN

6.1 USE CASE DIAGRAM:

Fig. 6.1 – Admin-User Functions

6.1.1. DESCRIPTION: In above Use case diagram shows that there are two actors:

1. User: User can create user profile, Login into app. User can encrypt or decrypt text, image and file.

2. Admin: Admin can create user profile, view user details and delete use profile From database.
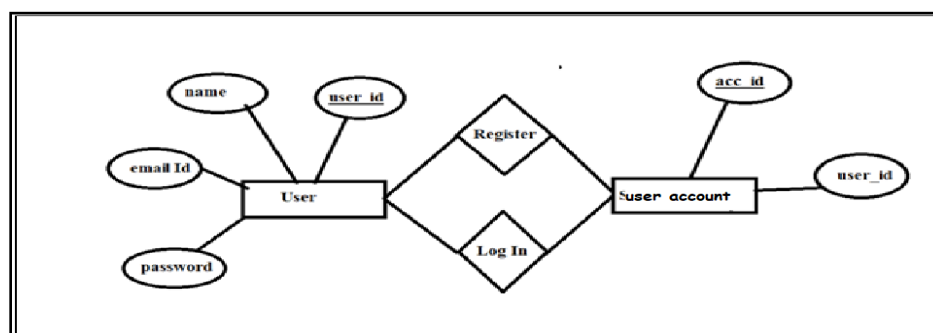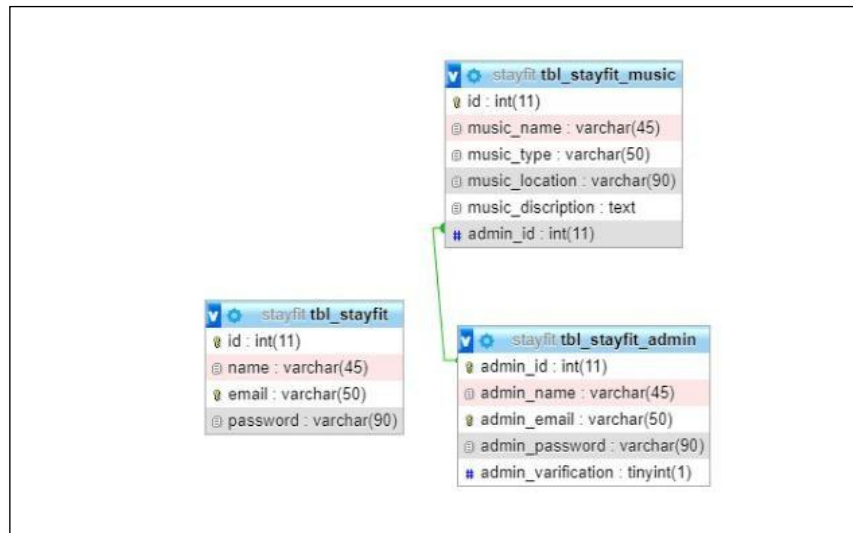
6.2 ER DIAGRAM:

Fig. 6.2 – ER Diagram

6.3 TABLE STRUCTURE:

Fig. 6.3 – Table Structure

6.4 FLOW CHART:

6.4.1 AES ENCRYPTION FLOW CHART:
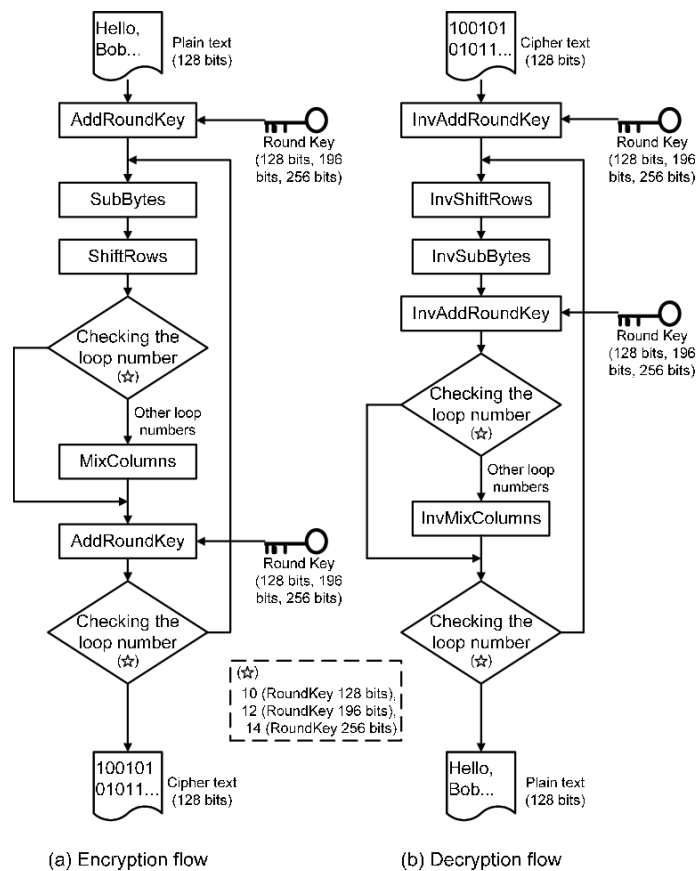
Fig. 6.4 – AES Encryption Flow Chart

6.4.2 IMAGE ENCRYPTION FLOW CHART:
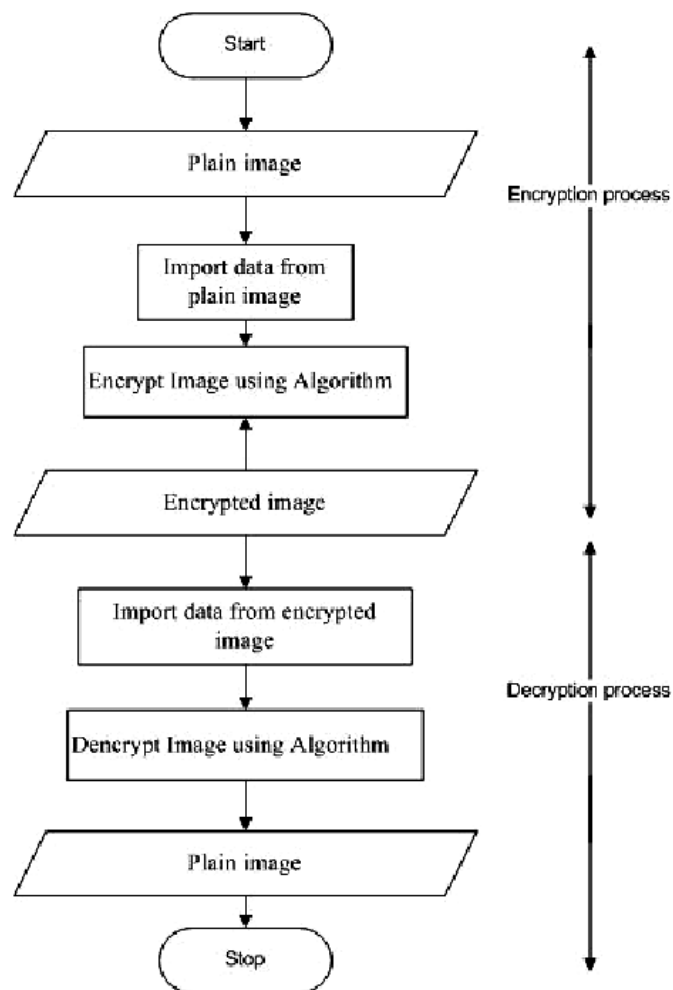
Fig. 6.5 – Image Encryption Flow Chart

Chapter 7
Output Screens
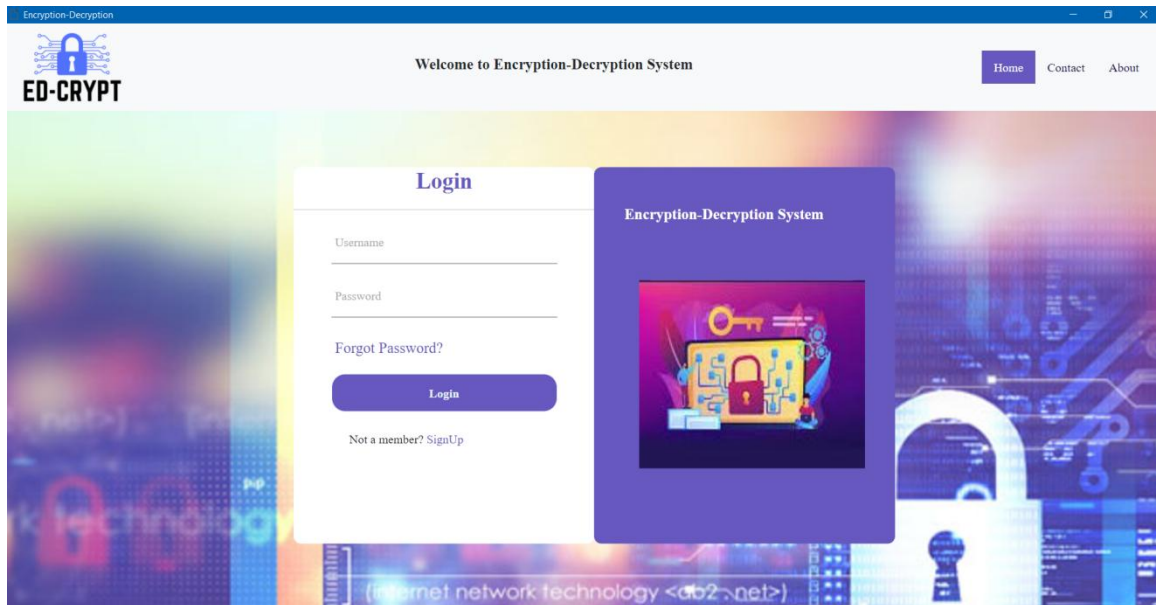
CHAPTER 7
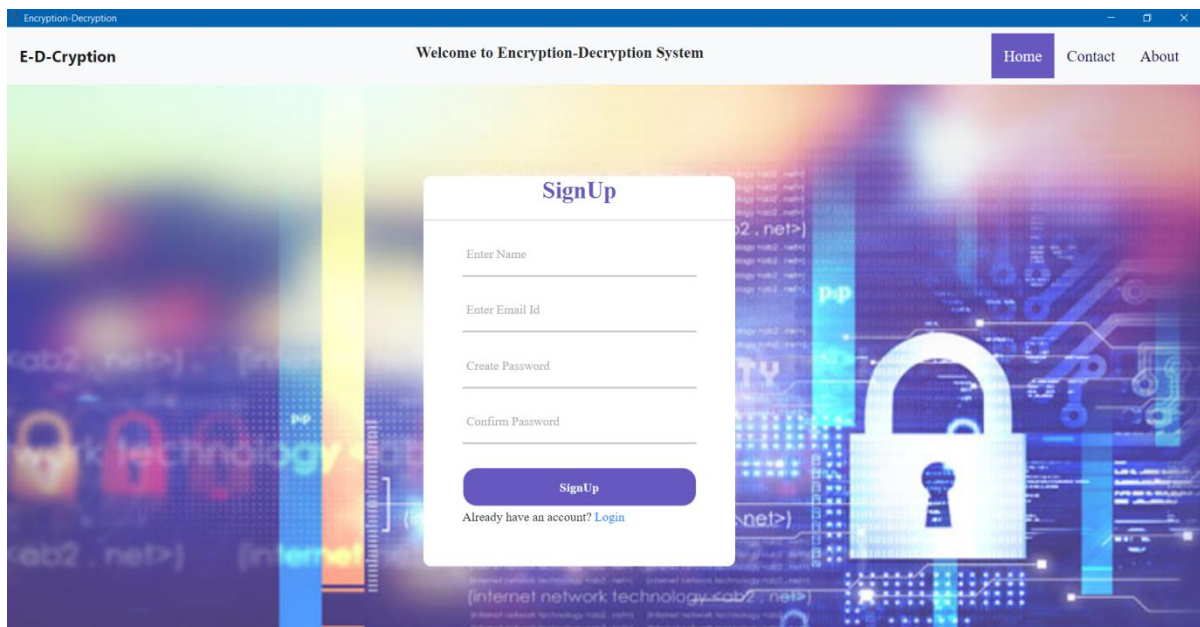# OUTPUT SCREENS

7.1 LOGIN PAGE

Fig. 7.1 – Login Page

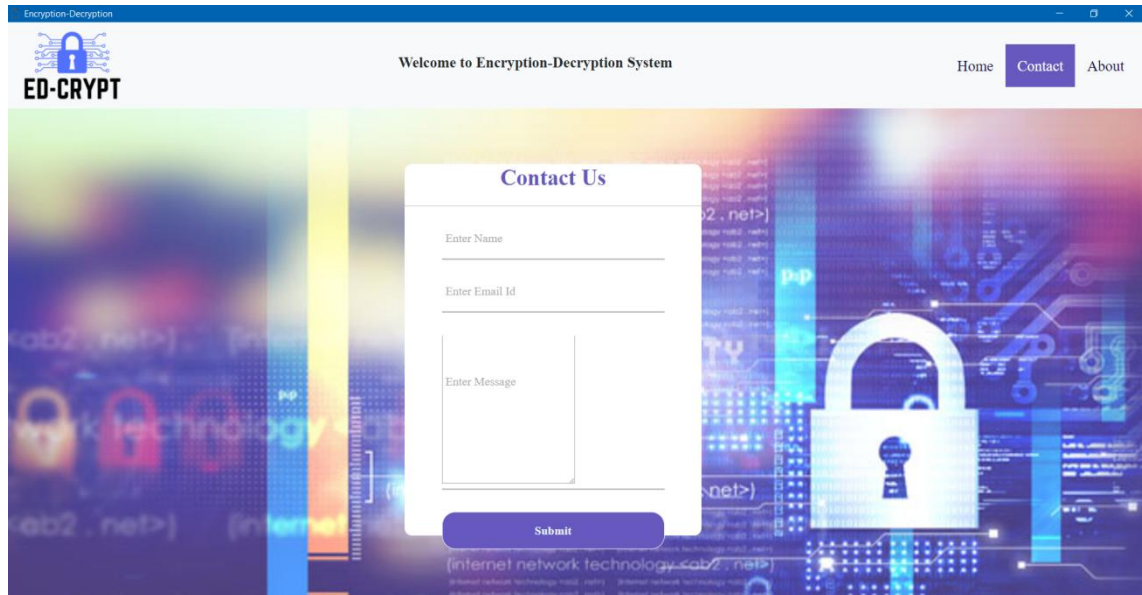## 7.2 SIGNUP PAGE

Fig. 7.2 – SignUp Page

7.3 CONTACT US PAGE

Fig. 7.3 – Contact Us Page

7.4 HOME PAGE
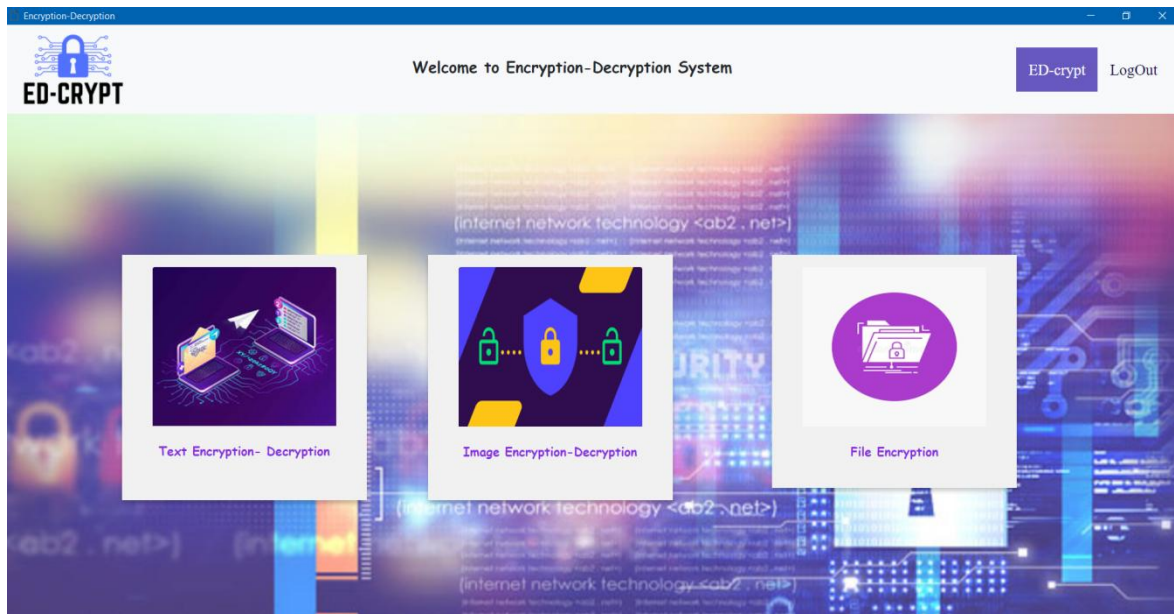
Fig. 7.4 – Home Page

7.5 TEXT ENCRYPTION-DECRYPTION

Fig. 7.5 – Text Encryption System

7.6 FILE ENCRYPTION-DECRYPTION

Fig. 7.6 – File Encryption System
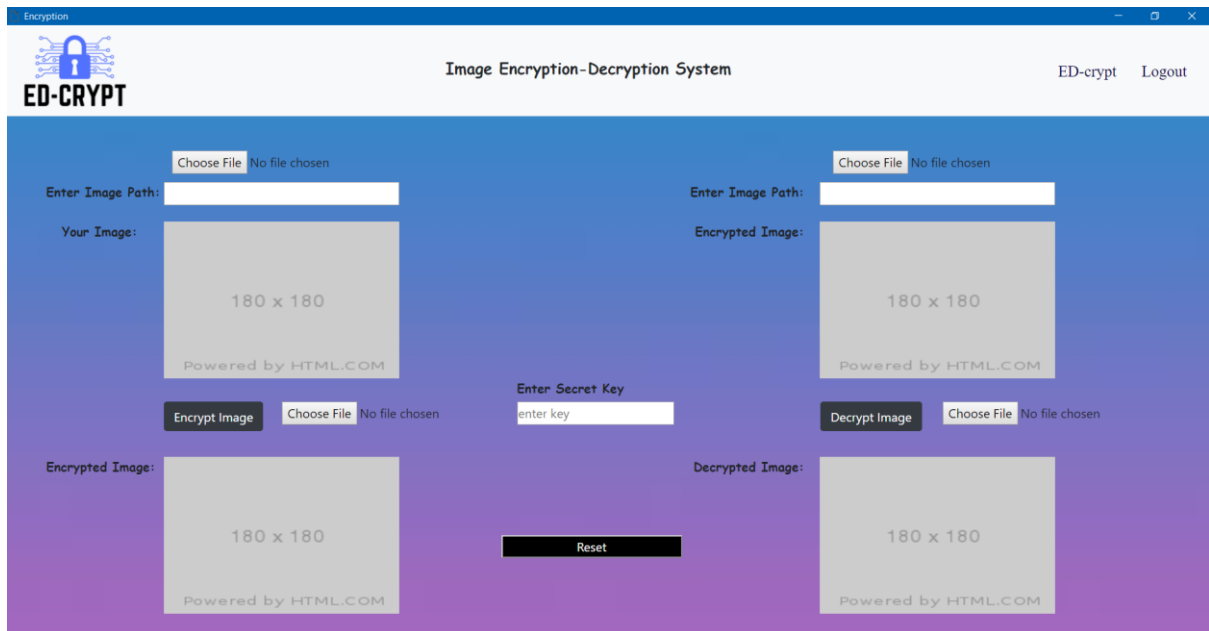
7.7 IMAGE ENCRYPTION-DECRYPTION

Fig, 7.7 – Image Encryption System
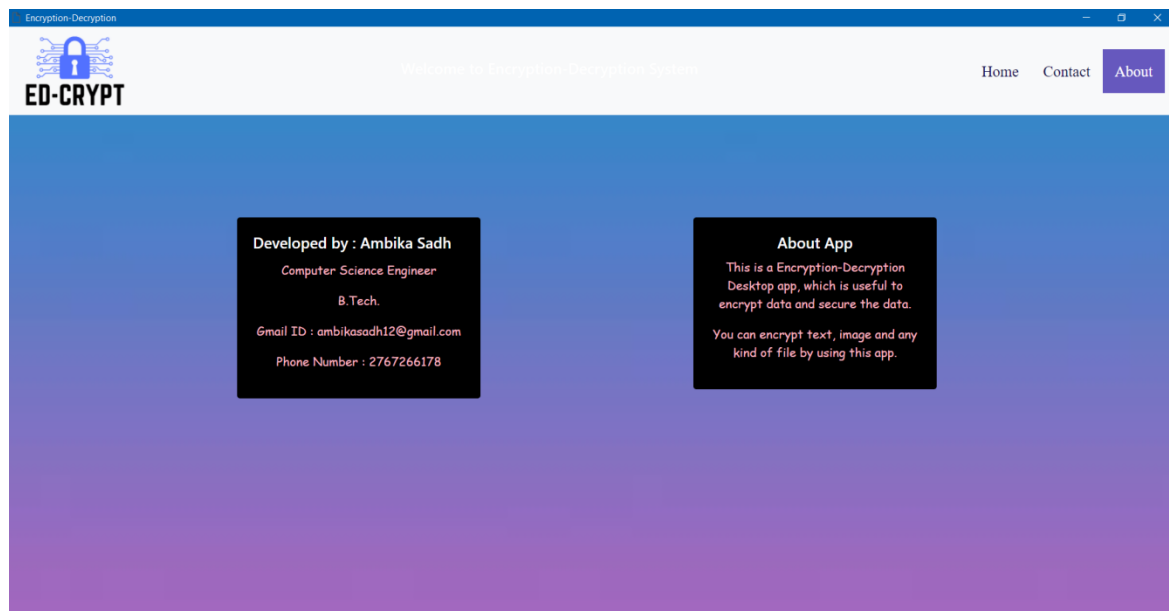
7.8 ABOUT US PAGE

Fig. 7.8 – About Us Page

Chapter 8
Deployment

CHAPTER 8
DEPLOYMENT

We have deployed or host our GUI app on github. GitHub is one of the world's largest community of developers. It's an intricate platform that fosters collaboration and communication between developers. GitHub has a number of useful features that enable development teams to work together on the same project and easily create new versions of software without disrupting the current versions.

8.1 DEPLOYEMENT PROCESS

- First, install Git from the official site https://git-scm.com/downloads and install it in your PC then after creating your profile on Github https://github.com, make a repository and clone (copy the link of your repository) your repository with HTTPS.

- Now go to Git Bash software and use this command to clone this repository to your PC.

  git clone [your copy link]

- Git Bash don't use **ctrl**+**V** to paste any segment so paste your link by using **shift**+**Ins** key

- Now you have cloned your Github repository to your system now add all you relevant codes in that cloned directory to upload it to your GitHub Profile.

- Now when you will type command **git status** you will see all those files you have added to the directory in red-colored untracked file segment like this. Here **laddu.txt** is the unracked file that I have just moved to the directory.

- Now to add these files into **staging** area (Staging is a step before the commit process in git. That is, a commit in git is performed in two steps: staging and actually commit. As long as a changeset is in the staging area, git allows you to edit it as you like to replace staged files with other versions of staged files, remove changes from staging, etc.) use command

- git add <files_Name with their respective extensions>

- Here you can see that now your files are successfully added to the staging area. Now you need to commit these files with a description. And to do so use

- git commit -m "Your description"

- Now we have committed these changes in our local system and to upload these changes to our remote profile use command

- git remote -v

- push these changes in our Github repository. Use the command below to upload your files or any changes.

- git push origin master

- Now,You have successfully uploaded your files to your GitHub repository.
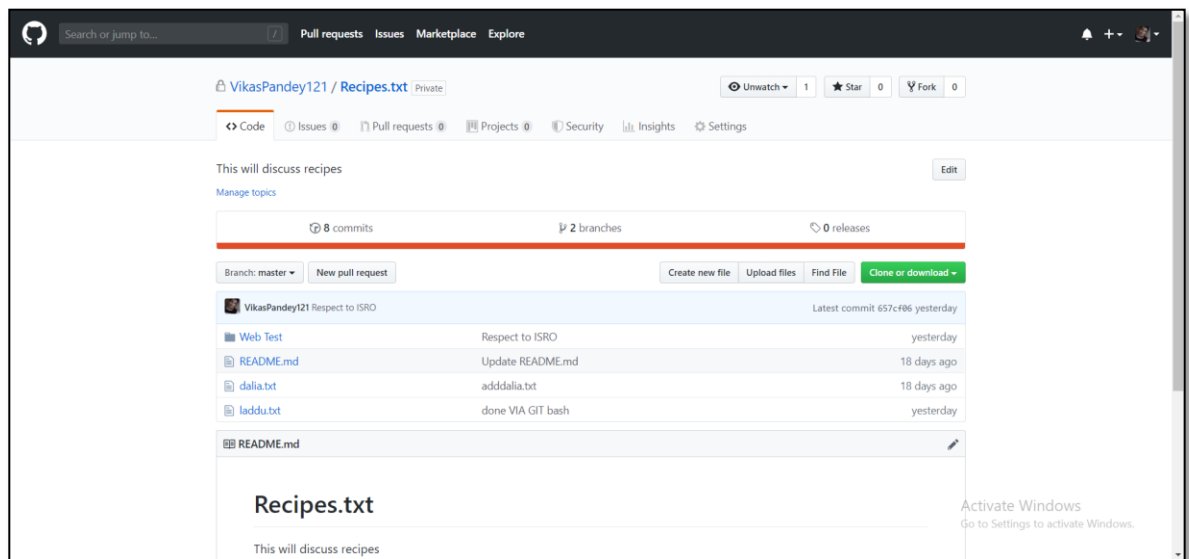
Fig. 8.1 – Github Screen

REFERENCES

WEBSITES

1. https://www.geeksforgeeks.org/create-html-user-interface-using-eel-in-python
2. https://www.simplilearn.com/data-encryption-methods-article/
3. https://www.geeksforgeeks.org/encrypt-and-decrypt-image-using-python/

PROJECT SUMMARY

About Project

Title of the project	Encryption- Decryption System
Semester	7th
Members	1
Team Leader	Ambika Sadh
Describe role of every member in the project	Role: Full Stack Developer
What is the motivation for selecting this project?	The motivation is to make secure our data by using encryption techniques so that we can share our data in secure format.
Project Type (Desktop Application, Web Application, Mobile App, Web)	Desktop Application

Tools &Technologies

Programming language used	Python
Compiler used (withversion)	Python 3.8
IDE used (with version)	Visual Studio Code 2.2
Front End Technologies (with version, wherever Applicable)	HTML5 JavaScript 6 CSS3
Back End Technologies (with version, wherever applicable)	Python 3.8
Database used (with version)	MySQL (10)

Software Design& Coding

Is prototype of the software developed?	No
SDLC model followed (Waterfall, Agile, Spiral etc.)	Incremental model

Why above SDLC model is followed?	We used this model because; it is a process of software development where requirements are broken down into multiple standalone modules of software development cycle. Incremental development is done in steps from analysis design, implementation, testing/verification, maintenance. Each iteration passes through the requirements, design, coding and testing phases. And each subsequent release of the system adds function to the previous release until all designed functionality has been implemented.
Justify that the SDLC model mentioned above is followed in the project.	We have used incremental model in which we have also broken down requirements into 3 modules: 1. Signup & Login module, 2. Text Encryption Module 3. Image and File Encryption Module. After that in each iteration passes through the requirements, design, coding and testing phases. Our project has taken 3 iterations to complete the project.
Software Design approach followed (Functional orObjectOriented)	Functional Oriented Approach
Name the diagrams developed (according to the Design approach followed)	Use Case Diagram
In case Object Oriented approach is followed, which of the OOPS principles are covered in design?	
No. of Tiers (example 3-tier)	3
Total no. of front end pages	8
Total no. of tables in database	2
Database is in which Normal Form?	3NF
Are the entries in database encrypted?	No

Front end validations applied (Yes / No)	Yes
Session management done (in case of web applications)	-
Is application browser compatible (in case of web applications)	-
Exception handling done (Yes / No)	Yes
Commenting done in code (Yes / No)	Yes
Naming convention followed (Yes / No)	Yes
What difficulties faced during deployment of project?	I have faced difficulty during working with frontend in visibility of data after encryption and working with python eel.
Total no. of Use-cases	1
Give titles of Use-cases	Admin-User Functions

Project Requirements

MVC architecture followed (Yes / No)	No
If yes, write the name of MVC architecture followed (MVC-1, MVC-2)	-
Design Pattern used (Yes / No)	Yes
If yes, write the name of Design Pattern used	ER Diagram, Table structure of database, Flow chart of Text and Image Encryption, Use Case Diagram
Interface type (CLI / GUI)	GUI
No. of Actors	2
Name of Actors	Admin, User
Total no. of Functional Requirements	5
List few important non-Functional Requirements	• Availability: The system provides the easy app service for the users and it is online system so any person across the world, having internet can access this service. Internet network using 10 mbps or higher

	speed network required.
	• Efficiency: Efficient usable interfaces will allow the users to navigate easily for doing meditation and exercise.
	• Reliable: Because of the user is preregister, and then user will have a reliable to access anytime.
	• Portability and Compatibility: Compatible with android with 9.0 or above version in android phones. The system acts as an "open" platform, then user have a flexible searching environment.
	• Security: A secure system protects your data. This software is secure, we provide login information of user and admin, so only by using correct login id password user or admin can use this system

Testing

Which testing is performed? (Manual or Automation)	Manual
Is Beta testing done for this project?	No

Write project narrative covering above mentioned points

"Encryption-Decryption system" is a desktop based application, which is developed for making secure message by using cryptography encryption decryption algorithms.

Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext). Whereas Decryption is the process of converting meaningless message (Ciphertext) into its original form (Plaintext).

SDLC Model: I have used incremental model in which I have also broken down requirements into 3 modules: Signup & Login module, Text Encryption module and Image & File Encryption module. After that in each iteration passes through the requirements, design, coding and testing phases. My project has taken 3 iterations to complete the project, at the end combine all modules and developed the project.

Functional oriented approach is followed and Use case diagram of admin – user functions made.

MySQL database is used and 2 table created in database. Database is in 3 NF. I have used Python EEL to develop the frontend part of GUI application.

In my project there are 2 actors- user and admin which have 5 and 2 functional requirements respectively.

Non functional requirements are security, availability, robustness, portability and so on.

Ambika Sadh   **Guide Signature**

0187cs181021   **Prof. Umesh Kumar Sahu**

APPENDIX-1

GLOSSARY OF TERMS

Encryption: Encryption in cryptography is a process by which a plain text or a piece of information is converted into cipher text or a text which can only be decoded by the receiver for whom the information was intended.

Decryption: Decryption is a process that transforms encrypted information into its original format. The process of encryption transforms information from its original format — called plaintext — into an unreadable format — called ciphertext — while it is being shared or transmitted.

AES: The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

HTML5: HTML5 is a markup language used for structuring and presenting content on the World Wide Web. It is the fifth and last major HTML version that is a World Wide Web Consortium (W3C) recommendation. The current specification is known as the HTML Living Standard.

CSS3: Cascading Style Sheets (CSS) is a language that is used to illustrate the look, style, and format of a document written in any markup language. In simple words, it is used to style and organize the layout of Web pages. CSS3 is the latest version of an earlier CSS version, CSS2.

Python EEL: Eel is a Python library for making simple offline HTML/JS GUI apps, with full access to Python capabilities and libraries. Eel hosts a local webserver, then lets you annotate functions in Python so that they can be called from Javascript, and vice versa.