**A MINI PROJECT REPORT**

**ON**

LEARNING PATH DASHBOARD FOR ENHANCING SKILLS.

Submitted to

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY, HYDERABAD

In partial fulfilment of the requirement for the award of the degree of

**BACHELOR OF TECHNOLOGY**

**in**

**COMPUTER SCIENCE AND ENGINEERING**

**By**

|  |  |
| --- | --- |
| **AMULYA REDDY YERUVA** | **217Y1A0572** |
| **SRINIVAS RAO TAMMIREDDY** | **217Y1A05C0** |

**Under the Guidance of**

Mr. T. S. Srinivas,

Associate Professor



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**



AUGUST, 2024



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

Date:

# CERTIFICATE

This is to certify that the project work entitled “**MAGPIE: A DEMONSTRATION OF SYMMETRIC ENCRYPTION**” work done by **AMULYA REDDY Y (217Y1A0572), SRINIVAS RAO T (217Y1A05C0) students** of Department of Computer Science and Engineering, is a record of bona fide work carried out by the members during a period from FEB,2024 to JULY,2024 under the supervision of **Mr. T. S. SRINIVAS**. This project is done as a fulfilment of obtaining Bachelor of Technology Degree to be awarded by Jawaharlal Nehru Technological University Hyderabad, Hyderabad.

The matter embodied in this project report has not been submitted by us to any other university for the award of any other degree.

|  |  |
| --- | --- |
| **AMULYA REDDY Y**  **(217Y1A0572)** | **SRINIVAS RAO T (217Y1A05C0)** |

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

Date: Mr. S. PRATAP SINGH

The Viva-Voce Examination of above students, has been held on………………………

|  |  |
| --- | --- |
|  | External Examiner |
| Head of the Department |  |
| Principal/Director | |

# ACKNOWLEDGEMENTS



We are happy to express our deep sense of gratitude and thanks to **Dr. R. Murali Prasad**,

Principal and **Dr. P. Sridhar, Director**, Marri Laxman Reddy Institute of Technology &

Management, and for having provided us with adequate facilities to pursue our project.

We would like to thank **Dr K. Abdul Basith**, Professor and Head, Department of Computer

Science Engineering, Marri Laxman Reddy Institute of Technology & Management, for having

provided the freedom to use all the facilities available in the department, especially the

laboratories and the library.

We sincerely thank our Project Coordinator, **Dr. Prathap Singh**, Associate Professor,

Department of Computer Science and Engineering, Marri Laxman Reddy Institute of

Technology & Management who has not only shown utmost patience, but was fertile in

suggestions.

We are very grateful to our Project Guide **Dr. Prathap Singh**, Associate Professor,

Department of Computer Science and Engineering, Marri Laxman Reddy Institute of

Technology & Management, for her extensive patience and guidance throughout our project

work.

We sincerely thank our seniors and all the teaching and non-teaching staff of the

Department of Computer Science for their timely suggestions, healthy criticism and motivation

during this work. We would also like to thank our classmates for always being there whenever

we needed help or moral support. With great respect and obedience, we thank our parents and

brother who have been the backbone of all our efforts. Finally, we express our immense

gratitude with pleasure to the other individuals who have either directly or indirectly

contributed at right time for the development and success of this work.

# INDEX

**CHAPTERS Page No.**

**ABSTRACT 7**

**LIST OF FIGURES 6**

**1. INTRODUCTION 8**

1.1 Project Overview 8

1.2 Objective 9

**2. LITERATURE REVIEW 11**

2.1 Survey Details 11

2.2 Existing System 12

2.3 Proposed System 12

**3. SYSTEMREQUIREMENT ANALYSIS 13**

3.1 Requirement Analysis 13

3.2 Requirements Specifications 13

3.3Language Specifications 14

3.4 Technologies Required 14

**4. SYSTEM DESIGN 16**

4.1 System Architecture 16

4.2 Use Case Diagram 16

4.3 Dataflow Diagram 17

4.4 Class Diagram 18

4.5 Sequence Diagram 19

**5. PROJECT DESCRIPTION 21**

**6. IMPLEMENTATION & RESULT 24**

6.1 Libraries Used 24

6.2 Code of the Project 24

6.3 Result / Output Screen 32

**7. TESTING 36**

7.1 Testing Strategies 36

7.2 Types of Testing 36

7.3 Test Cases 38

**8. SYSTEM RESULTS 40**

8.1 Outcomes of the Proposed System 40

8.2 Screenshots 40

**9. CONCLUSION AND FUTURE SCOPE 41**

9.1 Conclusion 41

9.2 Future Scope 41

**10. REFERENCES 42**

10.1 symmetric\_encryption.py 42

10.2 CLI.py 43

10.3 GUI.py 43

# LIST OF FIGURES

**Fig. No. Fig. Name Page No.**

1 Fig 4.1 Architecture 16

2 Fig 4.2 Use Case Diagram 17

3 Fig 4.3 Dataflow Diagram 18

4 Fig 4.4 Class Diagram 19

5 Fig 4.5 Sequence Diagram 20

6 Fig 6.2.1 Encryption (GUI) 33

7 Fig 6.2.2 Decryption (GUI) 34

8 Fig 6.2.3 Encryption and Decryption (CLI) 35

9 Fig 8.1 Final Results 41

# LIST OF TABLES

**S. No. Table Name Page No.**

1 Table 7.3 Test Case 40

# ABSTRACT

The project, named Magpie, is a Python-based application that implements symmetric encryption (END to END Encryption) and hashing techniques to secure text messages. It provides both a command-line interface (CLI) and a graphical user interface (GUI) for users to enter, encrypt, decrypt, and verify text messages using a secret key. The application utilizes the shift cipher for encryption and the SHA-256 algorithm for hashing.

The main objective of the project is to demonstrate the fundamental principles of cryptography and information security in a simple and interactive manner. It includes a tutorial and a README file that explain the concepts and usage of the application. Symmetric encryption using the shift cipher. Hashing uses the SHA-256 algorithm. Command-line interface (CLI) for text message operations. Graphical user interface (GUI) for easy interaction. Secret key-based encryption and decryption. Text message verification. Tutorial and README files for guidance.

The above abstract also aims for encryption and decryption of image by generating a super key and also using SHA 512 algorithm at a later stage.

The purpose of the Magpie project is to provide a practical example of how symmetric

encryption and hashing techniques can be used to secure text messages. By implementing a command-line interface and a graphical user interface, the project aims to make the concepts of cryptography and information security more accessible to users. The tutorial and README files further enhance the understanding of the application's concepts and usage.

**CHAPTER 1**

# INTRODUCTION

* 1. **PROJECT OVERVIEW**

Encryption and decryption are fundamental concepts in the field of cryptography, playing a crucial role in securing sensitive information and communications.

Encryption is the process of converting plaintext (readable data) into ciphertext (unreadable data) using an algorithm and an encryption key. The goal of encryption is to ensure that even if the ciphertext is intercepted or accessed by unauthorized parties, it remains unintelligible without the corresponding decryption key.

Decryption is the process of converting ciphertext back into its original plaintext form using a decryption algorithm and the corresponding decryption key. Decryption reverses the encryption process, allowing authorized parties to access and interpret the original message or data.

**Key Components of Encryption and Decryption:**

1. **Plaintext:** The original message or data that is to be encrypted.

2. **Ciphertext:** The encrypted form of the plaintext, which appears as random and unintelligible data.

3. **Encryption Algorithm:** A mathematical procedure or algorithm used to transform plaintext into ciphertext. Common encryption algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and RSA.

4. **Encryption Key:** A piece of information used by the encryption algorithm to perform the encryption process. The security of the encryption relies heavily on the strength of the encryption key.

5.**Decryption Algorithm:** A mathematical procedure or algorithm used to transform ciphertext back into plaintext. The decryption algorithm must be the inverse of the encryption algorithm.

6. **Decryption Key:** A piece of information used by the decryption algorithm to reverse the encryption process and recover the original plaintext. The decryption key must match the encryption key used to encrypt the data.

In summary, encryption and decryption are essential techniques for securing data and communications, enabling confidentiality, integrity, and authentication in various applications across industries.

* 1. **OBJECTIVE**

The objective of the Magpie is to provide a simple and secure solution for symmetric encryption and decryption of text messages. The module offers functionalities to generate encryption keys, encrypt plaintext messages, and decrypt ciphertext messages using the Fernet encryption scheme from the cryptography library.

**Key Components:**

1. Key Management:

**generate\_key ():** Generates a new symmetric encryption key and saves it to a file named ‘key.key’.

**load\_key ():** Loads the encryption key from the ‘key.key’ file. If the file does not exist, it generates a new key.

2. Encryption:

encrypt\_message (message: str, key: bytes) -> str: Encrypts a message using symmetric encryption with the provided key.

3. Decryption:

decrypt\_message (encrypted\_message: str, key: bytes) -> str | type [Invalid Token] | Exception | type [BinasciiError]: Decrypts an encrypted message using the provided key. It handles potential errors such as invalid tokens or bin ascii errors.

4. Error Handling:

The module handles errors such as missing key files and invalid tokens during decryption.

It raises custom exceptions (`KeyNotFoundError`) to notify users of key-related issues.

5. User Interface:

Magpie aims to offer a user-friendly interface and straightforward implementation, making it accessible to both beginners and experienced users. This could include providing clear documentation, intuitive APIs, and possibly graphical user interfaces (GUIs) or command-line interfaces (CLIs) for interacting with the sentiment analysis functionalities.

**Conclusion:**

The Symmetric Encryption Module offers a convenient and secure solution for symmetric encryption and decryption tasks in Python applications. It provides an easy-to-use interface while prioritizing security and error handling.

**CHAPTER 2**

# LITERATURE REVIEW

**2.1 SURVEY DETAILS**

Synthesizing information from scholarly articles, conference papers, books, and technical reports, a literature review on encryption and decryption provides a comprehensive understanding of cryptographic techniques, their applications, and their role in ensuring information security in the digital age.

Encryption and decryption typically cover a broad range of topics, including cryptographic algorithms, security protocols, applications, challenges, and advancements. Here’s an overview of what a literature review on encryption and decryption might include:

1. Historical Perspective:

Introduction to the evolution of encryption techniques from ancient times to modern cryptography.

Overview of classical ciphers such as Caesar cipher, Vigenère cipher, and Enigma machine.

2. Fundamental Concepts:

Explanation of basic cryptographic principles like symmetric encryption, asymmetric encryption, hashing, and digital signatures.

Description of common encryption algorithms such as AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and ECC (Elliptic Curve Cryptography).

3. Cryptographic Techniques:

Exploration of symmetric encryption algorithms and their modes of operation (e.g., ECB, CBC, GCM).

Discussion of asymmetric encryption algorithms and key exchange protocols (e.g., Diffie-Hellman key exchange, RSA key exchange).

Analysis of hash functions and their applications in data integrity verification.

4. Security Protocols:

Overview of secure communication protocols like TLS (Transport Layer Security) and its predecessor SSL (Secure Sockets Layer).

Examination of secure email protocols such as PGP (Pretty Good Privacy) and S/MIME (Secure/Multipurpose Internet Mail Extensions).

5. Applications and Use Cases:

Examination of encryption techniques in cloud computing, IoT (Internet of Things), and mobile communication.

Case studies highlighting the role of encryption in protecting sensitive data and mitigating security risks.

6. Security Analysis:

Research papers often include security analysis of cryptographic algorithms and systems, including symmetric encryption schemes like Fernet.

Security analysis may cover aspects such as resistance to known cryptographic attacks, cryptographic strength, and potential vulnerabilities or weaknesses.

7. Best Practices and Guidelines:

Literature might include best practices, guidelines, and standards for designing, implementing, and deploying cryptographic systems.

Best practices may cover areas such as cryptographic algorithm selection, key management, secure coding practices, and compliance with security standards and regulations.

**2.2 EXISTING SYSTEM**

1. The Existing Version of the Encryption System doesn’t provide the GUI (Graphical User Interface).
2. Haven’t involved Hash libraries (SHA-256) and Fernet.
3. Custom exceptions like key not found error are raised when necessary

**2.3 PROPOSED SYSTEM**

1. The Proposed Version of the Encryption System provides a User-friendly GUI.
2. Have used Hash libraries (SHA-256) and Fernet Cryptography.
3. Log errors for debugging and auditing purposes

**CHAPTER 3**

# SYSYTEM REQUIREMENTS ANALYSIS

**3.1 REQUIREMENT ANALYSIS**

**Project Perspective:**

Magpie implements a Python-based encryption and decryption system using the Fernet symmetric encryption scheme. It offers modular functions for key generation, loading, encryption, and decryption, while incorporating error handling mechanisms. The system interacts with the file system for key management and adheres to security best practices. With documentation, testing, and potential integration into various applications, it ensures secure data communication and storage, emphasizing scalability, compliance, and security auditing for robust deployment.

**Project Features:**

Magpie features collectively enable the project to offer a reliable and secure encryption and decryption solution, suitable for integration into a range of applications requiring data security.

1. Key management
2. Error Handling
3. Encryption and Decryption
4. Scalability
5. File interaction
6. Robustness
7. Security

**3.2 REQUIREMENT SPECIFICATIONS**

Certainly, here are the system specifications with numerical values:

1. Operating System:

- Compatible with Windows, macOS, Linux.

2. Python Version:

- Requires Python 3.x interpreter.

3. cryptography Library:

- Utilizes cryptography library.

- Installation: pip install cryptography.

4. Disk Space:

- Negligible: Minimal disk space for key file and messages.

5. Processing Power:

- Minimal processing power required.

6.RAM:

- Modest: Small amount of RAM needed for script execution and key loading.

7. Input/Output:

- Relies on standard file input/output operations.

8. Network Connectivity:

- Not required for core functionality.

These numerical specifications provide concise information about the system’s requirements and capabilities, aiding in deployment and resource allocation.

**3.3 LANGUAGE SPECIFICATIONS**

**Python:** Python is a high-level, general-purpose programming language. Its design philosophy emphasizes code readability with the use of significant indentation.

Python is dynamically typed and garbage-collected. It supports multiple programming paradigms, including structured (particularly procedural), object-oriented and functional programming.

It is often described as a “batteries included” language due to its comprehensive standard library.

**3.4 TECHNOLOGIES REQUIRED**

This Python code utilizes several libraries and features. Here are the technologies required and used in this code:

1. **Python**: The code itself is written in Python, so you need Python installed on your system to run it.

2. **cryptography**: This library provides cryptographic recipes and primitives to Python developers. In this code, it’s used for symmetric encryption and decryption, specifically utilizing “Fernet” which is a symmetric encryption algorithm.

3. **os**: The os module provides a way to interact with the operating system. In this code, it’s used for operations like getting the current working directory and checking if a file exists.

4. **os.path**: This module provides functions to interact with the filesystem path. In this code, it’s used for checking if a file exists.

5. **binascii**: This module provides tools for converting binary data to ASCII and vice versa. In this code, it’s used for handling errors related to binary ASCII conversions.

These are the main technologies used in this code. Make sure you have Python installed along with the cryptography library. You can install cryptography via pip:

> Pip install cryptography

6. **Tkinter**: Tkinter is the standard GUI (Graphical User Interface) toolkit for Python. It provides a fast and easy way to create GUI applications. It is used for creating windows, buttons, text fields, labels, etc., and handling events like button clicks, text input, etc.

7. **rich**: Rich is a Python library for rich text and beautiful formatting in the terminal. It’s used here for displaying colorful and formatted text in the command-line interface.

> Pip install rich

Ensure you have the necessary permissions to perform file operations in the directory where you run this code, as it deals with file I/O for storing and loading keys.

**CHAPTER 4**

# SYSTEM DESIGN

**4.1 SYSTEM ARCHITECTURE**

Architecture describes the overall functionality of the project with all the modules specified in it. It gives a clear picture of the internal process of the projects. The architecture along with modules can be displayed as the following.

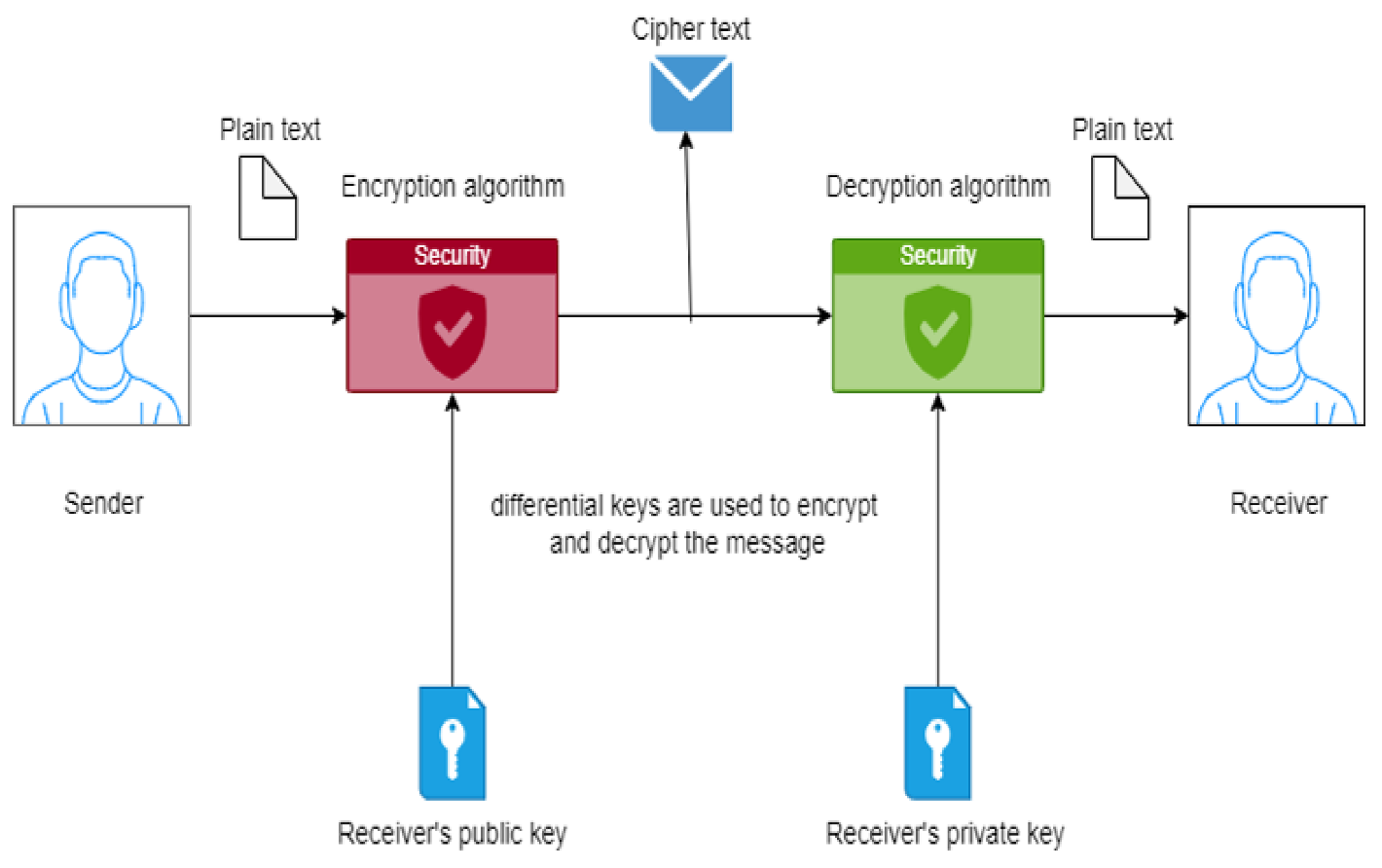


Figure 4.1: Architecture

The above figure shows the basic architecture of the encryption and decryption process.

**4.2 USE CASE DIAGRAM**

A use case diagram in the Unified Modelling Language (UML) is a type of behavioural diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

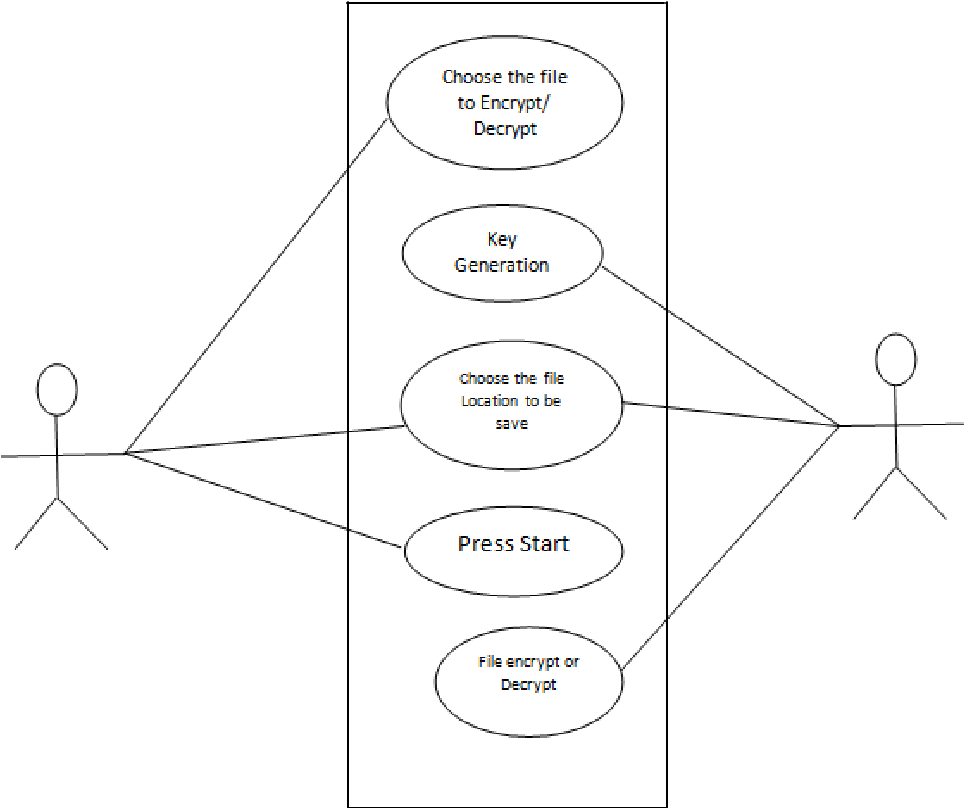


Figure 4.2: USE-CASE Diagram

**4.3 DATA FLOW DIAGRAM**

The DFD is also called as bubble chart. It is a simple graphical format that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system. The data flow diagram (DFD) is one of the most important modelling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

DFD show the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

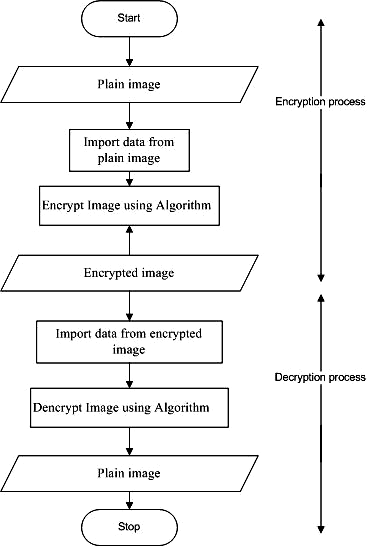


Figure 4.3: Data Flow Diagram for Image Cryptography using Magpie.

**4.4 CLASS DIAGRAM**

In software engineering, a class diagram in the Unified Modelling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system’s classes, their attributes, operations (or methods), and the relationships among objects.

The class diagram is the main building block of object-oriented modelling. It is used for general conceptual modelling of the structure of the application, and for detailed modelling, translating the models into programming code.

Class diagrams can also be used for data modelling. The classes in a class diagram represent both the main elements, interactions in the application, and the classes to be programmed.

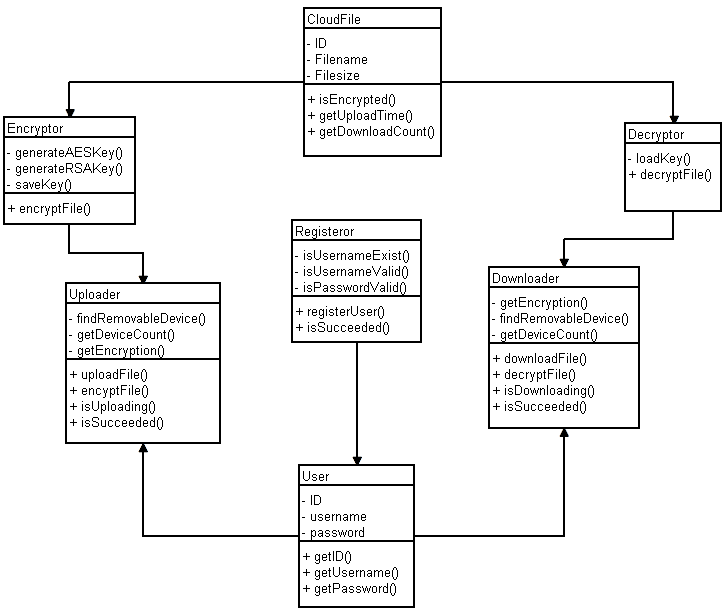


Figure 4.4: Class Diagram

**4.5 SEQUENCE DIAGRAM**

A sequence diagram is a type of interaction diagram because it describes how—and in what order—a group of objects works together.

These diagrams are used by software developers and business professionals to understand requirements for a new system or to document an existing process.

Sequence diagrams are sometimes known as event diagrams or event scenarios. A sequence diagram shows, as parallel vertical lines (lifelines), different processes or objects that live simultaneously, and, as horizontal arrows, the messages exchanged between them, in the order in which they occur.

This allows the specification of simple runtime scenarios in a graphical manner

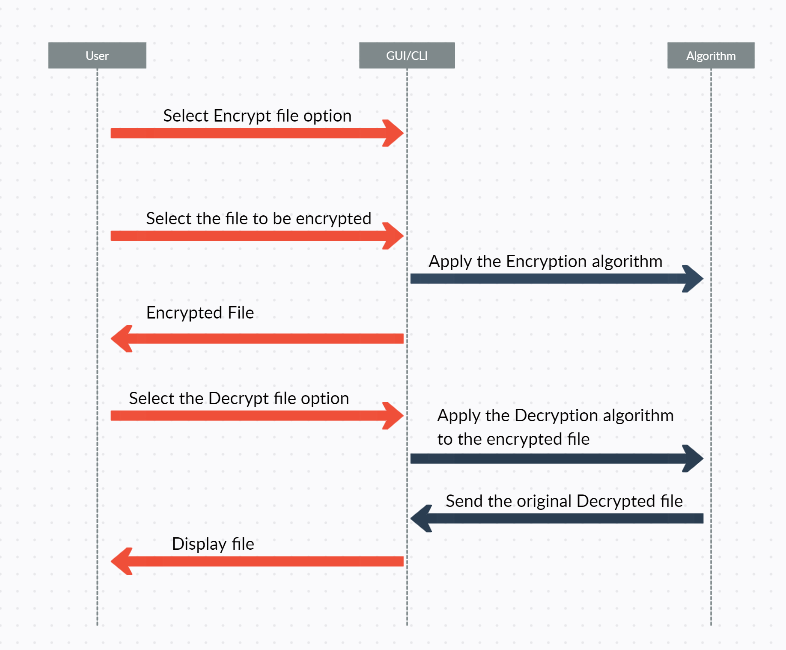


Figure 4.5: Sequence Diagram

**CHAPTER 5**

# PROJECT DESCRIPTION

The Secure Message Encryption and Decryption System is a Python-based application designed to provide robust encryption and decryption functionalities for securing sensitive messages. Leveraging symmetric encryption with the Fernet algorithm from the `cryptography` library, this system ensures the confidentiality and integrity of messages exchanged between parties.

**Key Features:**

**1. Key Management:**

- The system employs a file-based approach for key management, ensuring the security and persistence of encryption keys.

- Upon initialization, the system checks for the presence of a key file in the current directory. If no key file is found, a new key is generated and stored securely.

- Users have the option to manually backup or regenerate keys as needed, enhancing key management flexibility.

**2. Encryption:**

- Users can encrypt messages of arbitrary length using the provided encryption key.

- The encryption process utilizes the Fernet symmetric encryption algorithm, which guarantees strong security while maintaining efficiency.

- Encrypted messages are returned in a format suitable for transmission over insecure channels, ensuring confidentiality during transit.

**3. Decryption:**

- Encrypted messages can be decrypted by authorized parties possessing the appropriate decryption key.

- The system validates the integrity of encrypted messages during decryption, detecting any unauthorized modifications or tampering.

- Robust error handling mechanisms are implemented to handle scenarios such as invalid keys or corrupted ciphertexts, ensuring the reliability of the decryption process.

4. Error Handling and Exception Reporting:

- Custom exceptions, including `KeyNotFoundError`, `InvalidToken`, and `BinasciiError`, are defined to capture and handle specific error conditions gracefully.

- Exception messages provide clear and informative feedback to users, facilitating troubleshooting and resolution of issues encountered during encryption or decryption.

**Usage:**

**1. Encryption Workflow:**

- Users initiate the encryption process by providing the plaintext message and the encryption key.

- The system encrypts the message using the specified key and returns the corresponding ciphertext.

- Encrypted messages can then be securely transmitted or stored, safeguarding sensitive information from unauthorized access.

**2. Decryption Workflow:**

- Authorized recipients obtain encrypted messages and the corresponding decryption key.

- By supplying the encrypted message and the decryption key to the system, users can decrypt the ciphertext and retrieve the original plaintext message.

- Decrypted messages are presented to users in their original form, enabling seamless access to sensitive information while preserving data confidentiality.

**Future Enhancements:**

**1. User Interface Enhancements:**

- Develop a user-friendly command-line interface (CLI) or graphical user interface (GUI) to streamline user interactions and improve usability.

- Integrate features such as key generation, encryption, and decryption into a cohesive and intuitive workflow, enhancing user experience.

**2. Advanced Encryption Techniques:**

- Explore advanced encryption techniques, such as hybrid encryption or authenticated encryption, to enhance security and resilience against emerging threats.

- Investigate the integration of cryptographic protocols like TLS/SSL for secure communication between distributed systems or networked applications.

**3. Cross-Platform Compatibility:**

- Ensure cross-platform compatibility by optimizing the application for deployment on diverse operating systems, including Windows, macOS, and Linux distributions.

- Implement platform-specific optimizations and compatibility checks to ensure consistent behavior across different environments.

**Conclusion:**

The Secure Message Encryption and Decryption System represents a fundamental building block for implementing secure communication and data protection in Python-based applications.

By prioritizing key management, robust encryption algorithms, and error handling mechanisms, the system offers a reliable solution for safeguarding sensitive information against unauthorized access and tampering.

**CHAPTER 6**

# IMPLEMENTATION & RESULT

**6.1 LIBRARIES USED**

1. **cryptography.fernet**: This library provides an implementation of symmetric encryption using the Fernet algorithm. Fernet is a symmetric encryption algorithm that guarantees the integrity and confidentiality of data. It is part of the `cryptography` library, which offers various cryptographic functionalities in Python.

2. **os**: The `os` module provides a way to interact with the operating system. In this script, it's being used to access functionalities related to file handling and directory operations, such as getting the current working directory (`getcwd`) and checking if a file exists (`isfile`).

3. **bin ascii**: The `binascii` module provides functions for converting between binary data and ASCII-encoded hexadecimal representations. In this script, it's specifically importing the `Error` class, which might be used for handling errors related to binary-to-text encoding and decoding.

---These libraries collectively enable the generation, loading, encryption, and decryption of messages using symmetric key cryptography in Python---

1. **tkinter (`import tkinter as tk`):** This library is the standard GUI toolkit for Python. It provides various widgets (such as buttons, labels, text fields, etc.) that can be used to create graphical user interfaces.

2. **ttk (`from tkinter import ttk`)**: The `ttk` module within tkinter provides access to the themed widget set, which includes enhanced versions of the standard tkinter widgets with a more modern and consistent appearance across different platforms.

3. **filedialog (`from tkinter import filedialog`):** The `filedialog` module within tkinter provides dialogs for opening and saving files. It allows users to interactively select files or specify file paths.

---These libraries collectively enable the creation of a GUI application for symmetric encryption and decryption, allowing users to input text, perform encryption or decryption operations, and save/load text to/from files interactively---

1. **symmetric\_encryption:** This appears to be a custom module containing functions for generating keys, loading keys, encrypting messages, and decrypting messages using symmetric encryption. It likely contains the implementations of these functionalities using the Fernet algorithm or similar symmetric encryption techniques.

2. **rich (`from rich import print as rprint`):** The `rich` library is used for adding color and style to console output in Python. It provides enhanced features for formatting text, including colors, styles, and panel layouts, making the CLI output more visually appealing and readable.

3. **rich.panel (`from rich.panel import Panel`):** The `Panel` class from the `rich.panel` module is used to create stylized panels for displaying messages or sections of text. It allows for customizing the border style, background colour, and text alignment of the panel, enhancing the presentation of information in the CLI.

4. **rich.console (`from rich.console import Console`):** The `Console` class from the `rich.console` module provides an interface for interacting with the console and controlling the display of text output. It allows for printing styled text, accepting user input, and managing console-related operations in a rich text environment.

-These libraries collectively enable the creation of a command-line tool for symmetric text encryption and decryption, providing users with an interactive interface for encrypting and decrypting messages securely

**6.2 CODE OF THE PROJECT**

The code of the project comprises of 3 files, symmetric\_encryption.py, CLI.py and GUI.py.  
Here is the Pseudocode for the main logic

symmetric\_encryption.py

Import necessary modules and classes  
 from \_\_future\_\_ import annotations  
 from os import getcwd  
 from os.path import isfile  
 from cryptography.fernet import Fernet  
 from cryptography.fernet import InvalidToken  
 from binascii import Error as BinasciiError  
  
Define KeyNotFoundError class inheriting from FileNotFoundError  
 Initialize with a custom message indicating the key file is not found  
 Override \_\_str\_\_ method to return the custom message  
  
Define generate\_key function  
 Generate a symmetric encryption key using Fernet  
 Save the key to a file named 'key.key'  
 Return the loaded key using load\_key function  
  
Define load\_key function  
 Check if 'key.key' file exists  
 If not, raise KeyNotFoundError with the current directory as argument  
 If KeyNotFoundError is caught, generate a new key using generate\_key function  
 Open 'key.key' file in read-binary mode  
 Read and return the key  
  
Define encrypt\_message function  
 Arguments: message (string), key (bytes)  
 Create a Fernet instance with the provided key  
 Encrypt the message (encoded to bytes) using Fernet instance  
 Return the encrypted message (decoded to string)  
  
Define decrypt\_message function  
 Arguments: encrypted\_message (string), key (bytes)  
 Create a Fernet instance with the provided key  
 Try to decrypt the encrypted message (encoded to bytes) using Fernet instance  
 Catch InvalidToken and return InvalidToken  
 Catch BinasciiError and return BinasciiError  
 Catch any other Exception and return the exception  
 Return the decrypted message (decoded to string)  
  
*# Example usage (commented out in actual code)  
# print(decrypt\_message(encrypt\_message('hi', load\_key()), load\_key()))  
# print(decrypt\_message('', load\_key()))*

./GUI.py

import tkinter as tk  
from tkinter import ttk  
from tkinter import filedialog  
from symmetric\_encryption import generate\_key, load\_key, encrypt\_message, decrypt\_message, InvalidToken, BinasciiError  
  
ICON\_DATA = b''  
  
  
def browse\_files() -> None:  
 *"""Browse for a file and load its content into the top field."""* key\_lable.setvar(key.get())  
 try:  
 filename = filedialog.askopenfilename(initialdir="/", title="Select a File",  
 filetypes=(("Text files", "\*.txt\*"), ("all files", "\*.\*")))  
  
 *# Open and read file* with open(filename, 'r') as file:  
 top\_text\_field.delete('1.0', 'end')  
 top\_text = file.read()  
 top\_text\_field.insert('1.0', top\_text)  
 except FileNotFoundError:  
 return None  
  
  
def save\_file() -> None:  
 *"""Save the text in the bottom field to a file."""* filename = filedialog.asksaveasfilename(initialdir="/", title="Save File",  
 filetypes=(("Text files", "\*.txt\*"), ("all files", "\*.\*")))  
 if filename.partition('.')[0] == '':  
 *# TODO: Handle empty filename* return None  
 if filename.partition('.')[2] != 'txt':  
 *# C:\\users\%USERNAME%\downloaded\_files\test.txt.csv* if filename.partition('.')[2] == '':  
 filename += '.txt'  
 else:  
 filename = filename.partition('.')[0] + '.txt'  
  
 *# Open and write file* with open(filename, 'w') as file:  
 file.write(bottom\_text\_field.get('1.0', 'end-1c'))  
  
  
def convert\_text() -> None:if radio\_bool.get():  
 *# Complete the encrypt function and also the decrypt function* if top\_text\_field.get('1.0', 'end-1c') == '':  
 credits\_label.config(text='Magpie: No text to encrypt', foreground='red')  
 return None  
  
 if key.get() == '':  
 get\_key()  
  
 \_key = key.get()  
 plain\_text = top\_text\_field.get('1.0', 'end-1c')  
 cipher\_text = encrypt\_message(plain\_text, \_key.encode())  
 credits\_label.config(text='Magpie: Encryption successful', foreground='green')  
  
 bottom\_text\_field.config(state='normal') *# Enable editing* bottom\_text\_field.delete('1.0', 'end')  
 bottom\_text\_field.insert('1.0', cipher\_text)  
 bottom\_text\_field.config(state='disabled') *# Disable editing* else:  
 \_key = key.get()  
 cipher\_text = top\_text\_field.get('1.0', 'end-1c')  
  
 *# Extract the decrypted message from the result based on its type* plain\_text = decrypt\_message(cipher\_text, \_key.encode())  
  
 *# Handle the decrypted message based on its type  
 # Check the type of the decrypted message* if isinstance(plain\_text, str):  
 *# Insert the decrypted message as a string* bottom\_text\_field.config(state='normal') *# Enable editing* bottom\_text\_field.delete('1.0', 'end')  
 bottom\_text\_field.insert('1.0', plain\_text)  
 bottom\_text\_field.config(state='disabled') *# Disable editing* credits\_label.config(text='Magpie: Decryption successful', foreground='green')  
 elif isinstance(plain\_text, InvalidToken):  
 credits\_label.config(text='Magpie: Invalid Token error occurred', foreground='red')  
 elif isinstance(plain\_text, Exception):  
 credits\_label.config(text='Magpie: Exception occurred during decryption', foreground='red')  
 elif isinstance(plain\_text, BinasciiError):  
 credits\_label.config(text='Magpie: Binascii Error occurred', foreground='red')  
 else:  
 credits\_label.config(text='Magpie: Unknown error occurred. Please enter correct Cipher text.',  
 foreground='red')  
  
  
def new\_key() -> None:  
 key.set(generate\_key().decode())  
 key\_lable\_text.set('Using KEY: ' + key.get() + " (Generated)")  
 return None  
  
  
def clear\_key() -> None:  
 key.set('')def get\_key() -> None:  
 key.set(load\_key().decode())  
 if radio\_bool.get():  
 key\_lable\_text.set('Using KEY: ' + key.get() + " (Loaded)")  
 return None  
  
  
*# app*app = tk.Tk()  
app.title("Magpie")  
app.iconbitmap(r'./magpie\_32.ico')  
*# app.geometry("300x150") # for 730p 'ish screens*app.geometry('685x500')  
app.minsize(width=685, height=500)  
  
*# VARIABLES*key = tk.StringVar()  
radio\_bool = tk.BooleanVar(value=True)  
key\_lable\_text: tk.StringVar = tk.StringVar(  
 value='Using KEY: ' + key.get() + " (Not yet loaded. Will be loaded on conversion.)")  
  
*# label*greeting\_label = ttk.Label(app, text="Welcome to")  
greeting\_label.pack()  
  
*# title*title\_label = ttk.Label(app, text='TEXT Encrypter', font='calibre 24 bold')  
title\_label.pack(side='top')  
  
input\_lable = ttk.Label(app, text="Enter your text:")  
input\_lable.pack(side='top', fill='x', padx=(10, 0))  
  
*# top entry field*top\_text\_field = tk.Text(app, width=50, height=5, background='light blue', wrap='word', maxundo=15, undo=True, )  
top\_text\_field.pack(side='top', expand=True, fill='both', padx=10, pady=5)  
top\_text\_field.focus()  
  
*# key Frame*key\_frame = ttk.Frame(app)  
  
key\_lable = ttk.Label(key\_frame, textvariable=key\_lable\_text, font='courier 8 bold')  
key\_lable.pack(side='left', padx=(10, 0), pady=0)  
  
key\_entry = ttk.Entry(key\_frame, show=u"\u25CF", width=30, textvariable=key, foreground='black')  
key\_entry.configure(validate='key', validatecommand=(key\_entry.register(lambda text: len(text) <= 44), "%P"))key\_load\_button: object = ttk.Button(key\_frame, text='Load Key', command=get\_key, state='normal')  
key\_load\_button.pack(side='right', padx=10)  
  
key\_clear\_button: object = ttk.Button(key\_frame, text='Generate Key', command=new\_key, state='normal')  
key\_clear\_button.pack(side='right', padx=10)  
  
key\_frame.pack(pady=10, side='top', fill='x', anchor='center')  
  
*# Options Frame*options\_frame = ttk.Frame(app, relief=tk.GROOVE, padding=(10, 5))  
  
*# Radio button field*radio\_frame = ttk.Frame(options\_frame, relief=tk.GROOVE, padding=10)  
  
  
def radio\_func():  
 if radio\_bool.get():  
 get\_key()  
 key\_entry.pack\_forget()  
 key\_clear\_button.configure(state='normal', text='Generate Key', command=new\_key)  
  
 else:  
 key\_lable\_text.set('Enter your KEY:')  
 key\_entry.pack(side='left', fill="x", expand=True, padx=10)  
 key.set('')  
 key\_clear\_button.configure(text='Clear Key', command=clear\_key)  
  
  
*# options*encrypt\_radio = (ttk.Radiobutton(radio\_frame,  
 text='Encrypt',  
 value=True,  
 command=radio\_func,  
 variable=radio\_bool)  
 .pack(side='left', fill='y', padx=20))  
  
decrypt\_radio = (ttk.Radiobutton(radio\_frame,  
 text='Decrypt',  
 value=False,  
 command=radio\_func,  
 variable=radio\_bool)  
 .pack(side='left', fill='y', padx=20))  
  
radio\_frame.pack(side='left') *# convert button*convert\_button = ttk.Button(options\_frame, text='Convert', command=convert\_text)  
convert\_button.pack(side='left', padx=(10, 10))  
  
options\_frame.pack(side='top', pady=10)  
  
file\_frame = ttk.Frame(options\_frame, relief=tk.GROOVE, padding=5)  
  
open\_file\_button = (ttk.Button(file\_frame, text='Open File', command=browse\_files).  
 pack(side="top", pady=5))  
save\_file\_button = (ttk.Button(file\_frame, text='Save Text', command=save\_file).  
 pack(side="top", pady=5))  
  
file\_frame.pack(expand=True, fill='x', pady=10, side='right')  
  
output\_lable = (ttk.Label(app, text="Your Output:").  
 pack(side='top', fill='x', padx=(10, 0)))  
*# Output field  
  
# bottom entry field*bottom\_text\_field = tk.Text(app, width=50, height=5, background='light yellow', wrap='word')  
bottom\_text\_field.pack(side='top', expand=True, fill='both', padx=10, pady=5)  
  
credits\_label = ttk.Label(app, text="Made by: Magpie", font='calibre 10 bold')  
credits\_label.pack(side='bottom', pady=10)  
  
*# Start the main event loop*app.mainloop()

**6.3 RESULT / OUTPUT SCREENS**

**To encrypt-decrypt test files using the GUI tool**

1. Run the Magpie installer to install the necessary dependencies.
2. Click the Open File button to choose a text file.
3. Enter the key in the corresponding field.
4. Choose one of the following options:
   * Encrypt a message: Select the Encrypt button.
   * Decrypt a message: Select the Decrypt button.
   * Exit the tool: Click the X button.
5. Click on the Convert button to start the encryption or decryption process.
6. Save the encrypted or decrypted text file to the desired location.
7. Follow the prompts to enter the necessary information for encryption or decryption.

**OUTPUT:**

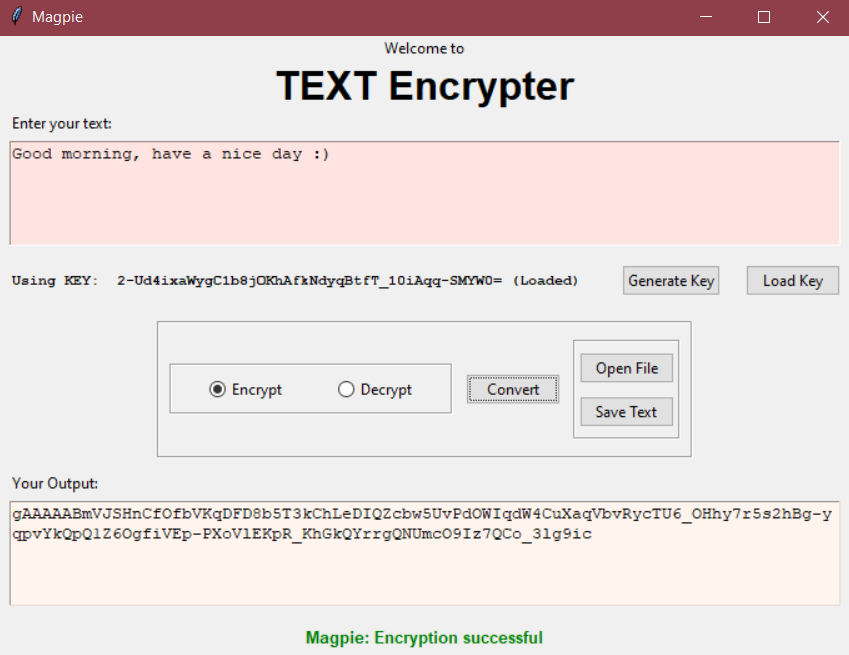


Figure 6.2.1: Plain Text to Cipher text (Encryption)

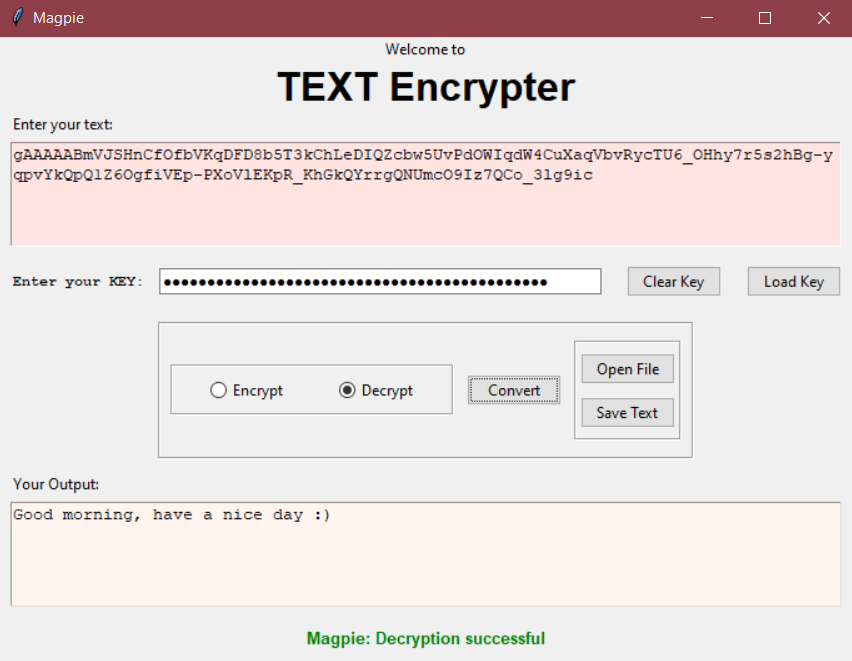


Figure 6.2.2: Cipher text to Plain text (Decryption)

**To encrypt-decrypt test files using the CLI tool**

1. Run the script symmetric\_encryption.py to import the necessary functions.
2. Execute the main script text\_encryption.py to start the tool.
3. Choose one of the following options:
   * Encrypt a message: Enter 1, e, or E.
   * Decrypt a message: Enter 2, d, or D.
   * Exit the tool: Enter 3, break, b, B, exit, or Exit.
4. Follow the prompts to enter the necessary information for encryption or decryption.
5. The tool will display the encrypted or decrypted message based on the chosen option.

**OUTPUT:**

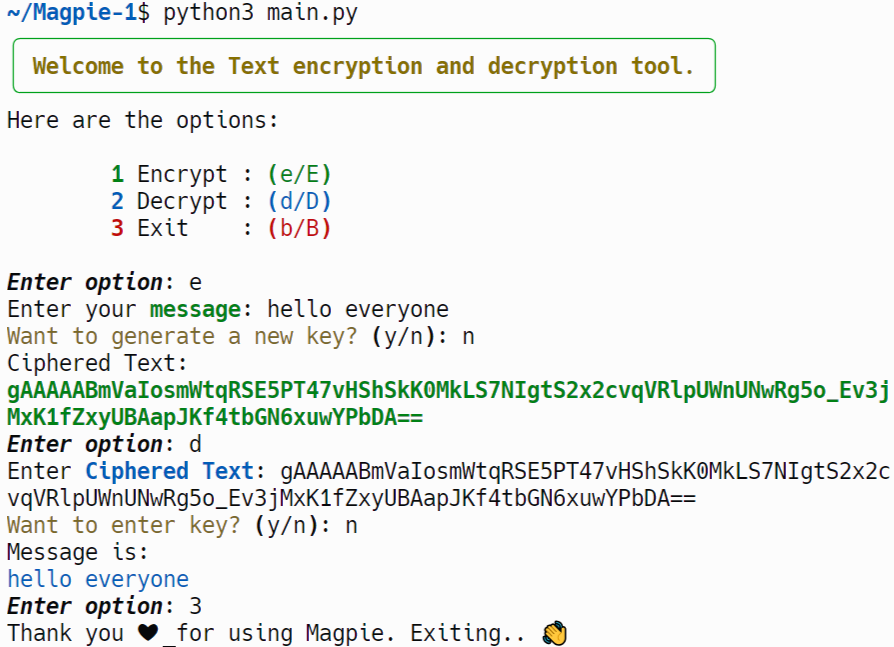


Figure 6.2.3: Encryption and Decryption using CLI

**CHAPTER 7**

# TESTING

**7.1 TESTING STRATEGIES**

The purpose of testing is to discover errors. Testing is the process of trying to discover very conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

**White Box Testing**

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

**Black Box Testing**

Black Box Testing is testing the software without any knowledge of the inner Workings, structure or language of the module being tested.

Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document.

It is a testing in which the software under test is treated, as a black box. You cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

**7.2 TYPES OF TESTING**

**Unit testing**

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated.

**Integration testing**

Integration tests are designed to test integrated software components to determine if they run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of.

**Functional Testing**

Functional tests provide systematic demonstrations functions tested are available as that specified by the business and technical requirements, system documentation, and user manuals. Functional testing is centered on the following items:

**Valid Input:** identified classes of valid input must be accepted.

**Invalid Input:** identified classes of invalid input must be rejected.

**Functions:** identified functions must be exercised.

**Output:** identified classes of application outputs must be exercised.

**Systems / Procedures:** interfacing systems or procedures must be invoked.

**Performance Testing**

Assess the system's performance under various conditions, including processing speed, resource utilization, and scalability to handle varying workloads.

**Robustness Testing**

Test the system's resilience to input variations, such as changes in lighting conditions, different writing instruments, and alterations in signature styles.

**Usability Testing**

Evaluate the user interface and user experience to ensure that the forgery detection system is user-friendly and accessible for its intended users.

**Security Testing**

Verify the system's resistance to adversarial attacks and attempts to manipulate the forgery detection process, ensuring the security of sensitive signature data.

**Cross-browser and Cross-platform Testing**

Confirm that the forgery detection system works consistently across different web browsers and platforms, ensuring a broad user reach.

**Scalability Testing**

Assess the system's ability to handle an increasing volume of signatures and users, ensuring it can scale effectively without compromising performance.

**Regression Testing**

Perform tests after each system update or modification to ensure that new changes do not negatively impact existing functionality.

**Accuracy Testing**

Validate the accuracy of the forgery detection system by comparing its results against a trusted benchmark, possibly using a curated dataset with known genuine and forged signatures.

**User Acceptance Testing (UAT)**

Involve end-users in the testing process to gather feedback on the system's usability, functionality, and overall performance.

**Documentation Testing**

Verify that documentation, including user manuals and system guides, accurately reflects the system's features and provides comprehensive instructions.

**Continuous Testing**

Implement automated testing processes to ensure continuous monitoring and rapid detection of issues during the development life cycle.

**Ethical Considerations Testing**

Assess the forgery detection system for potential biases and ethical concerns, ensuring fairness and equity in its application.

**7.3 TEST CASES**

**Writing Test Case**

**Test Case 1: Empty Message**  
Description: Test the behaviour when an empty message is encrypted and decrypted.

Test Steps:

* Encrypt an empty message.
* Decrypt the encrypted empty message.
* Verify if the decrypted message is also empty.

**Test Case 2: Large Message**  
Description: Test the behaviour when a large message is encrypted and decrypted.  
Test Steps:

* Encrypt a large message (larger than the block size).
* Decrypt the encrypted large message.
* Verify if the decrypted large message matches the original large message.

**Test Case 3: Binary Message**  
Description: Test the behaviour when a binary message is encrypted and decrypted.  
Test Steps:

* Encrypt a binary message.
* Decrypt the encrypted binary message.
* Verify if the decrypted binary message matches the original binary message.

**Test Case 4: Encrypt and Decrypt a Message**  
Description: Encrypt a message, then decrypt it and verify if the decrypted message matches the original message.  
Test Steps:

* Encrypt a sample message using the encrypt\_message function.
* Decrypt the encrypted message using the decrypt\_message function.
* Verify if the decrypted message matches the original message.

**Test Case 5: Key File Not Found**  
Description: Test the behaviour when the key file is not found.  
Test Steps:

* Remove the key.key file from the directory.
* Attempt to encrypt or decrypt a message.
* Verify if the function generates a new key file and performs the encryption or decryption.

**Test Case 6: Invalid Key**  
Description: Test the behaviour when an invalid key is provided for decryption.  
Test Steps:

* Encrypt a sample message.
* Attempt to decrypt the encrypted message using an invalid key.
* Verify if the function raises an InvalidToken exception.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S. No. | Input | Option | Output | Result |
| 1 | Test 1 | Encrypt | gAAAAABmuQxyvffg26es3W  gaYIVDQl\_ViCTLmDSbwxY\_mri6i4-2EOczqHE2QQGLq3HJRvn3  qZsp24Ofz2sC8vsLr5LCEN6uRg== | Passed |
| 2 | gAAAAABmuQxyvffg26es3WgaYIVDQl\_V  iCTLmDSbwxY\_mri6i4-2EOczqHE2QQGLq3HJRvn3qZsp24  Ofz2sC8vsLr5LCEN6uRg== | Decrypt | Test 1 | Passed |
| 3 | Test 2 | Decrypt | Unknown Error | Passed |

Table 7.3: Test cases

**CHAPTER 8**

# SYSTEM RESULTS

**8.1 OUTCOMES OF THE PROPOSED SYSTEM**

Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases test strategy and approach. Field testing will be performed manually, and functional tests will be written in detail.

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects. The task of the integration test is to check that components or software applications, example: components in a software system or one step up software applications at the company level interact without error.

Test Results All the test cases mentioned above passed successfully. No defects encountered. User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements. Test Results: All the test cases mentioned above passed successfully. No defects encountered.

**8.2 SCREENSHOTS**

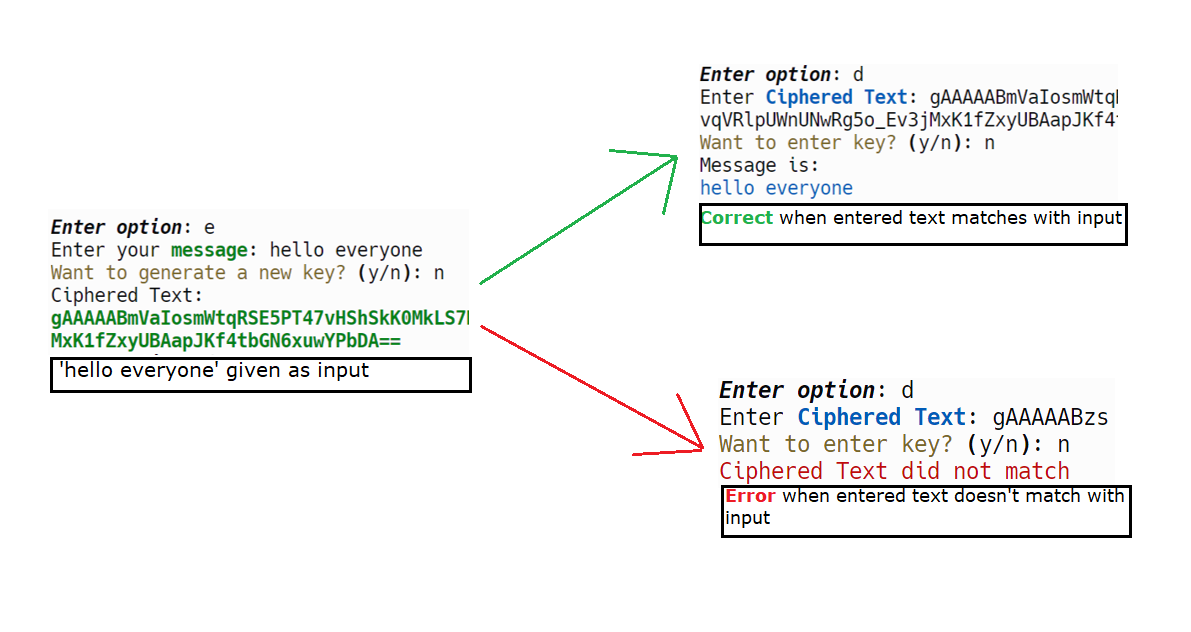


Figure 8.1: final result

**CHAPTER 9**

# CONCLUSION AND FUTURE SCOPE

**9.1 CONCLUSION**

The encryption and decryption mechanism encapsulated within the provided code represents a cornerstone of modern data security practices. By leveraging symmetric encryption, wherein the same key is used for both encryption and decryption, the mechanism ensures a streamlined and efficient approach to securing sensitive information. The Fernet module, a part of the widely-used cryptography library, serves as the backbone of this mechanism, offering a robust and battle-tested encryption algorithm. Encryption, the process of transforming plaintext into ciphertext, safeguards data against unauthorized access during transmission or storage. This is accomplished through the encrypt message function, which accepts a plaintext message and an encryption key, facilitating the conversion of the message into an encrypted format. Conversely, decryption, the reverse process of encryption, is facilitated by the decrypt message function. Here, the encrypted message is decrypted using the same encryption key, ensuring the recovery of the original plaintext. The mechanism further prioritizes resilience through meticulous error handling, ensuring that potential decryption errors, such as invalid tokens or formatting inconsistencies, are promptly addressed. The generate key function generates a new encryption key and persists it in a file, while the load key function ensures consistent access to the encryption key for subsequent encryption and decryption operations. This comprehensive approach to encryption and decryption not only safeguards data against unauthorized access but also helps in gaining confidence in the security and reliability of sensitive information across diverse applications and environments.

**9.2 FUTURE SCOPE**

The encryption and decryption mechanism presented in the provided code already offers a solid foundation for securing sensitive data. However, there are several avenues for future enhancement and expansion:

**Multi-factor Authentication:** Enhancing the encryption mechanism to support multi-factor authentication can add an extra layer of security. This could involve incorporating token-based authentication, or other factors beyond traditional passwords.  
**Image-Encryption:** Encrypting images by making a mediator for conversion image files to byte code and vice versa. For more security SHA-512 is implemented.

**CHAPTER 10**

# REFERENCES

## symmetric\_encryption.py

1. **Cryptography Library:**
   * *Cryptography*: A package designed to expose cryptographic recipes and primitives to Python developers. It includes both high-level recipes and low-level interfaces to common cryptographic algorithms such as symmetric ciphers, message digests, and key derivation functions.
     + Cryptography. (n.d.). Retrieved from <https://cryptography.io/>
2. **Python Standard Library:**
   * *os Module*: This module provides a way of using operating system-dependent functionality like reading or writing to the file system.
     + Python Software Foundation. (n.d.). os — Miscellaneous operating system interfaces. In *Python 3 Documentation*. Retrieved from <https://docs.python.org/3/library/os.html>
   * *os.path Module*: This module implements some useful functions on pathnames.
     + Python Software Foundation. (n.d.). os.path — Common pathname manipulations. In *Python 3 Documentation*. Retrieved from <https://docs.python.org/3/library/os.path.html>
   * *binascii Module*: This module contains a number of methods to convert between binary and various ASCII-encoded binary representations.
     + Python Software Foundation. (n.d.). binascii — Convert between binary and ASCII. In *Python 3 Documentation*. Retrieved from <https://docs.python.org/3/library/binascii.html>
3. **PEP 484 – Type Hints:**
   * *Type Annotations*: Python's type annotations enable optional type checking via static type checkers, which can find type errors before the code runs.
     + van Rossum, G., & Lehtosalo, J. (2014). PEP 484 – Type Hints. Python Enhancement Proposals. Retrieved from <https://peps.python.org/pep-0484/>

Here are the references for the two Python scripts:

## CLI.py

1. **Rich Library Documentation**: The Rich library is used for creating attractive command-line interfaces. The print function from rich and the Panel, Console classes are utilized for displaying text in various styles. You can refer to the official documentation for more details:
   * [Rich Documentation](https://rich.readthedocs.io/en/stable/)
2. **Python Match Statement**: The match statement in Python, introduced in version 3.10, is used for pattern matching. It helps in selecting code blocks to execute based on the structure of the input. Official documentation is available at:
   * [Python Pattern Matching](https://docs.python.org/3/whatsnew/3.10.html#pattern-matching)
3. **Python File I/O**: The script utilizes basic Python file I/O operations to load and save keys and messages. This includes opening, reading, and writing files. Documentation can be found here:
   * [Python File I/O](https://docs.python.org/3/tutorial/inputoutput.html#reading-and-writing-files)

## GUI.py

1. **Tkinter Library Documentation**: Tkinter is the standard Python interface to the Tk GUI toolkit. It is used extensively in this script for creating the GUI elements like buttons, labels, text fields, etc. The documentation provides a comprehensive guide to the various components:
   * [Tkinter Documentation](https://docs.python.org/3/library/tkinter.html)
2. **Tkinter filedialog Module**: The filedialog module is part of Tkinter and is used to open and save files through a file dialog box in the GUI. The official reference is available at:
   * [Tkinter filedialog](https://docs.python.org/3/library/tkinter.filedialog.html)
3. **Python StringVar and BooleanVar**: The script uses StringVar and BooleanVar from Tkinter to manage the state of variables that are tied to widgets in the GUI. These are commonly used for managing user input and control states. Documentation is here:
   * [StringVar and BooleanVar](https://effbot.org/tkinterbook/variable.htm)
4. **Base64 Encoding**: The script checks the length of keys and utilizes Base64 encoding for secure message encryption. Python's base64 module handles this encoding:
   * [Base64 Encoding in Python](https://docs.python.org/3/library/base64.html)