IMAGE ENCRYPTION USING AES ALGORITHM

Project report submitted in partial fulfilment of the requirement for the degree of Bachelor of Technology

in

Computer Science and Engineering/Information Technology

By

Rishabh Singh Parmar(191221)

Sahaj Mankotia(191231)

Under the supervision of Dr. Pankaj Dhiman

to

Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology
Waknaghat, Solan-173234, Himachal Pradesh

Candidate's Declaration

I hereby declare that the work presented in this report entitled **"Image Encryption Using AES"** in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering/Information Technology** submitted in the department of Computer Science & Engineering and Information Technology**,** Jaypee University of Information Technology Waknaghat is an authentic record of my own work carried out over a period from January 2023 to May 2023 under the supervision of **Dr. Pankaj Dhiman, Assistant Professor (SG) of department Computer Science & Engineering and Information Technology.** I also authenticate that I have carried out the above-mentioned project work under the proficiency stream **Information Security.**
The matter embodied in the report has not been submitted for the award of any other degree or diploma.

Rishabh Singh Parmar (191221)

Sahaj Mankotia (191231)

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

Dr. Pankaj Dhiman

Assistant Professor (SG)

Computer Science & Engineering and Information Technology

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

PLAGIARISM VERIFICATION REPORT

Date: ....

Type of Document (Tick): PhD Thesis | M.Tech Dissertation/ Report | B.Tech Project Report | Paper

Name: ____________________________ __Department: _________________ Enrolment No _________

Contact No. _______________________________E-mail. _______________________________________

Name of the Supervisor: ____

Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters): _________________________

____

____

UNDERTAKING

I undertake that I am aware of the plagiarism related norms/ regulations, if I found guilty of any plagiarism and copyright violations in the above thesis/report even after award of degree, the University reserves the rights to withdraw/revoke my degree/report. Kindly allow me to avail Plagiarism verification report for the document mentioned above.

Complete Thesis/Report Pages Detail:

– Total No. of Pages =

– Total No. of Preliminary pages =

– Total No. of pages accommodate bibliography/references =

(Signature of Student)

FOR DEPARTMENT USE

We have checked the thesis/report as per norms and found **Similarity Index** at ....(%). Therefore, we are forwarding the complete thesis/report for final plagiarism check. The plagiarism verification report may be handed over to the candidate.

(Signature of Guide/Supervisor) **Signature of HOD**

FOR LRC USE

The above document was scanned for plagiarism check. The outcome of the same is reported below:

Copy Received on	**Excluded**	**Similarity Index (%)**	**Generated Plagiarism Report Details** (Title, Abstract & Chapters)	
	• All Preliminary Pages • Bibliography/Images/Quotes • 14 Words String		Word Counts	
Report Generated on			Character Counts	
		Submission ID	Total Pages Scanned	
			File Size	

Checked by
Name & Signature **Librarian**

....

Please send your complete thesis/report in (PDF) with Title Page, Abstract and Chapters in (Word File) through the supervisor at plagcheck.juit@gmail.com

ACKNOWLEDGEMENT

Firstly, we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the project work successfully.

We are really grateful and wish our profound indebtedness to Supervisor Dr. Pankaj Dhiman, Assistant Professor (SG), Department of Computer Science & Engineering and Information Technology., Jaypee University of Information Technology, Wakhnaghat. Deep Knowledge & keen interest of our supervisor in the field of "Information Security" to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stages have made it possible to complete this project.

We would like to express our heartiest gratitude to Dr. Pankaj Dhiman, Department of Computer Science & Engineering and Information Technology, for his kind help to finish our project.

We would also generously welcome each one of those individuals who have helped me straight forwardly or in a roundabout way in making this project a win. In this unique situation, I might want to thank the various staff individuals, both educating and non- instructing, which have developed their convenient help and facilitated our undertaking.

Finally, I must acknowledge with due respect the constant support and patience of our parents.

Rishabh Singh Parmar (191221)

Sahaj Mankotia (191231)

Table of Contents

List of Abbreviations

Abbreviations	Full form
AES	Advanced Encryption Standard
GUI	Graphical User Interface
DES	Data Encryption Standard
SP	Substitution – Permutation
SSD	Solid State Drive
VPN	Virtual Private Network

List of Figures

List of Graphs

ASTRACT

The symmetric encryption technique that is presently more widely used and understood is called Advanced Encryption Standard (AES). It can be detected at least six times faster than triple DES.

A successor was needed since DES's key size was insufficient. It was believed that as processing power rose, it would be susceptible to a thorough key search attack. Triple DES was developed to solve this problem, however it was found to be slow.This project employs a method that first encrypts an image with AES before re-encrypting the image.

The user is prompted for an alphanumeric key once the picture has been processed and encrypted as a file in binary format. Using the SHA256 hashing technique improves the security of verification tests used to represent secret information. The process starts by using data to generate a hash function, which is then applied to the hash string generated to represent the encrypted key. The generated AES cypher is then used to encrypt the picture and hash string. Thanks to the AES cypher's built-in Cypher Feedback mode of operation, the block encryptor may be employed as a stream cypher.

Chapter 1

1.1 Introduction

1.1.1 CRYPTOGRAPHY

Cryptography or cryptology is the study of and use of techniques for encrypted communication in the setting of adversarial behavior. Cryptography is more commonly used to describe the development and analysis of techniques that prevent the general population or other individuals from receiving private messages. Data confidentiality, accuracy of data, and authentication are given top priority in contemporary cryptography. Modern cryptography has connections to the disciplines of mathematics, computer science, electrical engineering, communication science, and physics.

Cryptography is utilised in several sectors, including the military, digital currencies, chip-based payment cards, and electronic commerce.

1.1.2 ENCRYPTION

Encryption can be used to scramble data so that only approved parties can decipher it. The process of converting plaintext—text that can be read by humans—into ciphertext—text that cannot be read by humans—is known technically as encryption. To put it simply, encryption modifies readable data to appear random. Encryption requires a cryptographic key, which is a set of integers that both the sender and the recipient of a message may agree upon. Intricate keys are necessary for encryption's true security. Although encrypted data appears random, encryption really operates in a logical, predictable fashion, allowing anybody with the right key to decode encrypted data and return it to plaintext.

1.1.2.1 Types of encryption

- Symmetric encryption employs a single key that is utilised for both encryption and decryption by all communication participants.
- Asymmetric encryption, sometimes referred to as public key encryption, employs two keys, one for encryption and the other for decryption. The word "public key" refers to the encryption key, which is made available to everyone, whereas the term "private key" refers to the decryption key, which must be kept private.

1.1.2.2 Symmetric Encryption Method

Symmetric encryption is a kind of cryptography that utilises just one key for both the encryption and decoding of electronic data. The key must be shared among the parties communicating using symmetric encryption in order to be used in the decryption process. Asymmetric encryption, which encodes and decodes information with two sets of keys—one open and one private—is different from this encryption method.

By using symmetric encryption techniques, data is converted into a format that cannot be comprehended by anybody without the secret key to decode it. After the message has been sent to the intended recipient who also possesses the key, the algorithm reverses its course and restores the message to its prior, understandable condition.

There are two types of symmetric encryption techniques:

- Block algorithms: Specific bit lengths in blocks of digital data are jumbled with the use of a special secret key.
- Data is protected as it streams rather than being saved in the system's memory using stream algorithms, and the system stores the encrypted data within its internal storage while waiting for whole blocks.

1.1.3 DECRYPTION

The phrase for the reverse of encryption is decryption. Cypher Text is transformed into Plain Text in this process. A decryption technique must be applied at the receiving end for cryptography to be able to reconstruct the original message from a non-readable message (Cypher Text).

Decryption uses the same technique as encryption, which is reverse conversion. An identical key is needed to decrypt data and decrypt it again to get the data back to how it was originally.

A key component of decryption is the system's extraction and transformation of the disorganised data into verbal and visual representations that are simple for the reader and the system to grasp. Both manual and automated decryption techniques are available.

1.1.4 AES INTRODUCTION

Image security is crucial in today's systems for image communication. Keep unauthorised users away from sensitive picture data. Unauthorised users are difficult to locate and recognise. Different approaches have been put forth by numerous academics to secure the transmission of photographs. Today, nearly all digital services, including internet communication, imaging systems for the military and healthcare, and multimedia systems, require adequate security for the transmission and storage of digital pictures.

Due to the growing use of multimedia technologies, the internet, and cellphones, image encryption solutions are needed to safeguard photographs from such attacks. In this system, we use AES (Advanced Encryption Technique) to encrypt photos. Such encryption techniques help thwart intrusion attempts.

Use 128-, 192-, and 256-digit keys to decrypt these special blocks. These blocks are first encoded, and then the ciphertext is created by concatenating them. It is built on an SP organisation or backup level organisation.

A 128-bit key has 192 components and 10 cycles.14 iterations using a 256-bit key.

AES encryption scrambles [1] plain text data into a sort of cypher code that is unreadable to both authorised and third parties, even if someone succeeds in deciphering the cypher code before the knowledge reaches its intended destination. The data is decoded and returned to its original, understandable form by the recipient using a secret code.

As a consequence, owing to the AES safe encryption and decryption capabilities [2], sensitive information may be transmitted over the Internet over secure SSL channels without worrying about being intercepted by an outsider or hacker. Sharing such information is exemplified by the quickly expanding usage of utilising cellphones for financial transactions. Only the user will be able to see the information because it will be encrypted.

The AES algorithm is extremely user-friendly and cost-effective. It is also unaffected by any copyright problems. As a result, it may be used globally by any person or company.

The AES algorithm [3] is easy to incorporate into both software and hardware systems. It is quite flexible.

Virtual private networks (VPNs) that are implemented in switches for LAN and WAN networks also employ AES encryption. The Internet Protocol (IP) address is sent to a secure server at the opposite end of the network to do this. This works nicely for networks running open-source software.

The 256-bit Advanced Encryption Standard (AES) [4] approach is recommended by national security agencies in many countries, including India, for storing and transmitting sensitive data over secure communication channels. The finance ministry, along with the military and other sectors of the government, regularly store data using 256-bit AES encryption.

The employment of the AES algorithm in conjunction with other cryptographic-based techniques [5] increases the effectiveness of the encryption process, which is used to transform private and sensitive data into encrypted form and share it.

1.1.4.1 Features of AES -

- SP Organisation: As a result of the DES computation [6], it provides an SP community shape rather than a Feistel discern form.
- Key Expansion: It starts with a single key in the first stage and eventually expands to several keys used in individual rounds.
- Byte Information: The AES encryption computation uses byte information rather than cycle information. The 128-bit block length is therefore treated as sixteen bytes at some point in the encryption process.
- Key Length: The number of rounds to be completed depends on how long the key will be used to scramble the data. [7] 192-piece key length has 12 rounds, the 128-digit key length has 10 adjustments, and
- 128/192/256-bit keys and 128-bit data.
- Symmetric key, symmetric block cypher.
- More powerful and quicker than Triple-DES.

The following criteria were also taken into consideration when deciding on the next AES algorithm:

- Security: Algorithms have to exhibit greater levels of attack resistance than previously submitted cyphers in order to compete.
- The competition's most important factor was going to be security strength.
- The computational and memory efficiency of the proposed methods was to be evaluated, and the release was meant to be open, non-exclusive, and without any licensing costs.
- Implementation: The method's adaptability, suitability for implementation in hardware or software, and overall simplicity required to be taken into consideration.

1.2 Problem Statement

The working capability of modern technologies, including laptops, personal computers, and several other supplementary devices for correspondence and data transfer, is constantly rising. As a result, the consumers' reach has increased. Along with these clients, a rising number of unauthorised customers are also making inappropriate attempts to obtain information. The issue of data security is raised here. Various sources provide photographs over a shaky channel, some image data contains confidential information, and some images themselves are extremely secret and must be stolen by attackers. We frequently misuse the AES equation to encode and decode photos in order to address this issue.

Unauthorised clients cannot understand this encrypted data [8]. At the least ideal outcome, AES can be used to decode the encrypted data that is often transmitted over the network. The secure transmission of the picture is then ensured.

In contemporary hardware and software, AES is a widely used and supported encryption technique. AES is not now the target of any successful cryptanalytic attacks. Additionally, AES contains built-in flexibility for key lengths, which acts as some degree of "futureproofing" against improvements in the efficiency of doing exhaustive key searches.

1.2.1 Reasons for data encryption

- Privacy: Only the intended recipient or the authorised data owner will be able to access messages or data that is at rest thanks to encryption. Due to this, it is challenging for governments, ad networks, Web service providers, and hackers to intercept and read sensitive data.

- Security: Encryption aids in preventing data breaches whether the data is in motion or at rest. In the event that the hard drive has been correctly encrypted, the information on a lost or stolen computer will still be secured. Similar to this, encrypted communications enable private information to be transmitted between parties without being seen.
- Data integrity: On-path attacks and other undesirable behaviors can be curbed using encryption. Data being transmitted over the Internet cannot be changed route to the recipient thanks to encryption and other integrity measures.
- Authentication Public key encryption, among other things, can be used to demonstrate that a website's owner is the person listed as the owner of the private key in the website's TLS certificate. Visitors to websites can be certain that they are connected to a trustworthy website thanks to this.
- Regulations: Due to all of these reasons, firms managing user data are required by several industry and governmental rules to maintain encryption. A few regulatory and compliance needs, like HIP, demand encryption.

1.2 OBJECTIVES

AES OBJECTIVES -

- AES can be used to protect against intrusion attempts and unauthorised access. This uses different-length cryptographic process keys.
- This security protocol is the most trustworthy since it is used in both hardware and software.
- The AES encryption technique uses greater key sizes, including 128, 192, and 256 bits, making it more secure against hackers.
- It is among the commercial and open-source solutions that is most widely used globally. It is the most widely used security protocol and is used for a wide range of applications, such as payments, e-commerce, encrypted data storage, etc.
- No one can hack into your personal information.
- It takes around 2128 attempts to break a 128-bit encryption. Because of this, it is exceedingly difficult to attack, making it a very safe protocol.

  This project's goal is to provide a safe method of sending and receiving photos. Before sending an image across a network, it should be encrypted, and it should be appropriately decoded on the receiving end.

PROJECT OBJECTIVES -

- Secure picture transmission over a network, such as the internet.
- Assure no changes are performed when sending over the network.
- Encrypt an image to an unreadable format.
- Decrypt an encrypted image to the original image.

1.4 METHODOLOGY

Each cypher encrypts and decrypts data stored in blocks of 128 bits using a special cryptographic key that consists of 128, 192, or 256 bits[10].

The same key is used for encoding and decoding figures. Both sender and recipient must be aware of and use a same secret key.

Keys of 192 or 256 digits are necessary for extremely sensitive information.

A round is made up of a few handling procedures, such as substituting, rendering, and blending the plaintext of the data into the final form of cypher text.

Since a block has a size of 16 bytes, the data from a single block is included in a 4x4 frame, with one byte of information in each cell.

Essentially, the first key is expanded to (n+1) keys, where an is the number of rounds to use in the encryption cycle. For a 128- digit key, the number of turns is 16 and the number of keys to craft is 10+1, 11 keys.

Each Round has 4 steps -

1. Sub Bytes
2. Shift Rows
3. Mix Column
4. Add Round Key

For each block, the cited progressions are applied sequentially. Each block is successfully encrypted before being combined to form the final ciphertext. The following are the means [12]:

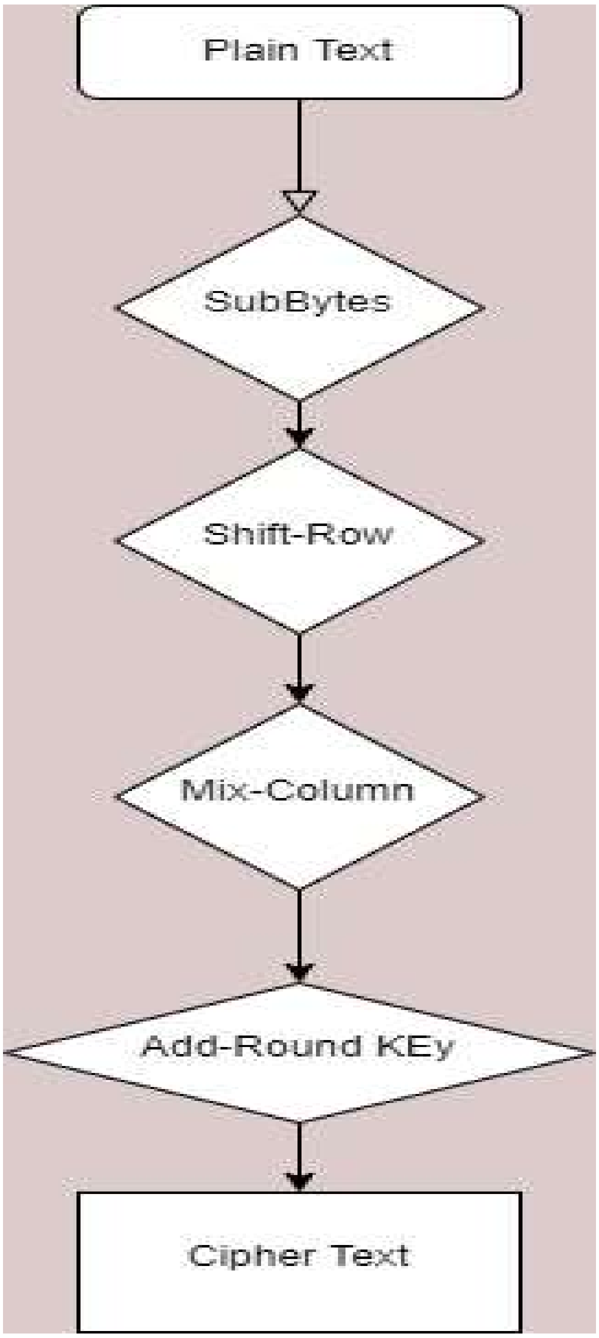
Add round key: XORs the produced primary key (K0) with the block information that is kept in the status indicator. sends the produced state cluster to the following step as a contribution.

Subbytes: Each byte in the status cluster is converted to hexadecimal in this phase, with a space in the center. To produce new characteristics for the most recent national show, these portions are the lines and sections that were prepared with a replacement box (S- Box).

Shift rows: swaps the elements of the column among themselves. Do not read the main column. The following column's components should be placed one situation to the side. Move the last row three places to the side as well as the elements in the third column two successive positions to the side.

Mix Column: To get another segment for the next status display, a frame identical to each segment in the status group is duplicated. Expanding each area with a comparable, regular grid will qualify it as a state exhibit for the following level. In this mood round, you shouldn't finish this stage.

Round Key added: The health indicator that was obtained in the previous phase is XORed with the key for the lap. The resultant status indicator becomes the ciphertext for the block if this is the final round; otherwise, it is sent as a new status cluster item for the following round.



GRAPH 1 - AES PROCEDURE

(src – [12] made using DRAWIO)

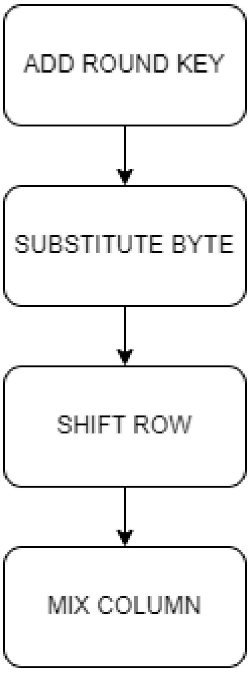
1.4.1 Encryption Method

Three steps make up AES's encryption process[11]: the opening round, the major phases, and the last round.

The first round is AddRoundKey.

2. AddRoundKey; Main Rounds; SubBytes; ShiftRows; MixColumns;

3. ShiftRows, AddRoundKey, SubBytes, ShiftRows, Final Round



GRAPH 2 - ENCRYPTION STEPS

(src – [12] -made using DRAWIO)

1.4.2 Decryption Method

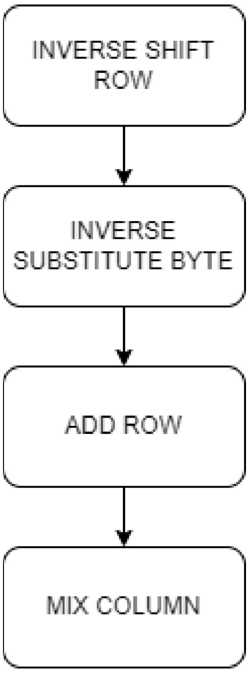
An AES ciphertext's decryption procedure is quite identical to its encryption procedure in reverse. The four steps are carried out in the reverse sequence in each round.

1. ShiftRows, Inverse Final Round, AddRoundKey, and SubBytes

2. Inverted Main Round AddRoundKey MixColumns - This step is identical to the encryption's MixColumns step, but the matrices used to perform the operation is different.

When decrypting data, bytes are replaced using a lookup table called ShiftRows SubBytes -Inverse S-box.

3. AddRoundKey for the Inverse Initial Round.



GRAPH 3 - DECRYPTION STEPS

(src – [12] - made using DRAWIO)

1.4.3 Key Expansion Algorithm

A well-liked and very safe symmetric encryption method is the Advanced Encryption Standard. It operates on data blocks that of a specific size and creates the round encryption keys using a key expansion method. We'll discuss the key expansions algorithm that AES uses.

Using 128-bit blocks of key, the AES-128 encryption method is used to encrypt data. The key expansion method expands this 128-bit key. These circular keys are utilised throughout both the encryption and decryption operations.

The key expansion algorithm's four fundamental parts are the

- key scheduling,
- byte substitution,
- row shifting,
- column mixing.

Key Scheduling

The first step in the key expansion algorithm is the generation of the key schedule. In this method, the 128-bit key is split into 4 words. These words, together with additional 32-bit words, are then used to create the round keys.

To create the key schedule, a number of operations are applied to the starting key and the previously created words. Round constant XOR, XOR, and substitution using the S-box are some of these processes.

Byte Substitution

The next step in the key expansions approach is byte substitution utilising the S-box. The S-box, a pre-defined table, replaces each input byte with an equivalent byte. The security of the encryption process is increased by this non-linear substitution.

Row Moving

The third stage of the key expansions method involves row shifting. This includes modifying the rows of the key schedule by a specific amount of bytes. Depending on the round number, various numbers of bytes are sent for each round.

Column Mixing

The final step in the key expansions method is column mixing. This involves performing many operations on the columns of the main schedule. These procedures consist of an XOR with additional columns and a fixed polynomial multiplication. These circular keys are utilised throughout both the encryption and decryption operations.

In conclusion, the key expansion procedure is an essential component of the AES encryption method. It employs a 128-bit key to generate the 11 round keys required for encryption and decryption. The main expansion algorithm's four fundamental stages really do expansion. By combining these activities, the encryption process is given an exceptionally high level of security and is able to produce trustworthy round keys.

For the design of my system, I used –

- Pyqt5 for interface
- Base64 for binary conversion
- Crypto. Cipher for using AES

Chapter 2: LITERATURE SURVEY

The authors of [1] offer a novel "Chaotic Key-Based Design for Image Encryption and Decryption". It is advised to encrypt and decode images using a VLSI architecture. Bit-by-bit XORing or XNORing is used to generate predetermined variables for the chaotic binary sequence of each pixel's grey level. Some of the features include good security, negligible distortion, and low computational effort. Low hardware costs, rapid processing, and efficient hardware usage are advantages of VLSI design. Both the architecture and the MPEG2 scheme are included, and simulation results are also accessible.

The authors of [2] describe a customized AES dependent algorithm for image cryptography. The most popular technique for safeguarding photos is encryption. There are many applications for images and videos, including in telemedicine, medical imaging, multimedia systems, and military communication. There are several ways to preserve pictures, including vector quantization. Breaking the image down into component vectors and encoding and decoding them one at a time is one of several vector quantization approaches. Or by making a lot of reflections, which ensures that the image won't be seen by unauthorised users.

The creators of [3] provide secure photo encryption using AES. Security is the most significant and serious issue in today's society.
Protecting personal information from unauthorised access has become a major concern as the use of pictures for communication has increased. Giving security to someone is challenging. There are several strategies for protecting data from unauthorised users. AES is used when a photograph has to be encrypted or decrypted. The image is first altered using the key into an illegible format, then when the receiver approves it, it is changed back into the original image.

An AES-based photo encryption and decryption solution is provided by the developers of [4]. Effective security for picture transmission is built using the AES encryption and decryption method. AES has replaced Data Encryption

Standard because it provides more security. Data is encrypted using a 128-bit key and either bitwise exclusives or operations on image-set pixels with the AES key expansion.

The authors of [5] offer An Image Encryption Dependent n AES Key Extension. A fast rate of transmission with finite bandwidth, redundancy, bulk capacity, and pixel correlation are only a few of the characteristics of images.
Certain characteristics must be taken into account before encrypting the picture. The AES method is employed with key expansion to do bit wise exclusive encryption or work with a picture pixel set and a 128 bit key.
The key is generated using AES Key Expanding on both the transmitter and receiver sides.

In this article [6], we also discovered that there is a trade-off between security and speed by comparing the lengths of time required for various encryption and decryption computations of varying log sizes. The two factors of time and safety are crucial in deciding on a computation since multiplying the difference by one of them would change how the framework represents productivity and safety.

The coordination of this document [7] is as follows: A brief history of AES calculation is provided in Section 2. Segment 3 examines related work. Segment 4 provides the AES calculus evaluation rules. The AES calculation's fundamental framework is given. Section 6 presents the AES calculation's encryption cycle. The AES Extended Key makes sense in section 7. Section 8 details the decryption procedure. AES launch pads are covered in Section 9.

This paper [8] proposes a computation for intelligent photo encryption based on out-of-order bundling and a modified AES calculation. This generates the encryption key using the Amold unordered sequence. The first image is then encoded using the round keys from the Riot framework and a customized AES computation. The proposed computation encodes images that are resistant to differential attacks by increasing diffusivity while simultaneously reducing the temporal complexity of the approach. The essential space of the proposed method is large enough to fend off attacks from animal power. Since the underlying qualities and picture information are so important to this method, even little modifications to these elements can have a big impact on the encoded image. Since the underlying qualities and picture information are so important to this method, even little modifications to these elements can have a big impact on the encoded image. Using quantitative testing, we show how this tactic may protect the image from actual attackers. The results of the entropy test show that the entropy values are very close to ideal, demonstrating that the suggested computation is resistant to entropy attacks. According to game results, it is impossible to make small changes to the first frame, and the key causes significant changes to both the encoded frame and the first frame.

In [9] The security of computer circuits is seriously threatened by actual idle raids like control scans. In this white paper, we propose a side-channel production team strategy that meets a wide range of security needs and is encrypted using the Progressed Encryption Standard (AES). They demonstrate how to defend against high-demand, multivariate assaults when mistakes have comparable random costs to sensitive circuits. Despite the adaptability of our AES arrangement, it is simpler, quicker, and necessitates fewer inconsistencies than the protected AES operating on the opposing side channel. For instance, each S-Box activity in our First Request-Secure-AES tariff only takes 18 bits of randomness and 6 KGE of chip space.

In [10] In an open organisation, handling information, communication, messaging, and electronic exchange presents a number of security-related challenges. Combining message encryption with secret composition, or cryptography, makes data secure and impenetrable. The symmetric encryption standard put forward by NIST is called AES. AES developed into a very safe, quick, and powerful encryption algorithm. AES is commonly utilised because of its extraordinary strength and effectiveness. Digital assaults, however, have increased recently, prompting security specialists to stay busy in the lab creating new strategies to fend off intruders. Animal Power Assault, Differential Assault, Logarithmic Assault, and Direct Assault are all potential attacks in the symmetric calculation. Therefore, an AES computation with a combined method of dynamic key age and dynamic S-box age is presented in order to ensure good security in message transmission. In the crossover technique, we first use Dynamic Key Age to gradually increase complexity in order to create confusion and spread the code text, and then we use Dynamic S-Box Age to make it more challenging for an attacker to execute static layout investigations.

Rijndael's approach is [12] The provider uses AES, a high-level encryption standard. The US Public Policy and Research Organisation chose the Rijndael block cypher as a high (AES) in October 2000. AES is expected to gradually replace the currently utilised (DES) as the most popular information encryption invention. The creators of the well-known cartoon character Rijndael introduce Rijndael in this book without any prior knowledge. Applications of direct and divergent cryptanalysis are embraced, along with thorough explanations of Secret Math and the broad-path strategy as basic planning principles. All known assaults on the procedure construction are verified by the resulting components, which also handle execution and advancement issues.

Chapter 3 - SYSTEM DEVELOPMENT

3.1 Algorithm Overview

The essence of AES is this: we organize every block of the plaintext into a 4x4 grid and over and over play out a bunch of procedure on it. we tend to decision each cycle a spherical, and that we perform 10, twelve or fourteen rounds relying upon the key length (this is an extra boundary picked by NIST).

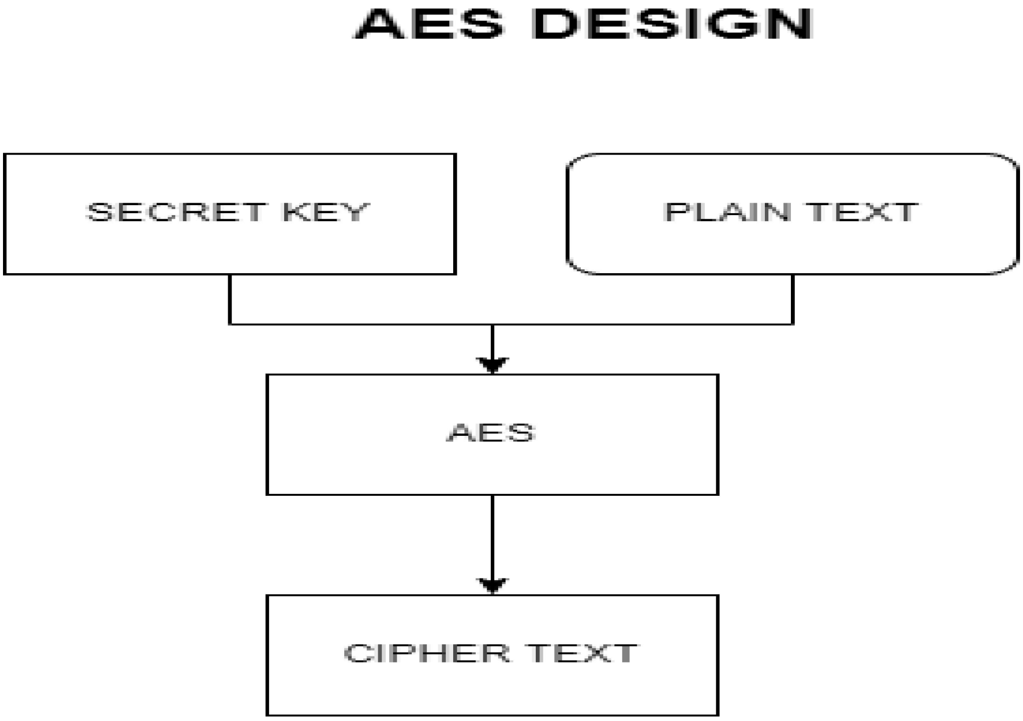


FIGURE 1 - AES DESIGN

(src – [12] - made using DRAWIO)

10 rounds for a 128-digit key12 rounds for a 196-piece key14 rounds for a 256-cycle key For each round, we turn out a round key from the super key utilizing the Rijndael Key Timetable. There are four procedure on the 4x4 grid that we characterize:

1. subBytes()
2. shiftRows()
3. mixColumns()
4. addRoundKey()

A few out of every odd spherical of tasks are some things terribly similar: for the first round, we tend to simply add the round key, and for the last round we overlook the mixColumns () step. Thus, the pseudocode for the AES calculation may look something like this:

System Design Procedure -

Firstly, We have frontend made using python module named pyqt(). This provides an interactive window for the user. The user needs to provide the location of the image to be encoded/decoded. After this, user can either go for encoding or decoding the image. It asks for a password, which is basically your encryption key. After these details are entered, we use the python functions declared in the code to encode/decode the image using AES file from crypto. Cypher module of python. When this process is done, the user will get encrypted/decrypted image as output which will be saved in the same directory as input image file.

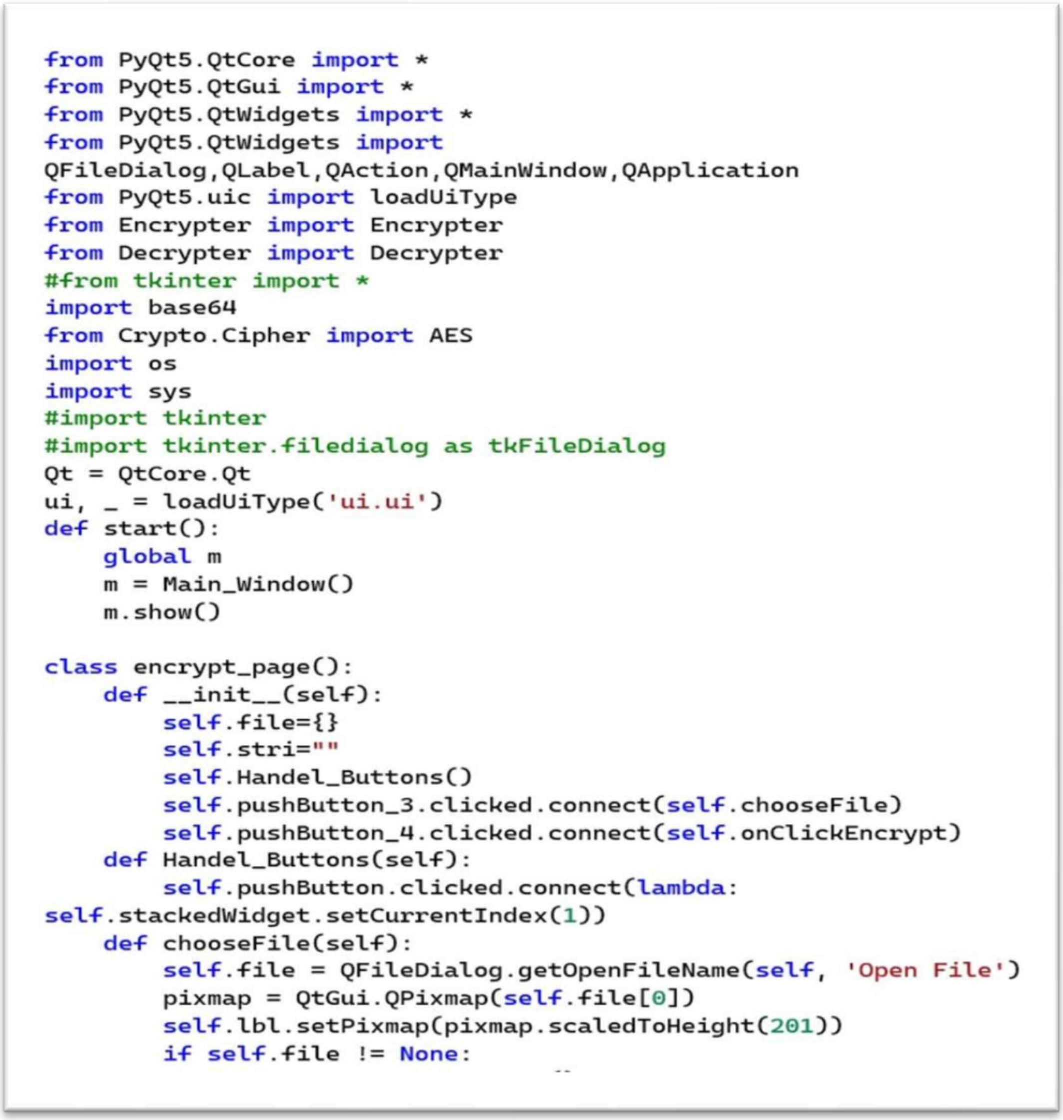
The interface window gives us a box for entering the location of image. Along with this box, it also contains two buttons for encoding and decoding the image. After clicking on one of these buttons, next window has a textbox to enter the password and a submit button. After submitting, it shows the filename of new image file generated.

Then we defined function for Encryption using AES pycryptodome and using cipher. Encrypt.

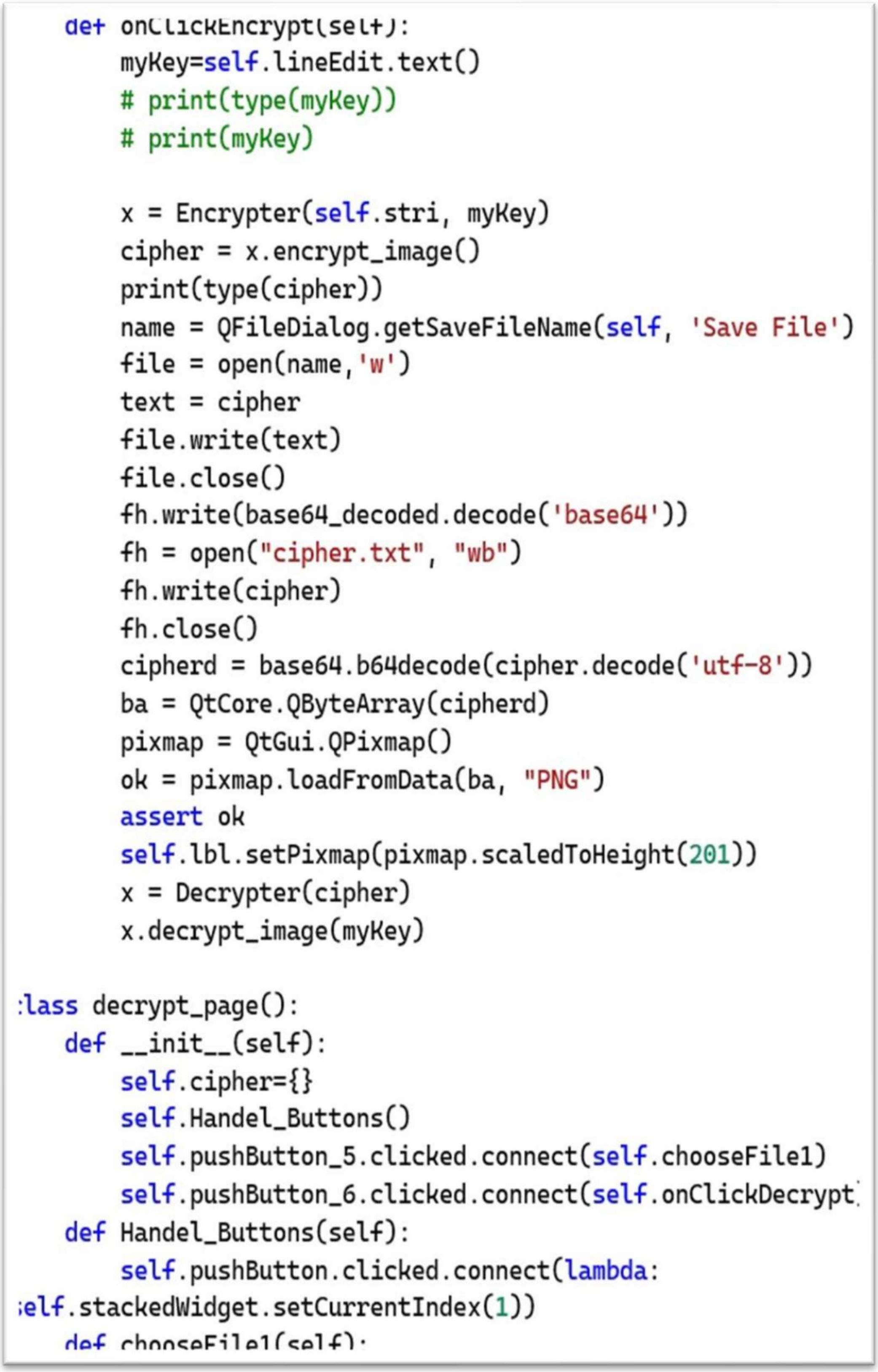
Similarly function for decryption using cipher. Decrypt.

3.2 CODE –

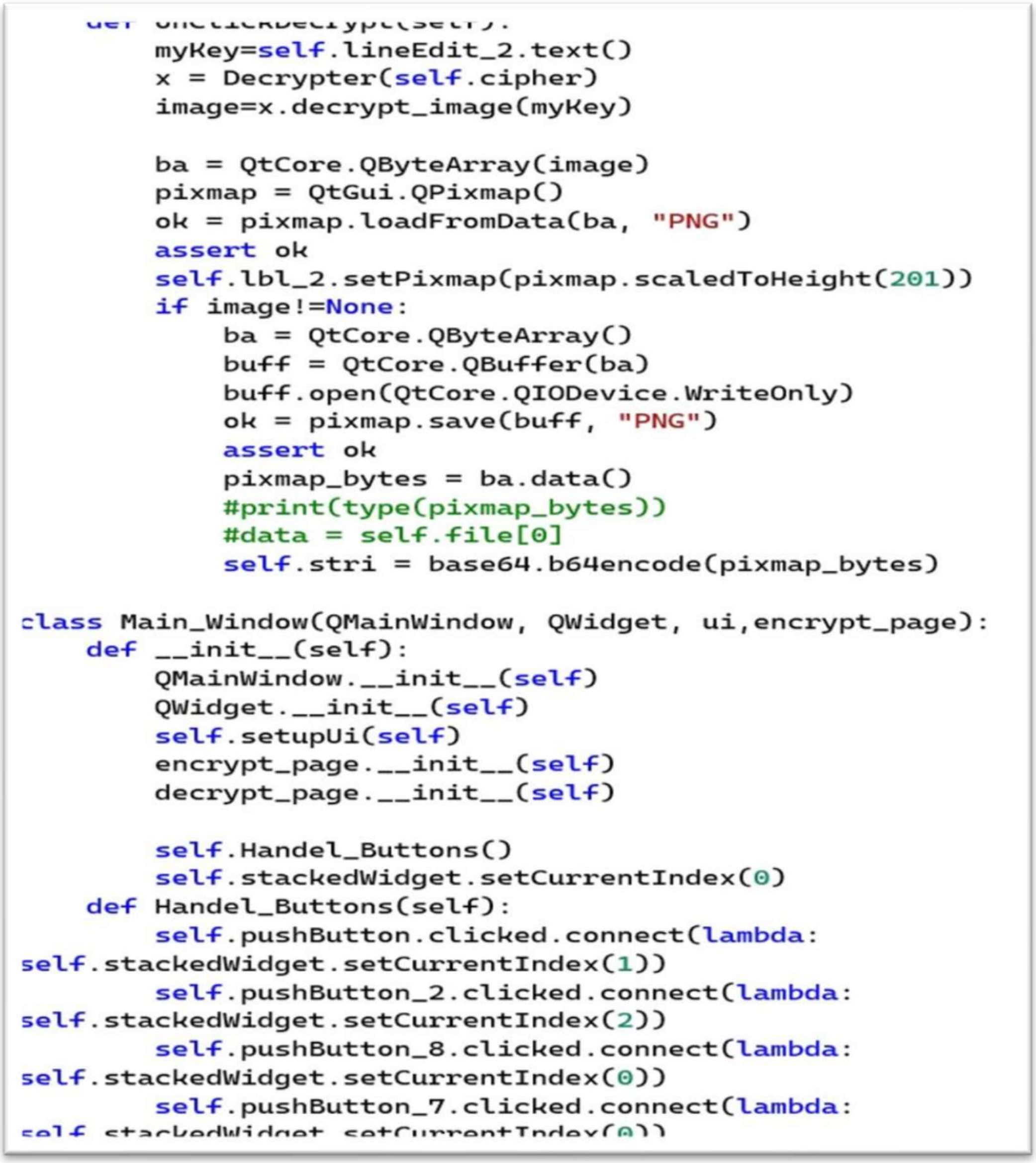
1. MAIN.PY



```
from PyQt5.QtCore import *
from PyQt5.QtGui import *
from PyQt5.QtWidgets import *
from PyQt5.QtWidgets import
QFileDialog,QLabel,QAction,QMainWindow,QApplication
from PyQt5.uic import loadUiType
from Encrypter import Encrypter
from Decrypter import Decrypter
#from tkinter import *
import base64
from Crypto.Cipher import AES
import os
import sys
#import tkinter
#import tkinter.filedialog as tkFileDialog
Qt = QtCore.Qt
ui, _ = loadUiType('ui.ui')
def start():
    global m
    m = Main_Window()
    m.show()

class encrypt_page():
    def __init__(self):
        self.file={}
        self.stri=""
        self.Handel_Buttons()
        self.pushButton_3.clicked.connect(self.chooseFile)
        self.pushButton_4.clicked.connect(self.onClickEncrypt)
    def Handel_Buttons(self):
        self.pushButton.clicked.connect(lambda:
self.stackedWidget.setCurrentIndex(1))
    def chooseFile(self):
        self.file = QFileDialog.getOpenFileName(self, 'Open File')
        pixmap = QtGui.QPixmap(self.file[0])
        self.lbl.setPixmap(pixmap.scaledToHeight(201))
        if self.file != None:
```

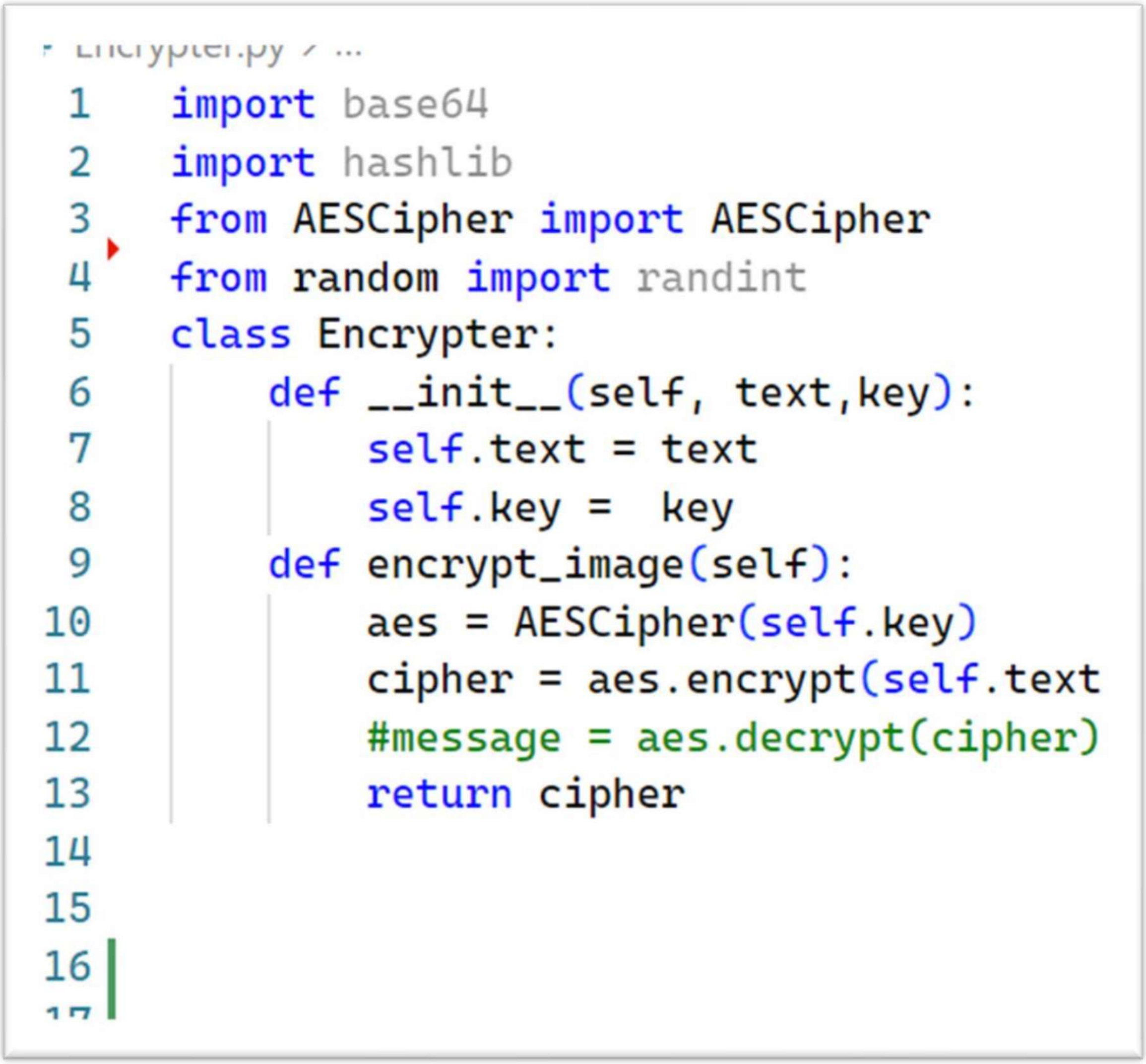


```
    def onClickEncrypt(self):
        myKey=self.lineEdit.text()
        # print(type(myKey))
        # print(myKey)

        x = Encrypter(self.stri, myKey)
        cipher = x.encrypt_image()
        print(type(cipher))
        name = QFileDialog.getSaveFileName(self, 'Save File')
        file = open(name,'w')
        text = cipher
        file.write(text)
        file.close()
        fh.write(base64_decoded.decode('base64'))
        fh = open("cipher.txt", "wb")
        fh.write(cipher)
        fh.close()
        cipherd = base64.b64decode(cipher.decode('utf-8'))
        ba = QtCore.QByteArray(cipherd)
        pixmap = QtGui.QPixmap()
        ok = pixmap.loadFromData(ba, "PNG")
        assert ok
        self.lbl.setPixmap(pixmap.scaledToHeight(201))
        x = Decrypter(cipher)
        x.decrypt_image(myKey)

class decrypt_page():
    def __init__(self):
        self.cipher={}
        self.Handel_Buttons()
        self.pushButton_5.clicked.connect(self.chooseFile1)
        self.pushButton_6.clicked.connect(self.onClickDecrypt)
    def Handel_Buttons(self):
        self.pushButton.clicked.connect(lambda:
self.stackedWidget.setCurrentIndex(1))
    def chooseFile1(self):
```



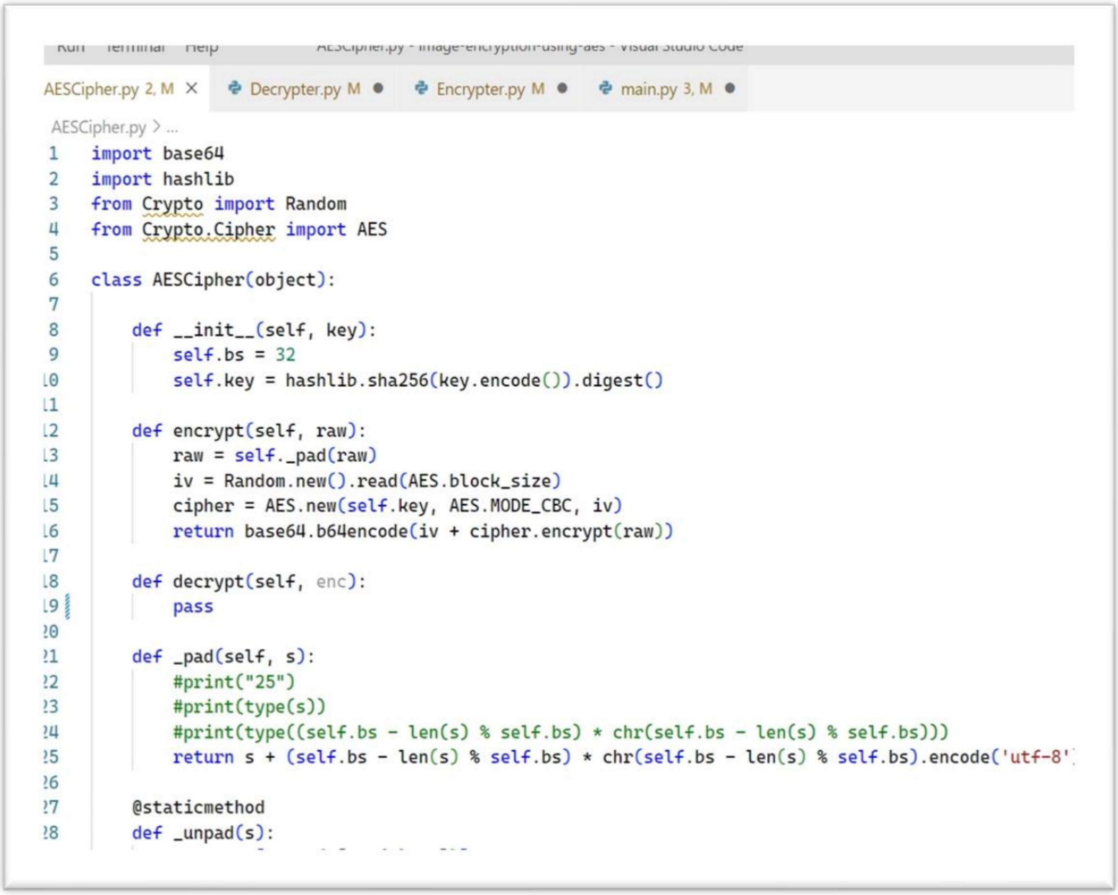
```
    def onClickDecrypt(self):
        myKey=self.lineEdit_2.text()
        x = Decrypter(self.cipher)
        image=x.decrypt_image(myKey)

        ba = QtCore.QByteArray(image)
        pixmap = QtGui.QPixmap()
        ok = pixmap.loadFromData(ba, "PNG")
        assert ok
        self.lbl_2.setPixmap(pixmap.scaledToHeight(201))
        if image!=None:
            ba = QtCore.QByteArray()
            buff = QtCore.QBuffer(ba)
            buff.open(QtCore.QIODevice.WriteOnly)
            ok = pixmap.save(buff, "PNG")
            assert ok
            pixmap_bytes = ba.data()
            #print(type(pixmap_bytes))
            #data = self.file[0]
            self.stri = base64.b64encode(pixmap_bytes)

class Main_Window(QMainWindow, QWidget, ui,encrypt_page):
    def __init__(self):
        QMainWindow.__init__(self)
        QWidget.__init__(self)
        self.setupUi(self)
        encrypt_page.__init__(self)
        decrypt_page.__init__(self)

        self.Handel_Buttons()
        self.stackedWidget.setCurrentIndex(0)
    def Handel_Buttons(self):
        self.pushButton.clicked.connect(lambda:
self.stackedWidget.setCurrentIndex(1))
        self.pushButton_2.clicked.connect(lambda:
self.stackedWidget.setCurrentIndex(2))
        self.pushButton_8.clicked.connect(lambda:
self.stackedWidget.setCurrentIndex(0))
        self.pushButton_7.clicked.connect(lambda:
self.stackedWidget.setCurrentIndex(0))
```

2. ENCRYPTER.PY



```python
import base64
import hashlib
from AESCipher import AESCipher
from random import randint
class Encrypter:
    def __init__(self, text,key):
        self.text = text
        self.key =  key
    def encrypt_image(self):
        aes = AESCipher(self.key)
        cipher = aes.encrypt(self.text
        #message = aes.decrypt(cipher)
        return cipher
```

3. DECRYPTER.PY



```python
import base64
import hashlib
from Crypto import Random
from Crypto.Cipher import AES

class AESCipher(object):

    def __init__(self, key):
        self.bs = 32
        self.key = hashlib.sha256(key.encode()).digest()

    def encrypt(self, raw):
        raw = self._pad(raw)
        iv = Random.new().read(AES.block_size)
        cipher = AES.new(self.key, AES.MODE_CBC, iv)
        return base64.b64encode(iv + cipher.encrypt(raw))

    def decrypt(self, enc):
        pass

    def _pad(self, s):
        #print("25")
        #print(type(s))
        #print(type((self.bs - len(s) % self.bs) * chr(self.bs - len(s) % self.bs)))
        return s + (self.bs - len(s) % self.bs) * chr(self.bs - len(s) % self.bs).encode('utf-8'

    @staticmethod
    def _unpad(s):
```

Chapter 4 - Performance Analysis

4.1 System Properties

It uses python-based GUI which is user friendly and provides buttons for easy navigation. A person with basic understanding of computer can easily use this software for encrypting/decrypting image using key.

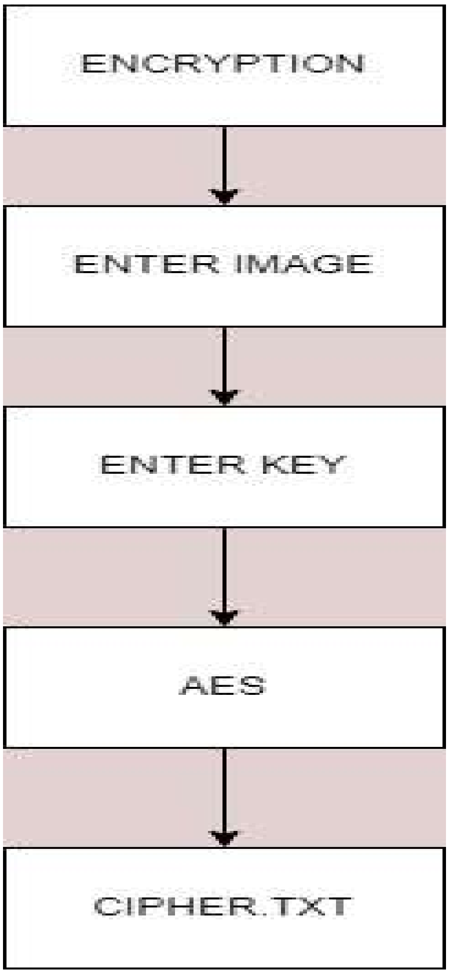
External factors do not affect the system. AES algorithm is universally accepted and generates consistent results therefore there are very less chances of errors. Error can occur only if there is a transmission glitch (the probability of which is very rare). So, the system is reliable.

The system is easy to test and find defects. The system is divided into different modules performing specific functions that can be tested individually.

Image size should be less than 10 mb. Decryption takes less than 10 seconds.

Encryption is done using encryption key. Decryption will happen only when same encryption key is used at the receiver side.

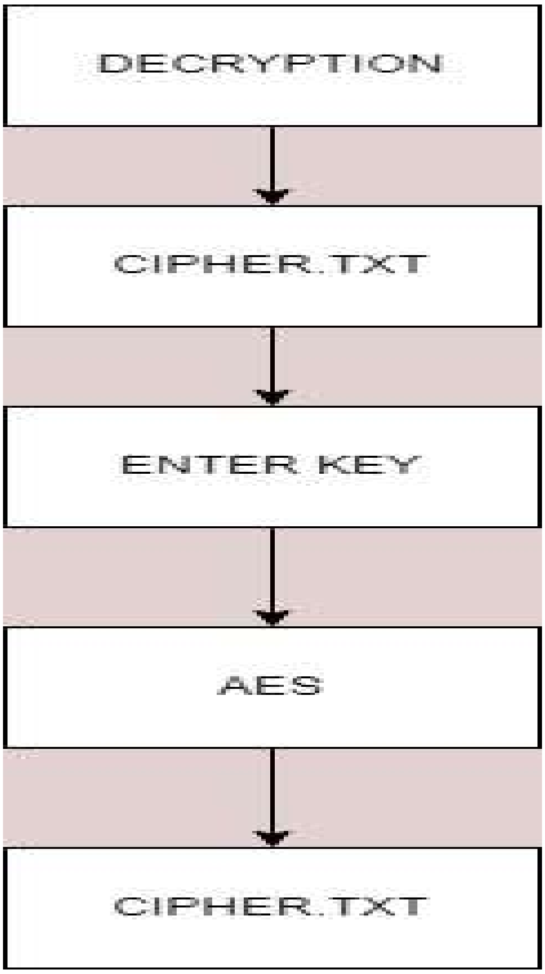
4.1.1 ENCRYPTION TECHNIQUE



GRAPH 4 - ENCRYPTION TECHNIQUE

(src - made using-DRAWIO)

4.1.2 DECRYPTION TECHNIQUE

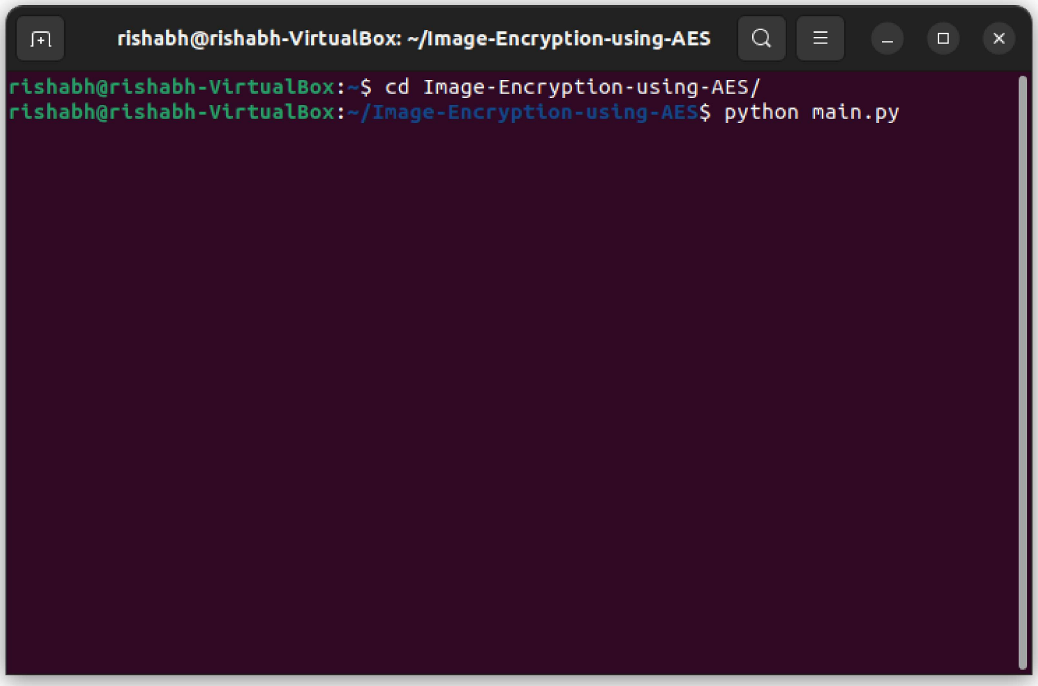


GRAPH 5 – DECRYPTION TECHNIQUE

(src - made using DRAWIO)

4.2 PROJECT IMPLEMENTATION STEPS

1.Call the program using terminal

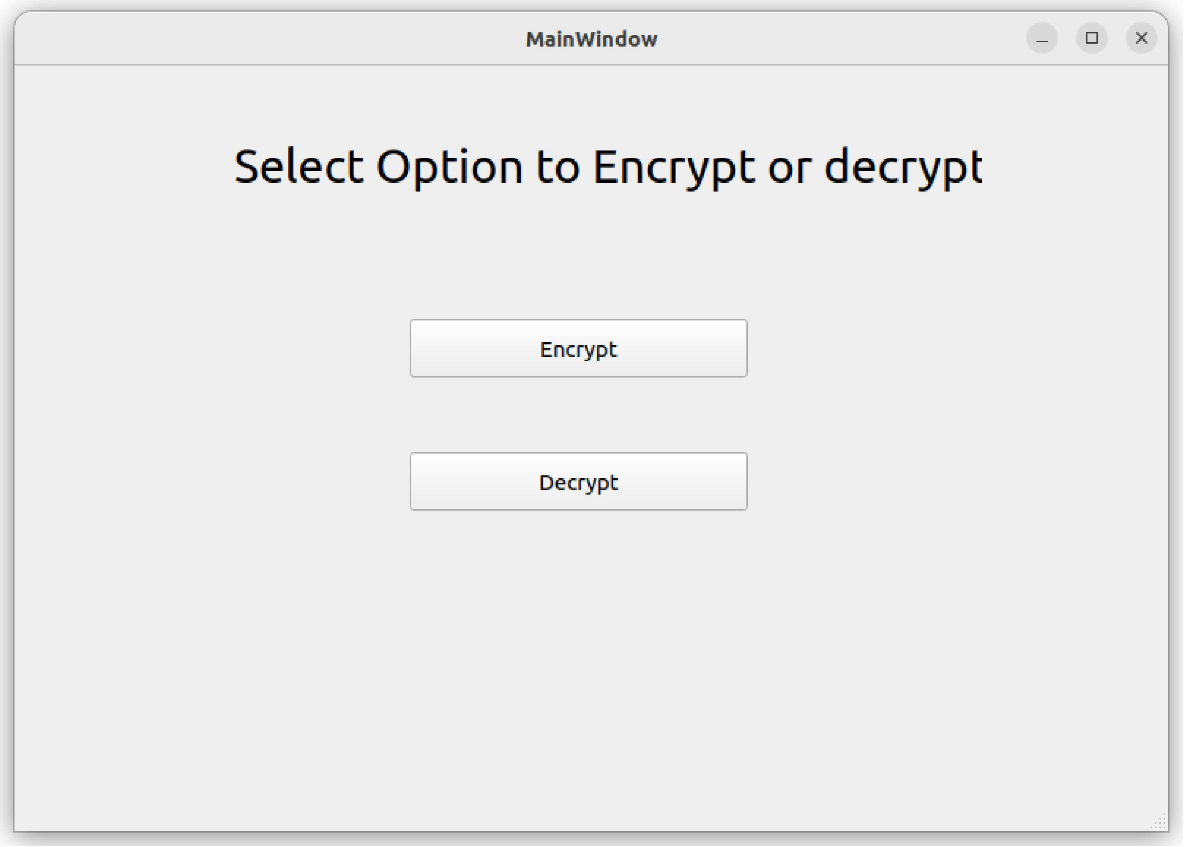


```
rishabh@rishabh-VirtualBox:~$ cd Image-Encryption-using-AES/
rishabh@rishabh-VirtualBox:~/Image-Encryption-using-AES$ python main.py
```

FIGURE 2 – PROJECT IMPLEMENTATION

(src – PROJECT IMPLEMENTATION)

2. After Running Gui Will Prompt User To Choose Encrypt Or Decrypt

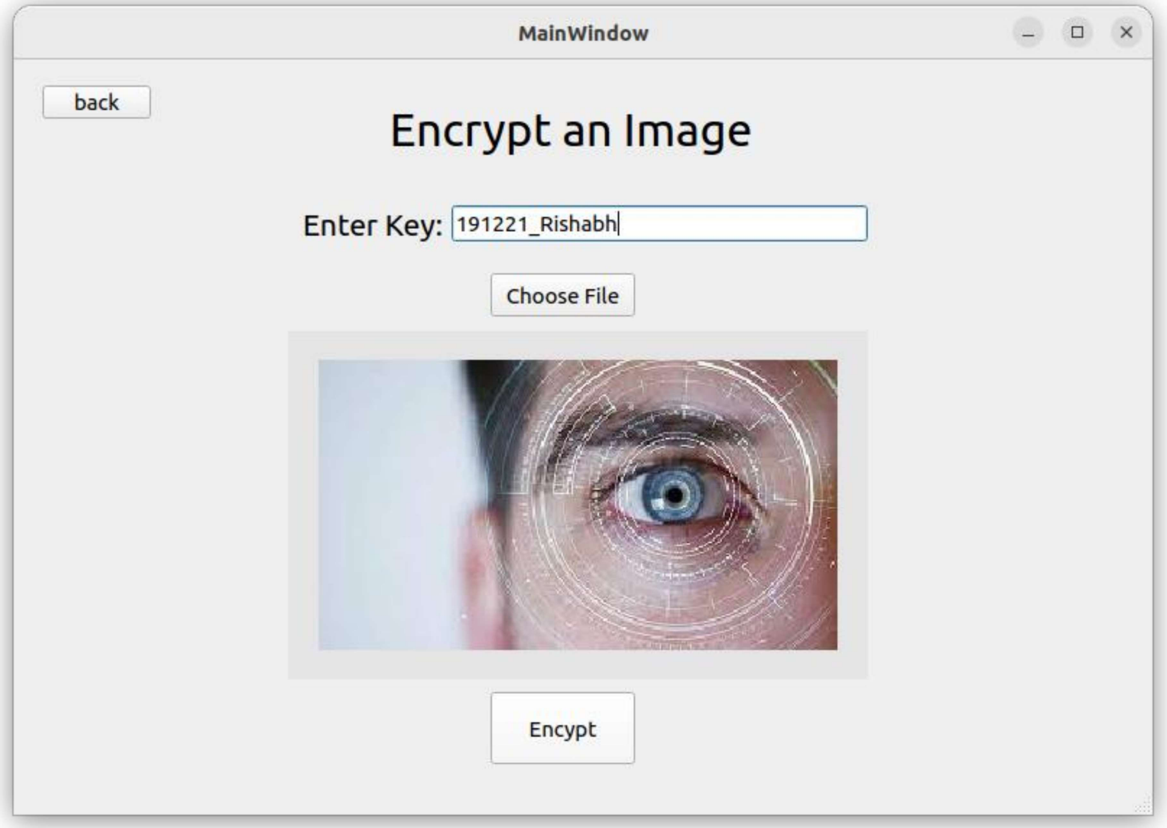


Select Option to Encrypt or decrypt

FIGURE 3- GUI

(src-PROJECT IMPLEMENTATION)

3. Now we select Image for encryption and enter key



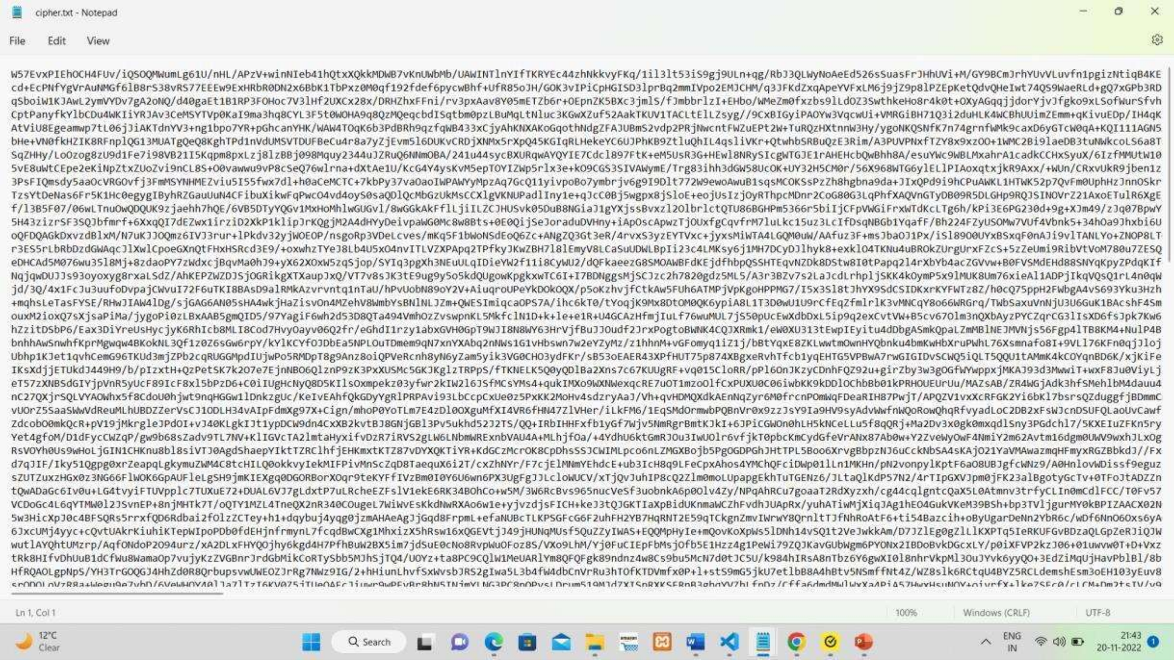
Encrypt an Image

Enter Key: 191221_Rishabh

FIGURE 4- Selecting Image for Encryption

(src - PROJECT IMPLEMENTATION)

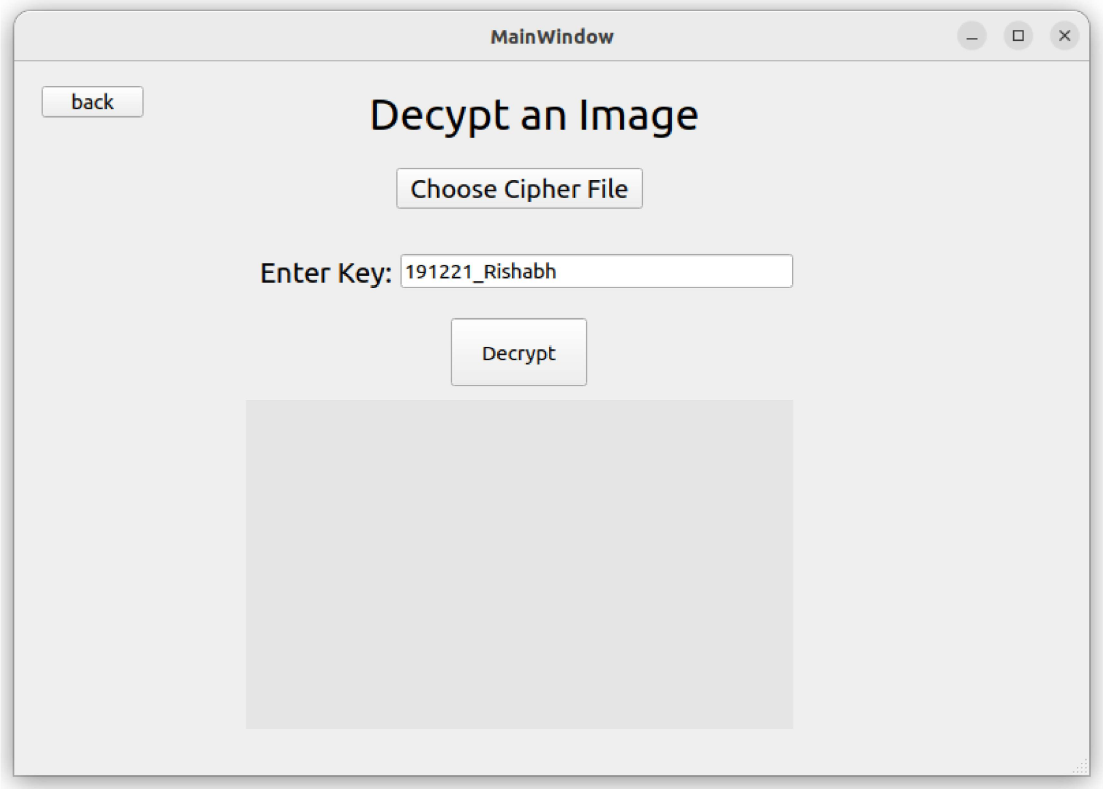
4. Cipher.Text Is Generated After Encryption



```
W57EvxPIEhOCH4FUv/iQSOQMWumLg61U/nHL/APzV+winNIeb41hQtxXQkkMDWB7vKnUWbMb/UAWINTlnYIfTKRYEc44zhNkkvyFKq/1il3lt53iS9gj9ULn+qg/RbJ3QLWyNoAeEd526sSuasFrJHhUVi+M/GY9BCmJrhYUvVLuvfn1pgizNtiqB4KE
cd+EcPNfYgVrAuNMGf6lB8rS38vRS77EEEw9ExHRbR0DN2x6BbK1TbPxz0M0qf192fdef6pycwBhf+UfR85oJH/GOK3vIPiCpHGISD3lprBq2mmIVpo2EMJCHM/q3JFKdZxqApeYVFxLM6j9jZ9p8lPZEpKetQdvQHeIwt74QS9WaeRLd+gQ7xGPb3RD
qSboiW1KJAwL2ymVYDv7gA2oNQ/d40gaEt1B1RP3FOHoc7V3lHf2UXCx28x/DRHZhxFFni/rv3pxAav8Y05mETZb6r+OEpnZK5BXc3jmlS/fJmbbrlzI+EHbo/WMeZm0fxzbs9lLdOZ3SwthkeHo8r4k0t+OXyAGqqjjdorYjvJfgko9xLSofWurSfvh
CptPanyfkYlbCDu4WKIiYRJAv3CeMSYTVp0KaI9ma3hq8CYL3F5t0WOHA9q8QzMQeqcbdISqtbm0pzLBuMqLtNluc3KGwXZuf52AakTKUV1TACLtElLZsyg//9CxBIGyiPAOYw3VqcwUi+VMRGiBH71Q3i2duHLK4WCBhUUimZEmm+qKivuEDp/IH4qK
AtViU8Egeamwp7tL06jJiAKTdnYV3+ng1bpo7YR+pGhcanYHK/WAW4TOqK6b3PdBRh9qzfqWB433xCjyAhKNXAKoGqothNdgZFAJUBmS2vdp2PRjNwcntFWZuEPt2W+TuRQzHXtnnW3Hy/ygoNKQSNfK7n74grnfWMk9caxD6yGTcW0qA+KQI111AGN5
bHe+VN0fkHZIK8RFnplQG13MUATgQeQ8KghTPd1nVdUMSVTDUFBeCu4r8a7yZjEvm5l6DUKvCRDjXNMx5rXpQ45KGIqRLHekeYC6UJPhKB9ZtluQhIL4qsliVKr+QtwhbSRBuQzE3Rim/A3PUVPNxfTZY8x9xzOO+1WMC2Bi9laeDB3tuNWkcoLS6a8T
SqZHHy/LoOzog8zU9d1Fe7i98VB21I5Kqpm8pxLzj8lzBBj098Mquy2344uJZRuQ6NNmOBA/241u44sycBXURqwAYQYIE7Cdcl897FtK+eM5UsR3G+HEwl8NRySIcgWTGJE1rAHEHcbQwBhh8A/esuYWc9WBLMxahrA1cadkCCHxSyuX/6IzfMMUtW10
5vE8uWtCEpe2eKiNpZtxZUoZvi9nCL8S+O0vawwu9vP8cSeQ76wlrna+dXtAe1U/KcG4Y4ysKvM5epTOYIZWp5rlx3e+kO9CGS3SIVAWymE/Trg83ihh3dGW58UcOK+UY32H5CM0r/56X968WTG6ylELlPIAoxqtxjkR9Axx/+WUn/CRxvUkR9jben1z
3PsFIQmsdy5aaOcVRGOvfj3FmMSYNHMEZviu5I55fwx7dl+h0aCeMCTC+7kbPy37vaOaoIWPAWYyMpzAq7GcQ11yivpoBo7ymbrjv6g9I9Dlt772W9ewoAwuB1sqsMCOKSsPzZh8hgbna9da+JIxQPd9i9hCPuAWKL1HTWK52p7QvFm0UphHzJnnOSkr
TzsYtDeNas6Fr5K1Hc0egygIByhRZGauUuN4CFibuXikwFqPwcO4vd4oyS0saQDlQcMbGzUkMsCCXlgVKNUPadlIny1e+qJcC0Bj5wgpx8jSloE+eojUsIzjOyRThpcMDnr2CoG80G3LqPhfXAQVnGTyDB09R5DLGHp9RQJSINOVrZ21AxoETulR6XgE
f/l3B5F07/06wLTnuOwQDQUK9zjaehh7hQE/6VB5DTyYQGv1MxHoMhlwGUGvl/8wGGkAkFflLjiILZCJHUSvk05DuB8NGiaJ1gYXjssBvxzl2OlbrlctQTU86BGHPm5366r5biIjCFpVWGiFrxWTdKcLTg6h/kPi3E6PG230d+9g+XJm49/zJq07BpwY
5H43zizrSF3SQJbfmrf+6XxqQI7dEZwx1irziD2XkP1klipJrKQgjM2A4dHYyDeivpaWG0Mc8w8Bts+0E0QijSeJoraduDVHny+iApOscApwzTjOUxfgCqvfrM7luLkc15uz3LcIfDsqNBGb1YqafF/Bh224FZyUSOMw7VUf4Vbnk5+34hOa9Jhxbi6U
oQFDQAGkDxvzdBlxM/N7uKJJOQmz6IVJ3rur+lPkdv32yjWOEOP/nsgoRp3VDeLcves/mKq5F1bWoNSdEoQ6Zc+ANgZQ3Gt3eR/4rvxS3yzEYTVxc+jyxsMiWTA4LGQM0uW/AAfuz3F+msJbaOJ1Px/iSl89O0UYxBSxqF0nAJi9vlTANLYo+ZNOP8LT
r3ES5rLbRbDzdGWAqcJlXwlCpoeGXnQtFHxHSRcd3E9/+oxwhzTYeJ8Lb4U5xO4nvITLVZXPApq2TPfkyJKwZBH7l8lEmyV8LCaSuUDWLBpIi23c4LMKsy6j1MH7DCyDJlhyk8+exklO4TKNu4uBROkZUrgUrxFZcS+5zZeUmi9RibVtVoM78Ou7ZESQ
eDHCAd5M076wu35l8Mj+8zdaoPY7zWdxcjBqvMa0hJ9+yX62XOxW5zqSjop/SYIq3pgXh3NEuULqIDieYW2f11i8CyWU2/dQFkaeezG8SMOAWBFdKEjdfhbpQSSHTEqvNZDk8DStw8I0tPapq2l4rXbYb4acZGVvw+B0FVSMdEHd88SNYqKpyZPdqKIf
NqjqwDUJJs93oyoxyg8rxaLSdZ/AhKEPZWZDJSjOGRikgXTXaupJxQ/VT7v8sJK3tE9ug9y5o5kdQUgowKpgkxwTC6I+I7BDNggsMjSCJzc2h7820gdz5ML5/A3r3BZv7s2LaJcdLrhpljSKK4kOymP5x9lMUK8Um76xieAl1ADPjIkqVQsQ1rL4n0qW
jd/3Q/4x1FcJu3uufoDvpajCWvuI72F6uTKI8BAsD9alRMkAzvrvntq1nTaU/hPvUobN89oY2V+AiuqroUPeYkDOkOQX/p5oKzhvjfCtkAw5FUh6ATMPjVpKgoHPPMG7/I5x3Sl8tJhYX9SdCSIDKxrKYFWTz8Z/h0cQ75ppH2FWbgA4vS693Yku3Hzh
+mqhsLeTasFYSE/RHwJIAW4lDg/sjGAG6AN05sHA4wkjHaZisvOn4MZehV8WmbYsBNlNLJZm+QWESImiqcaOPS7A/ihc6kT0/tYoqjK9Mx8DtOM0QK6ypiA8L1T3D0wU1U9rCfEqZfmlrlK3vMNCqY8o66WRGrq/TWbSaxuVnNjU3U6GuK1BAcshF4Sm
ouxM2ioxQ7sXjsaPiMa/jygoPi0zLBxAAB5gmQID5/97YagiF6wh2d53D8QTa494VmhOzZvswpnKL5MkfclN1D+k+le+e1R+U4GCAzHfmjIuLf76wuMUL7jS50pUcEwXdbDxL5ip9q2exCvtVW+B5cv67Olm3nQXbAyzPYCZqrCG3lIsXD6fsJpk7Kw6
hZzitDSbP6/Eax3DiYreUsHycjyK6RhIcb8MLI8Cod7HvyOayv06Q2fr/eGhdI1rzy1abxGVH0GpT9WJI8N8WY63HrVjfBuJJOudf2JrxPogtoBWNK4CQJXRmk1/eW0XU313tEwpIEyitu4dDbgASmkQpaLZmMBlNEJMVNjs56Fgp4lTB8KM4+NulP4B
bnhhAwSnwhfKprMgwqw4BKokNL3Qf1z0Z6sGw6rpY/kYlKCYfOJDbEa5NPLOuTDmem9qN7xnYXAbq2nNWs1G1vHbswn7w2eYZyMz/z1hhnM+vGFomyq1iZ1j/bBtYqxE8ZKLwwtmOwnHYQbnku4bmKwHbXruPWhL76Xsmnafo8I+9VLl76KFn0qjJloj
Ubhp1KJet1qvhCemG96TKUd3mjZPb2cqRUGGMpdIUjwPo5RMDpT8g9Anz8oiQPVeRcnh8yN6yZam5yik3VG0CHO3ydFKr/sB53oEAER43XPfHUT75p874XBgxeRvhTfcb1yqEHTG5VPBwA7rwGIGIDvSCWQ5iQLT5QQU1tAMmK4kCOYqnBD6K/xjKiFe
IKsXdjjETUkdJ449H9/b/pIzxtH+QzPetSK7k2O7e7EjnNBO6QlznP9zK3PxXUSMc5GKJKglzTRPpS/fTKNELK5Q0yQDlBa2Xns7c67KUUgRF+vq015CloRR/pPl6OnJKzyCDnhFQZ92u+girZby3w3gOGfWYwppxjMKAJ93d3MwwiT+wxF8Ju0ViyLj
eT57zXNBSdGIYjpVnR5yUcF89IcF8xl5bPzD6+C0iIUgHcNyQ8D5KIlsOxmpekz03yfwr2kIW2l6JSfMCsYMs4+qukIMXo9WXNWexqcRE7uOT1mzoOlfCxPUXU0C06iwbKK9kDDlOChbBb01kPRHOUEUrUu/MAZsAB/ZR4WGjAdk3hfSMehlbM4dauu4
nC27QXjrSQLVYAOWhx5f8CdoU0hjwt9nqHGGw1lDnkzgUc/KeIvEAhfQkGDyYgRlPRPAvi93LbCcpCxUe0z5PxKK2MoHv4sdzryAaJ/Vh+qvHDMQXdkAEnNqZyr6M0frcnPOmWqFDeaRIH87PwjT/APQZV1vxXcRFGK2Yi6bKl7bsrsQZduggfjBDmmC
vUOrZ5SaaSWwVdReuMLhUBDZZerVsCJ1ODLH34vAIpFdmXg97X+Cign/mhoP0YoTLm7E4zDl0OXguMfXI4VR6fHN47ZlVHer/iLkFM6/1EqSMdOrmwbPQBnVr0x9zzJsY9Ia9HV9syAdvWwfnWQoRowQhqRfvyadLoC2DB2xFsWJcnDSUFQLaoUvCawf
ZdcobO0mkQcR+pV19jMkrgleJPdOI+vJ40KLgkIJt1ypDCW9dn4CxXB2kvtBJ8GNjGBl3Pv5ukhd52J2TS/QQ+IRbIHHFxfb1yGf7Wjv5NmRgrBmtKJkI+6JPiCGWOn0hLH5kNCeLLu5f8qQRj+Ma2Dv3x0gk0mxqdlSny3PGdchl7/5KXEIuZFKn5ry
Yet4gfoM/D1dFycCWZqP/gw9b68sZadv9TL7NV+KlIGVcTA2lmtaHyxifvDzR7iRVS2gLW6LNbmWRExnbVAU4A+MLhjfOa/+4YdhU6ktGmRJOu3IwUOlr6vfjkT0pbcKmCydGfeVrANx87Ab0w+Y2ZveWyOwF4NmiY2m62Avtm16dgm0UWV9wxhJLxOg
RsVOYh0Us9wHoLjGIN1CHKnu8bl8siVTJ0AgdShaepYIktTZRClhfjEHKmxtKTZ87vDYXQKTiYR+KdGCzMcrOK8CpDhsSSJCWIMLpco6nLZMGXBojb5PgOGDPGhJHtTPL5Boo6XrvgBbpzNJ6uCckNbSA4sKAjO21YaVMAwazmqHFmyxRGZBbkdJ//Fx
d7qJIF/Iky51Qgpg0xrZeapqLgkymuZWM4C8tcHILQ0okkvyIekMIFPivMnScZqD8TaequX6i2T/cxZhNYr/F7cjElMNmYEhdcE+ub3IcH8q9LFeCpxAhos4YMChQFciDWp01lLn1MKHn/pN2vonpylKptF6aO8UBJgfcWNz9/A0HnlovWDissf9eguz
sZUTZuxzHGx0z3NG66FlWOK6GpAUFleLgSH9jmKIEXgq0DGORBorXOqr9teKYFfIVzBm0I0Y6U6wn6PX3UgFgJJLcloWUCV/xTjQvJuhIP8cQ2Zlm0moLUpapgEkhTuTGENz6/JLtaQlKdP57N2/4rTIpGXVJpm0jFK23alBgotyGcTv+0TFoJtADZZn
tQwADaGc6Iv0u+LG4tvyiFTUVpplc7TUXuE72+DUAL6VJ7gLdxtP7uLRcheEZFslV1ekE6RK34BOhCo+w5M/3W6RcBvs965nucVeSf3uobnkA6p0Olv4Zy/NPqAhRCu7goaaT2RdXyzxh/cg44cqlgntcQaX5L0Atmnv3trfyCLIn0mCdlFCC/T0Fv57
VCDoGc4L6qYTMW0l2JSvnEP+8njMHTk7T/oQTY1MZL4TneQX2nR340COugeL7WiWvEsKkdNwRXAo6w1e+yjvzdjsFICH+keJ3tQJGKTIaXpBidUKnmaWCZhFvdhJUApRx/yuhATiwMjXiqJAg1hEO4GukVKeM39BSh+bp3TVljgurMY0kBPIZAACX02N
5w3HicXpJ0c4BFSQRs5rrxfQD6Rdbai2fOlzZCTey+h1+dqybuj4yqg0jzmAHAeAgJjGqd8FrpmL+efaNUBcTLKPSGFcG6F2uhFH2YB7HqRNT2E59qTCkgnZmvIWrwY8QrnltTJfNhRoAtF6+ti54Bazcih+oByUgarDeNn2YbR6c/wDf6NnO6Oxs6yA
6JxcUMj4yyc+cQvtUAkrKiuhiKTepWIpoPDb0fdEHjnfrmynL7fcqdBwCXg1MhxizX5hRsw16xQGEVtjJ49jHUNqMUsf5QuZZyIWAS+EQQMpHyIe+mQovKoXpWs5lDNh14vSQ1t2VeJwkkAm/D7JZlEg0gZlLlKXPTq5IeRKUFGvBDzaQLGpZeRJiQJW
wutlAYQhtUMzrp/AqfONdoP2O94urz/xA2DLxFHYQOjhy6kgd4H7PfhBuW2BX5im7jdSuE0cNo8RvpWuOFoz8S/VXo9LhM/Yj0FuCIEpFbMsjOfb5E1Hzz4g1PeWi79ZQJKavGUbWgm6PYONx2IBDoBvkDGcxLY/p0iXFVP2kzJ06+01uwvw0T+D+Vxz
tRk8HIfvDhUuB1dCfWu8WamaOp7vujyKzZVGBnrJrdGbMikCoRTySbb5MJhSjTQ4/UOYz+ta8PC9CQlW1MeUARlYm8QFQFgk89ndnz4w8Cs9bu5McN7d0tJC5U/k984hIRsA8nTbz6Y6gwXI0l8nhrVkpMl3OuJYvk6yyQO+3EdZiMqUjHavPblBl/8b
HfRQAOLgpNpS/YH3TrGOQGJ4HhZd0R8QrbupsvwUWEOZJrRg7NWz9IG/2+hHiunLhvfSxWvsbJRS2gIwa5L3b4fW4dbCnVrRu3hTOfKTDVmfx0P+l+stS9mG5jkU7etlbB8A4hBtv5NSmffNt4Z/WZ8slk6RCtqU4BYZ5RCLdemshEsm3oEH103yEuv8
srODOLoVzR8a+Wegu9e7vbD/6VeWHOY40lJa7lTzI6KV0Z5iTUeOAFcJiuwr9wPFvBr8hN5INimYLNG3PC8nOPvsLDrum519MJd7XISpRXKSFRpB3ghqYV7hLfnDz/Cffa6dmdMWlWxXa4PiA57HwxHsuNOY+oivrfX+lke7SFc0/cLCM+Dm2tsIV/v9
```

FIGURE 5 - CIPHER.TEXT (src-PROJECT IMPLEMENTATION)

5.Decryption of Image By Entering Key And Choosing Cipher File

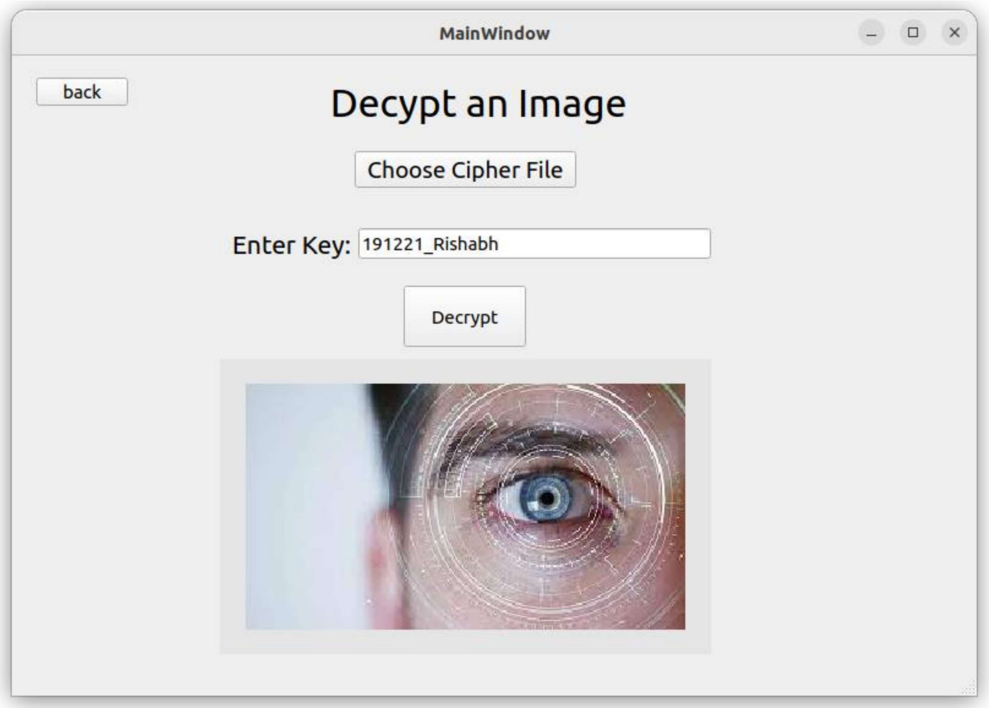


Decypt an Image

Enter Key: 191221_Rishabh

FIGURE 6 - DECRYPTION (src-PROJECT IMPLEMENTATION)

6.IMAGE RECOVERY



Decypt an Image

Enter Key: 191221_Rishabh

FIGURE 7 IMAGE RECOVERY(src -PROJECT IMPLEMENTATION)

4.3 Drawbacks

The key management required to utilise symmetric cyphers safely is a serious drawback. A separate key should preferably be shared by each unique pair of communication parties, and maybe for each ciphertext transferred as well. In order to keep them all reliable and hidden, an ever-large number of keys are needed, which rapidly necessitates complicated key management techniques.

Key Symmetric Exhaustion Every time a key is used in encryption, some information is "leaked" that an attacker may use to reassemble the key. The defense's against this behavior include the proper rotations of key that do encrypt large amounts of data as well as the usage of a key structure to prevent the abuse of master or key-encryption keys.

Data on attribution

Symmetric keys, in contrast to asymmetric certificates, lack embedded metadata to store data like the expiration date or a list of permissions to specify that the key may be used to encrypt but not decrypt, for example.

Standards that allow a key to be tied to information outlining its usage somewhat solve the latter problem. But a password-management system is necessary if you want complete control over how and when a key may be used.

Large-scale key management

When a scheme only uses a small number of keys, the management overhead is low and may be handled manually by humans. Tracking expiry dates and setting up a rotation of keys, however, rapidly becomes impossible with a big estate.

- Every block uses the same encryption scheme.
- If the AES key is not utilised correctly, a cryptanalytic attack may result. Key scheduling must be handled properly as a result.

Chapter 5 – Conclusion

5.1 Conclusion

We have developed a program that accurately encodes and decodes picture documents. This could help in reducing the problem of knowledge theft and breaches of other sensitive data. The record that we typically receive after coding is quite secure, and no one can extract anything from it. As a result, this document is given to a corporation without tension. Our devised arrangement may be a very little commitment that, in the present, could be highly useful in the medical or military domains.

An AES calculation execution is connected and re-specified for picture encoding and decoding using Python encoding. Even without rolls, significant photographs might be extensively redone. It has been demonstrated that the computations have a very secure key house and can withstand the majority of conventional attacks, such as the brutal power attack, figure attack, and plaintext attack.

To protect picture data from unauthorised access, image encoding and decoding using AES estimation is no longer necessary. One of the outstanding encryption and decryption features one may aspire for in the market is an effective implementation of AES symmetric key estimation.

5.2 Future Scope

To make the method more secure, one may be careful to choose a better key size, just as one may be careful to choose a larger information block to facilitate turnout. Even so, the extra area might have to be tolerated. In areas like media correspondence, a computation with an elevated level of security and throughput may thus realise optimal applications. Future research should concentrate on streamlining techniques for frameworks that permit flexible key lengths and activity ways. The schematic representation of the AES with 192- and 256-chance manner measures may be accessed with the 1-BOX procedures that were demonstrated. Finally, an effective global AES processor that satisfies the requirements for at-way dimensions may be distributed.

Future AES designs for 8-cycle data transfer might take the S-BOX conferring and pipelines framework into consideration. These strategies from ensuring mix to boot migration techniques may benefit other cryptography computations, notably over circular unrolled structures.

5.3 Applications

Samsung and other manufacturers of storage devices, popularly referred to as SSDs, employ the 256-bit AES algorithm.

The information we safeguard on Google Drive serves as an example of how AES is used. In the cloud, where customer information is kept and made available on Google, AES technology for encryption is employed. It makes use of an encryption algorithm with 256 bits, which is said to be more advanced and safer.

On Facebook and WhatsApp, the one-to-one conversation is securely transmitted as well as received using AES encryption with a strength of 256 bits.

The Microsoft BitLocker authentication method, which comes pre-installed with the Windows operating system, also makes use of the AES encryption techniques.

Data is processed using AES encryption on hard drives, self-encrypting programmes, and Iot of devices.

High-strength encryption in devicesmay have a potentially enormous market. Within the world of private correspondences, the seeming risk of spying is a significant commercial motivator. Expect important phone manufacturers like Nokia, Ericsson, Samsung, Motorola, TI, Casio, and others to join a group of modern businesses that want to deliver the IP. Once a major retailer introduces encryption for use with a regular phone, all other retailers are immediately forced to follow suit or risk losing customers to competition. The default speaking mode will be encryption in around 18 and a half years. Expect this quality to be included into every VoIP and landline phone system.

Network machines are one of the several supposedly Brobdingnagian markets for processed encoding. These are electronic devices that are naturally connected to an organisation. As more non-PC and distant devices connect to the internet, the frequency of cyberattacks against network infrastructure and specialised cooperatives will increase. Basic functions, including the board's power-framework and water-circulation frameworks, are moving online and will be protected. In fact, even basic devices like alarms or temperature warnings may be defenceless to engineer attacks. Keeping an engineer from electronically hollering "fire" comes at a high cost.

SSLS provides security for online program-based exchanges by utilising the Protected Attachment Layer convention; as a result, SSL is internet-specific. When deciding whether to build a web-based exchange or not, the availability of encoding on a website is frequently the deciding factor. No organisation has to lose revenue due to a lack of a secured association. It is essential to incorporate a resident SSL monitoring limiter within the server's farm for encryption and decipher traffic passing through the Site as transfer speed requirements increase.

Direct connections between customers and venture organisations are protected by VPNs. The high cost of dedicated telecommunication connections prevents changes in these connections' programming or instrumentation support. Although dedicated rent lines are quite private and safe, it would be very expensive to provide everyone a confidential line. Putting chaotic VPN traffic on open lines is far more cost-effective. - A business LAN should be able to complete and manage scrambled information streams within the gigabit range now, and in the multi-gigabit range shortly, despite the fact that few individual customers need a dedicated connection at Gbit/sec rates due to the growing number of VPN clients.

The High-level languages secret writing standard is used to bind remote organisations and confirm switches and degreed customers.

Wi-Fi organisations are currently utilised by default and have comprehensive code programming and security mechanisms with minimal weight in this computation. Coded Analysis: AES anticipates that a significant portion of clients and servers will need to approve the site server. This calculation helps with SSL/TLS encryption demonstrations to observe the highest level of safety and unending security and employs both spatially uniform and fuzzy encryption.

In addition to meeting organisational needs, AES is used to start encrypted file transfers between parties. Continue because corrupt chat messages, family photographs, and final reports are shared via encrypted data.

Security measures for processors: Discarded processor makers engage in enigmatic instrumentality-level compositions, employing every AES encryption similarity possible to boost security and frustrate attempts to prevent collapses. amid many low-key choices.

Chapter 6 - REFERENCES

[1] Jui-Cheng and Guo, “A New Chaotic Key-Based Design for Image Encryption and Decryption”, vol. 4, 2000, pp. 49-52. doi:10.1109/ISCAS.2000.858685.

[2] Lazhar “Zeghid, Medien & Machhout, Mohsen & Khriji,” World Acad. Sci. Eng. Technol., vol. 1, pp. 745-750, 2007. A Modified AES Based Algorithm for Image Encryption.

[3] P. R. Radhadevi, “Secure image encryption using AES,” Int. J. Res. Eng. Technol., vol. 01, no. 2, pp. 115-117, 2012. doi:10.15623/ijret.2012.0102006..

[4] R. Padate ., “Encryption and Decryption of Text Using AES Algorithm”, 2014/ vol. 6, no. 1, Jan., pp. 23-29, 2015.

[5] J. J. Amador and R. W. Green, “Symmetric-key block cipher for image and text cryptography,”, Int. J. Imaging Syst. Technol., vol. 15, no. 3, 178-188, 2005 [doi:10.1002/ima.20050].Pronika & Tyagi, S. (2021).

[6] “Performance analysis of encryption and decryption algorithm”, Indonesian Journal of Electrical Engineering and Computer Science. 23. 1030. 10.11591/ijeecs.v23.i2.pp1030-1038.

[7] Abdullah, Ako Muhamad. "Advanced encryption standard (AES) algorithm to encrypt and decrypt data." Cryptography and Network Security 16 (2017): 1-11.

[8] Arab, Alireza, Mohammad Javad Rostami, and Behnam Ghavami. "An image encryption method based on chaos system and AES algorithm." The Journal of Supercomputing 75.10 (2019): 6663-6682.

[9] Y. Yuan, Y. Yang, L. Wu and X. Zhang, "A High-Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation," 2018 IEEE International Conference on Electron Devices and Solid State Circuits (EDSSC), 2018, pp. 1-2, doi: 10.1109/EDSSC.2018.8487056.

[10] Groß, Hannes, Stefan Mangard, and Thomas Korak. "An efficient side-channel protected AES implementation with arbitrary protection order." Cryptographers' Track at the RSA Conference. Springer, Cham, 2017.

[11] F. J. D'souza and D. Panchal, "Advanced encryption standard (AES) security enhancement using hybrid approach," 2017 International Conference on Computing, Communication and Automation (ICCCA), 2017, pp. 647-652, doi: 10.1109/CCAA.2017.8229881.

[12] Daemen, Joan & Rijmen, Vincent. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. 10.1007/978-3-662-04722-4.

[13] Nechvatal J, Barker E, Bassham L, Burr W, Dworkin M, Foti J, Roback E. Report on the Development of the Advanced Encryption Standard (AES). J Res Natl Inst Stand Technol. 2001 Jun 1;106(3):511-77. doi: 10.6028/jres.106.023. PMID: 27500035; PMCID: PMC4863838