Excelssior Education Society's
K. C. College of Engineering & Management Studies & Research
Department of Computer Engineering

ENCRYPTION - DECRYPTION

(Caesar Cipher, Steganography)

GROUP MEMBERS

SAHIL A. SAWANT (B-17)

ADITYA P. SHINDE (B-25)

VINAYAK V. UTEKAR (B-42)

Under the Supervision of

Dr. POULAMI DAS ROY

OVERVIEW

- Introduction
- Literature Survey
- Problem finding and Motivation to the work
- Hardware and Software Requirements
- Methodology
- Proposed Techniques
- Results and Discussions
- Conclusion
- References

Introduction

- In cryptography, encryption is a process of encoding information. This process converts the original information into an alternative form known as ciphertext. Only authorized parties can decipher a ciphertext back to plaintext & access the original information.

- The conversion of encrypted data into its original form is called Decryption. If correct key / Password is provided, user will get the original information Generally text files, images, e-mail messages, user data and directories are encrypted.

- The word Steganography is derived from two Greek words- ‘stegos’ meaning ‘to cover’ and ‘grayfia’, meaning ‘writing’, thus translating to ‘covered writing’, or ‘hidden writing’.

- In this project we have used Caesar Cipher & Steganography. Which are most used technique and oldest for secret messaging and exchanging of confidential data

- Main difference is, Cryptography makes the data unreadable, or hides the meaning of the data, while Steganography hides the existence of the data.

Literature Survey

(Caesar Cipher)

Technique	Caesar Cipher
Person who introduced	Julius Caesar
Year	Around 100 BC
Specification	One of the earliest and widely used method for encryption messages.
Cipher type	Substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet.
Rotation Type	Mono-alphabetic Rotation
Example	If A is the 1st letter in message then with a shift of 1, A would be replaced by B, B would become C, and so on.
Representation	Modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25.
Encryption Formula	$E_n(x) = (x + n) mod\ 26$
Breaking cipher	Ciphertext-only scenario.
Decryption Formula	$D_n(x) = (x - n) mod\ 26$
Use for	Securing data and Secure messaging

Literature Survey

(Steganography)

Technology used	Python, Tkinter, Stegano
Technique	Steganography
Person who introduced	Johannes Trithemius
Year	1499
Specification	One of the earliest and widely used method for hiding existence messages.
Example	It is known that during both world wars, female spies used knitting to send messages, perhaps making an irregular stitch or leaving an intentional hole in the fabric.
Breaking stegano	Same as that of encryption but reverse.
Representation	Every text is distributed into 3 pixels, and after every 3 pixel a binary number is added which hides the given text
Use for	Securing / hiding the confidential text or data existence.
Problem solved	Cyber attacks, Secure data transfer and also Securing confidential information

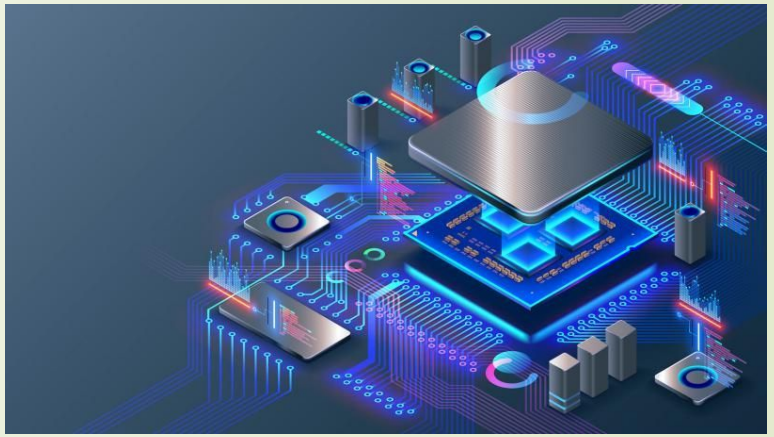
Problem Statement

How to secure your information from unauthorized access?

Secure message/ data transfer.

Encoder-Decoder – Secures your Information by Encoding the messages.

Hardware Requirements



SYSTEM :- INTEL CORE I3 (Min)
HARD DISK :- 512 GB
MONITOR : STANDARD LED MONITOR
INPUT DEVICES :- KEYBOARD
RAM:- 4 GB AND ABOVE
PROCESSOR : x32bit, x64 bit

Software Requirements

OPERATING SYSTEM :- WINDOWS 7 (Min)
PROGRAMMING LANGUAGE :- PYTHON
CODE EDITOR :- VS CODE / ATOM
LIBRARIES USED :- TKINTER & STEGANO

Methodology

- Import tkinter, numpy libraries.
- Initialized window to cover the whole screen.
- Added labels, input fields and buttons.
- Created a function **encrypt()** to encode the input string entered by user.
- Ask the user to provide a **key** which will help to decode the text while decrypting.
- Created a function **decrypt()** to decode the the encrypted text.
- If the user will enter same key used while encrypting text, it will show the decoded text.
- Click "**Show Result**" button to get the encoded text.

Methodology

- Import tkinter, stegano libraries.
- Initialized window to cover the whole screen.
- Added labels, input fields and buttons.
- Created a function **encode()** to encode the message and hide it into an image.
- A copy of that image will get downloaded in user's system.
- Created a function **decrypt()** to decode the encrypted image.
- Click "**Go**" button to get the encoded text.

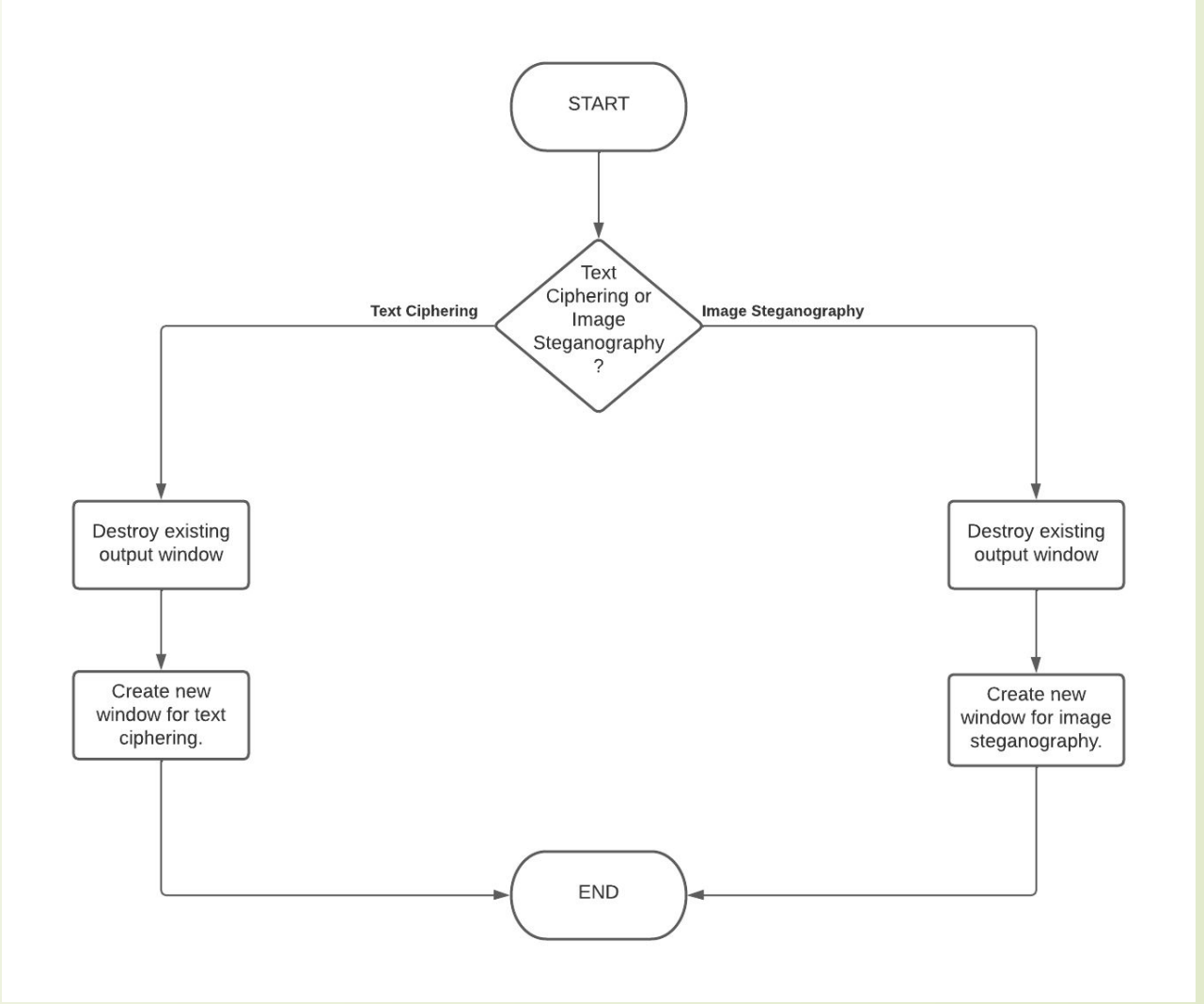
Algorithm

STEP 1 : START
STEP 2 : Initialize window.
STEP 3 : Enter name, key and message.
STEP 4 : Type ‘e’ to encrypt code in mode input field.
STEP 5 : Click on “Show Message” button for result.
STEP 6 : Copy the encrypted message.
STEP 7 : Click on “Reset” button.
STEP 8 : Now, Enter name, key, message and type ‘d’ to decrypt code.
STEP 9 : Click on “Show Message” button for result.
STEP 10 : Click on “Exit” button to exit program.
STEP 11 : STOP

Algorithm

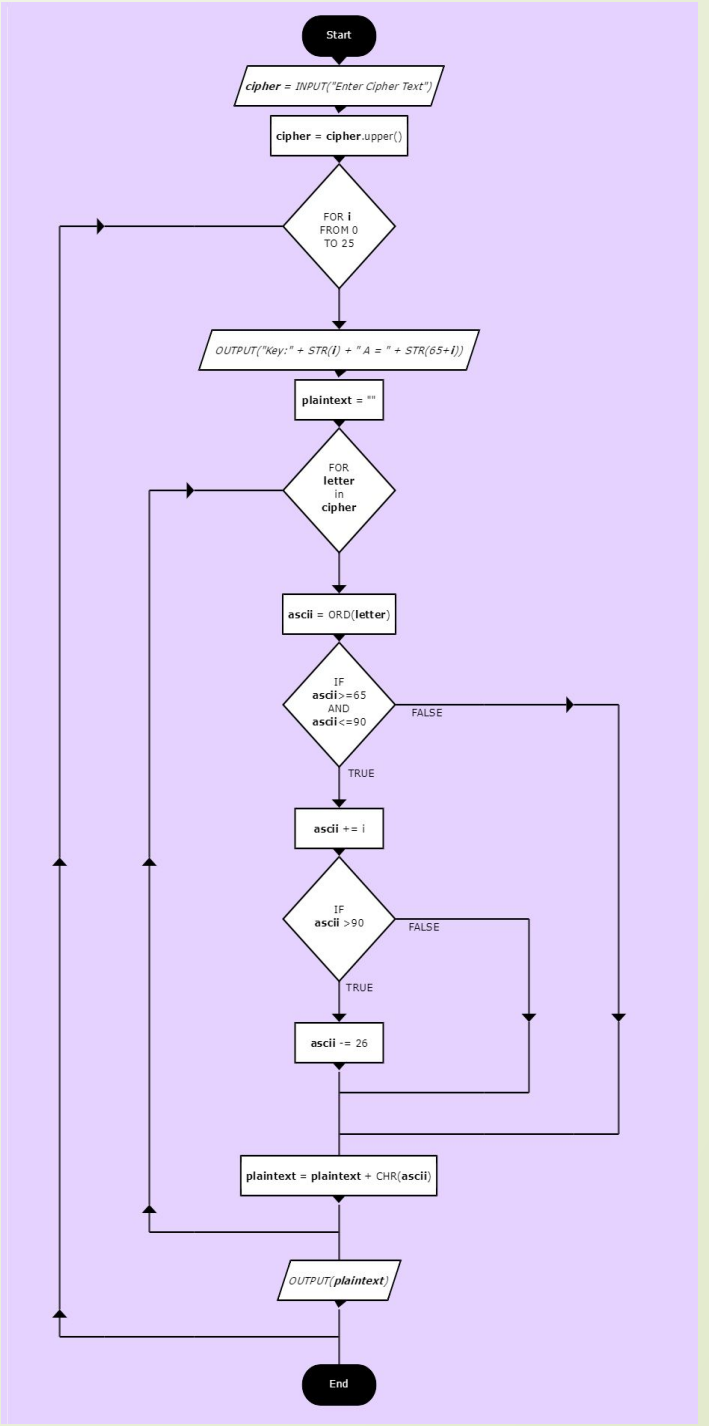
STEP 1 : START
STEP 2 : Initialize window.
STEP 3 : Enter message and upload address of cover image.
STEP 4 : Type ‘e’ to encrypt code in mode input field.
STEP 5 : Click on “Go” button to encode.
STEP 6 : Now, upload the encoded cover image.
STEP 7 : Type ‘d’ to decrypt code in mode input field.
STEP 8 : Click on “Go” button.
STEP 9 : STOP

Flowchart

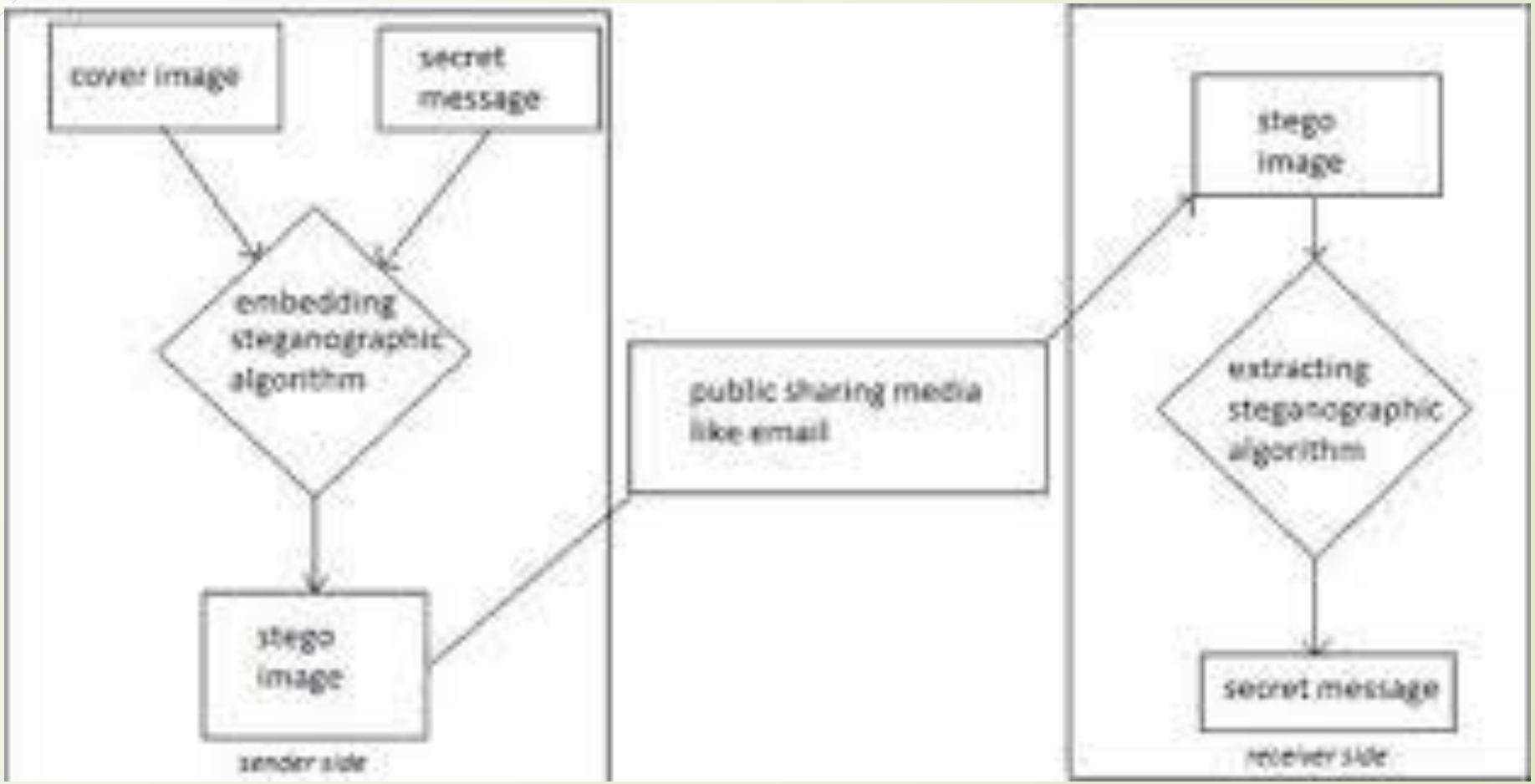

START
Text Ciphering or Image Steganography ?
Text Ciphering
Image Steganography
Destroy existing output window
Create new window for text ciphering.
Destroy existing output window
Create new window for image steganography.
END

Flowchart :

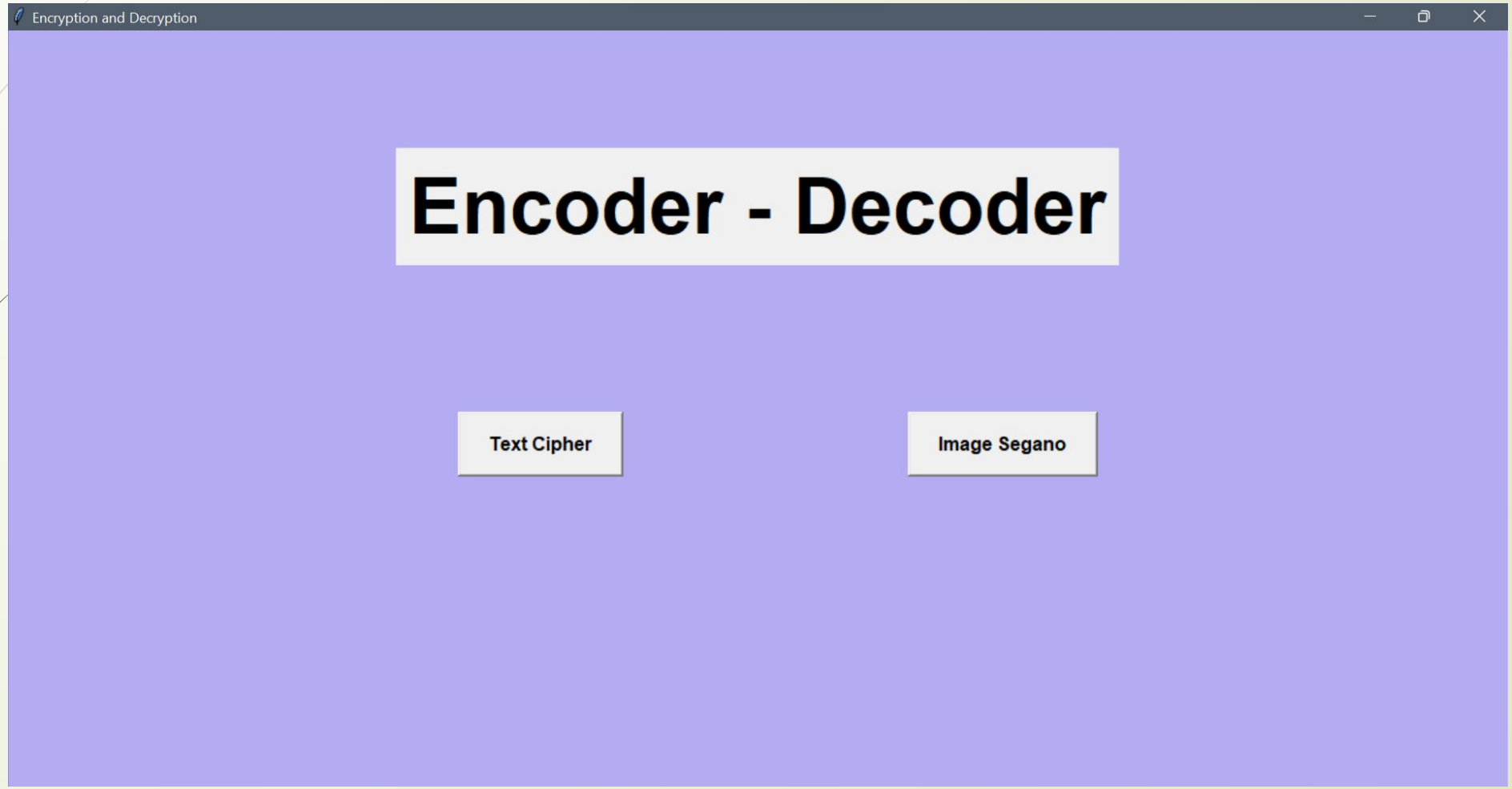
(Caesar Cipher)



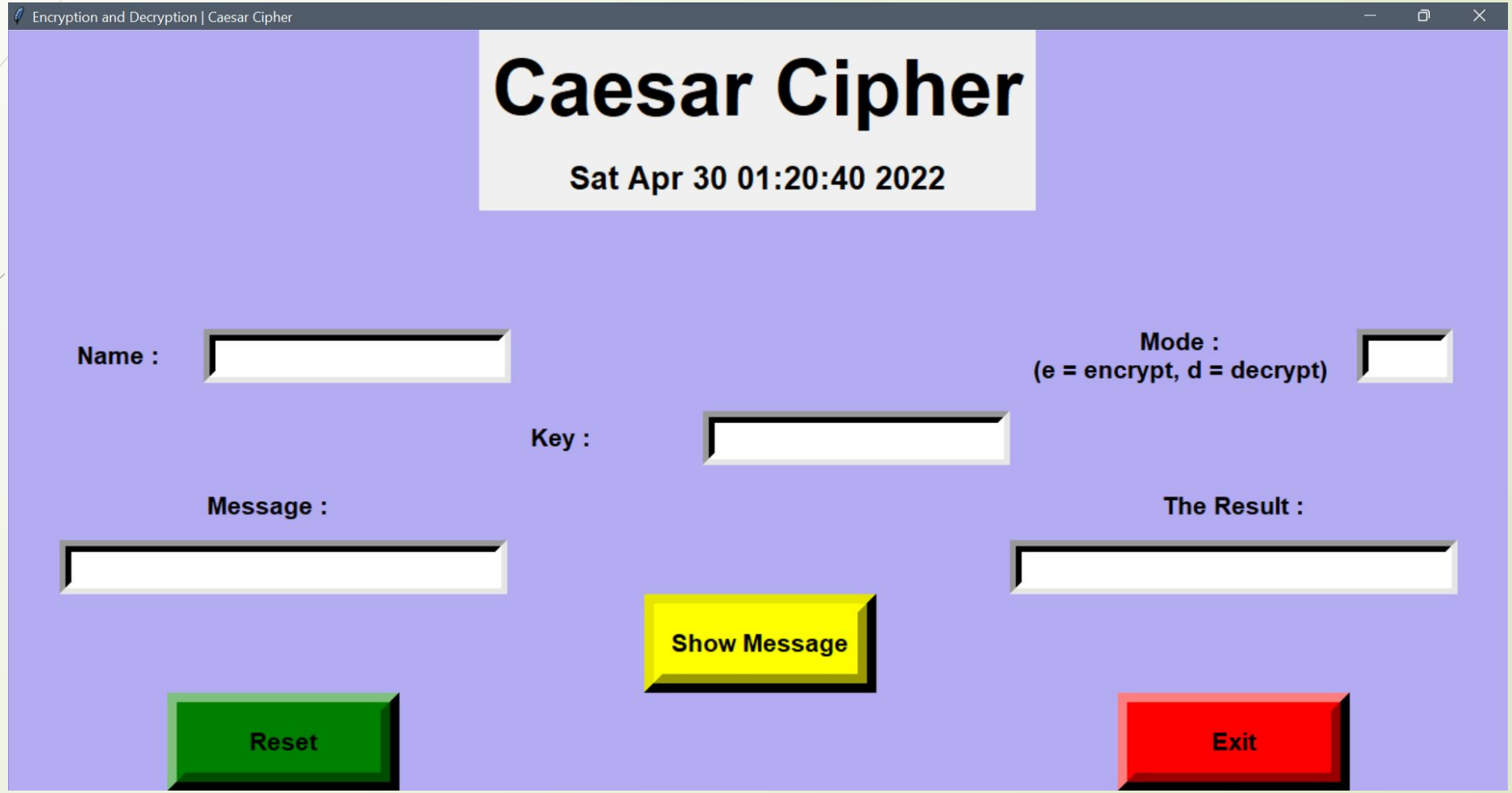
Flowchart : (Steganography)



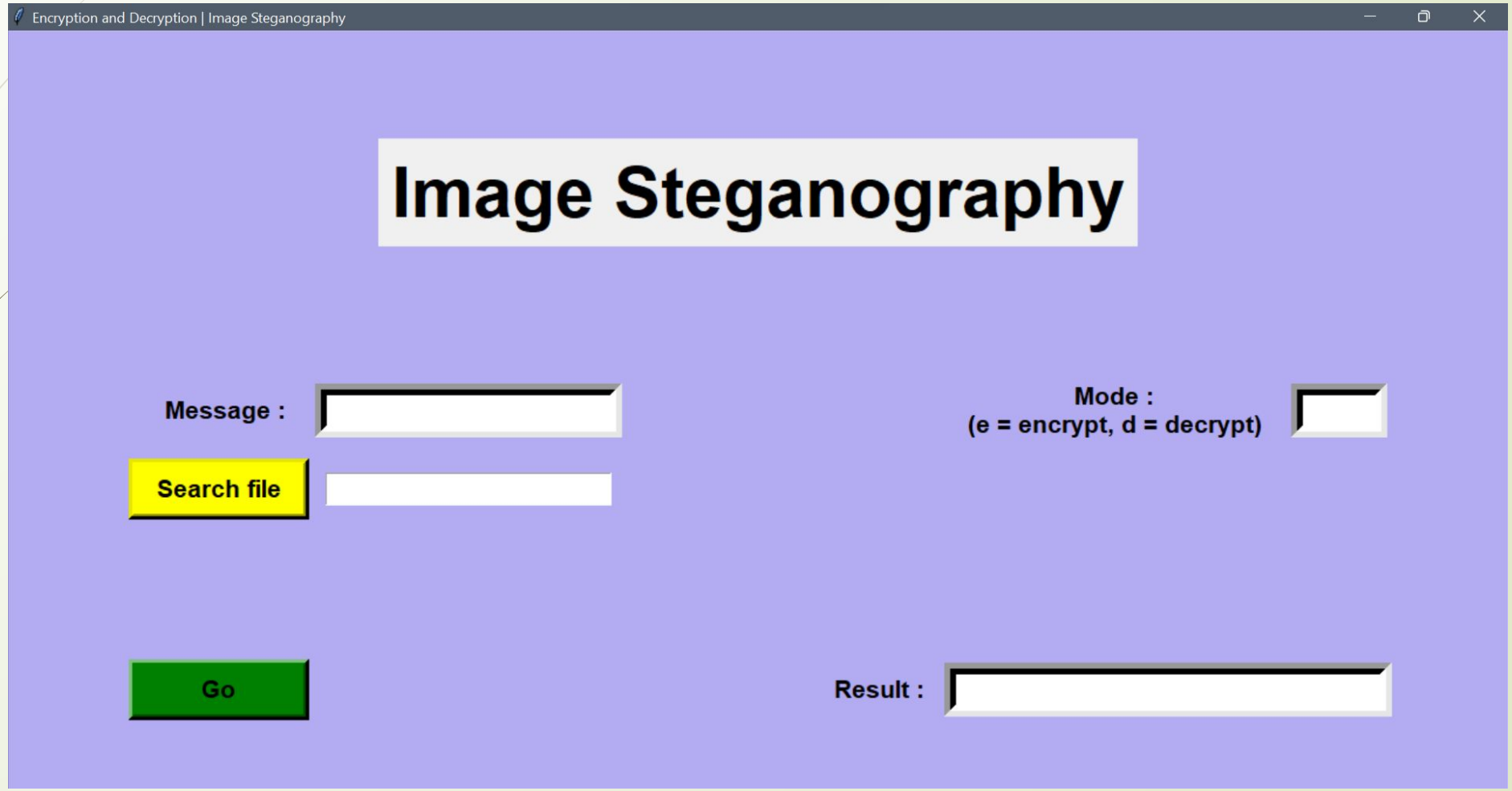
Results (Main Frame) :



Results (Caesar Cipher) :



Results (Steganography) :



Advantages

Encryption Provides Security for Data at All Times:
Generally, data is most vulnerable when it is being moved from one location to another. Encryption works during data transport or at rest, making it an ideal solution no matter where data is stored or how it is used.

Encryption Protects Privacy:
Encryption is used to protect sensitive data, including personal information for individuals. This helps to ensure anonymity and privacy, reducing opportunities for surveillance by both criminals and government agencies. Encryption technology is so powerful that some governments are attempting to put limits on the effectiveness of encryption—which does not ensure privacy for companies or individuals.

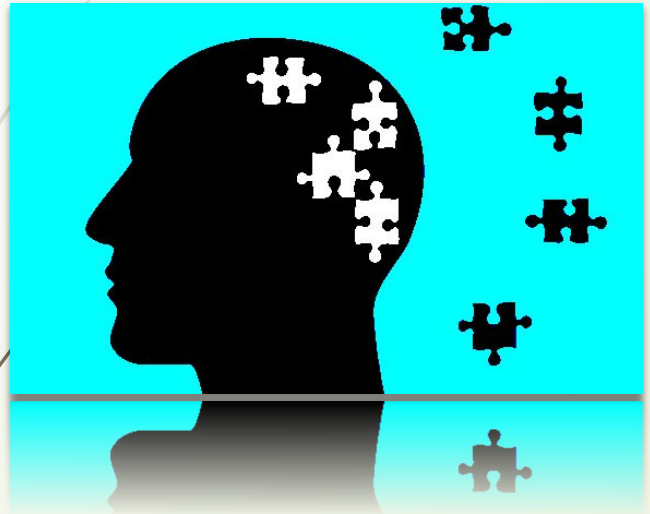
Encrypted Data Maintains Integrity:
Hackers don't just steal information, they also can benefit from altering data to commit fraud. While it is possible for skilled individuals to alter encrypted data, recipients of the data will be able to detect the corruption, which allows for a quick response to the cyber-attack.

Time complexity of the cipher is O(n):
Which means that running time increases at most linearly with the size of input.

Limitations

Forgetting Passwords/Key:

General most of the people forget the password/keys so they find difficulties to access the message or data.



Requiring Cooperation:

Using encrypted files that are designed to be opened and shared by two or more people can be disadvantageous when one or more participants finds it a burden to use encryption.

Developing a False Sense of Security:

A disadvantage of encrypted files is that relying on them to keep things secret could lull you into a false sense of security. A determined person may marshal overwhelming computer resources to decrypt your secret files.

Applications

1)**Encryption/Decryption in emai**l: Email encryption is a method of securing the content of emails from anyone outside of the email conversation looking to obtain a participant's information. In its encrypted form, an email is no longer readable by a human. Only with your private email key can your emails be unlocked and decrypted back into the original message.

2) **Defense Government Organizations**- to facilitate secret communication

3) **For sending highly confidential message or details on Social Media like Card details or Bank Information**.

4) **Encryption is also used to protect data in transi**t, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years.

Applications

5)**Encryption can be used to protect data "at rest"**, such as information stored on computers and storage devices (e.g. USB flash drives). In recent years, there have been numerous reports of confidential data, such as customers' personal records, being exposed through loss or theft of laptops or backup drives; encrypting such files at rest helps protect them if physical security measures fail

6) **Digital rights management systems**, which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering (see also copy protection), is another somewhat different example of using encryption on data at rest.

Future Scope

1. More encoding cipher options could be added such as ADVANCED ENCRYPTION STANDARD (AES), TRIPLE DES (DATA ENCRYPTION STANDARD).

2. More secure and user oriented encryption can be done

3. It will be used in all purpose such as Internet banking, Sharing Personal details,
   Military & Defence connections and also identifing Terrorist threats ,
   Securing your data in own devices more safely,

Conclusion

- Early encryption techniques were often utilized in military messaging. Since then, new techniques have emerged and become common place in all areas of modern computing.In today's world as Cyber Attacks have grown in large number there is a need to secure our data.

- Thus, we have successfully developed an Encoder-Decoder project in Python. We used the popular tkinter library & stegano library for rendering graphics on a display window and encoded - decoded using the Ceasar Cipher method & Steganography for encrypting. In this way, we can encode our message and decode the encoded message in a secure way by using the Password key

References

1) Tkinter library:
https://docs.python.org/3/library/tkinter.html
https://www.tutorialspoint.com/python/python_gui_programming.htm#%20:~:text=Tkinter%20is%20the%20standard%20GUI,to%20the%20Tk%%2020GUI%20toolkit.&text=Import%20the%20Tkinter%20module

2)Cesar Cipher:
https://en.wikipedia.org/wiki/Caesar_cipher
https://cryptography.fandom.com/wiki/Caesar_cipher

3)Steganography:
https://en.wikipedia.org/wiki/Steganography
https://www.techtarget.com/searchsecurity/definition/steganography

THANK YOU