

A Project Report
On
TEXT ENCRYPTION AND DECRYPTION

Submitted by
Adib Shaikh
Husen Shaikh

In partial fulfillment for the award of the degree of
Bachelor of Technology
IN
Computer Science and Engineering



Pradnya Niketan Education Society, Pune.
NAGESH KARAJAGI *ORCHID* COLLEGE OF
ENGINEERING & TECHNOLOGY
SOLAPUR.

2022-2023



Pradnya Niketan Education Society , Pune.
NAGESH KARAJAGI ORCHID COLLEGE OF ENGG. & TECH.,
SOLAPUR.

Gut No. 16, Solapur-Tuljapur Road, Tale Hipparaga, Solapur – 413 002
Phone: (0217) 2735001/02, Fax. (0217) 2735004

Certificate

This is to certify that Mr. Adib Shaikh of class TE-B Roll No.51 has satisfactorily completed the Project work entitled Encryption and Decryption using Cryptography Algorithm as prescribed by Dr.Babasaheb Ambedkar Technological University Lonere, Maharashtra, India in the academic year 2022-23.

Date of Submission: 24-12-2022

Project Guide

Head of Department

Examiners:

1 : _____

2 : _____



Pradnya Niketan Education Society , Pune.
NAGESH KARAJAGI ORCHID COLLEGE OF ENGG. & TECH.,
SOLAPUR.

Gut No. 16, Solapur-Tuljapur Road, Tale Hipparaga, Solapur – 413 002
Phone: (0217) 2735001/02, Fax. (0217) 2735004

Certificate

This is to certify that Mr. Husen Shaikh of class TE-B Roll No. 52 has satisfactorily completed the Project work entitled Encryption and Decryption using Cryptography Algorithm as prescribed by Dr. Babasaheb Ambedkar Technological University Lonere, Maharashtra, India in the academic year 2022-23.

Date of Submission: 24-12-2022

Project Guide

Head of Department

Examiners:

1 :

2 : _

ACKNOWLEDGEMENT

We are thankful to Department of computer science & Engineering, Nagesh Karajgi Orchid College of Engineering & Technology, Solapur for giving us opportunity to undertake project in their organization.

We would like to mention our sincere gratitude's towards our Principal Dr. J. B. Dafedar and H.O.D Prof. V. V.Bag, Computer Science and Engineering Department, for giving us this opportunity to carry out this project. We take this opportunity to express our sincere thanks to our guide Prof. V. V.Bag for his guidance and encouragement.

We are thankful to our guide Prof. V. V.Bag for his guidance at every step throughout our project report. Finally, we take this opportunity to mention our sincere thanks to one and all those who helped us directly and indirectly in the completion of this project report.

Mr. Adib Shaikh

Mr. Husen Shaikh

ABSTRACT

Securing data encryption and decryption using Cryptography and Steganography techniques. Due to recent developments in stego analysis, providing security to personal contents, messages, or digital images using steganography has become difficult. By using stego analysis, one can easily reveal existence of hidden information in carrier files. This project introduces a novel steganographic approach for communication between two private parties. The approach introduced in this project makes use of both steganographic as well as cryptographic techniques. In Cryptography we are using RSA. In Steganography we are using Image Steganography for hiding the data. And we also use Mutual Authentication process to satisfy all services in Cryptography i.e., Access Control, Confidentiality, Integrity, Authentication. In this way we can maintain the data more securely. Since we use RSA algorithm for securing the data and again on this, we perform Steganography to hide the data. Such that any other person in the network cannot access the data present in the network. Only the sender and receiver can retrieve the message from the data.

LIST OF FIGURES

Figure No.	Name of the figure	Page No.
1.1	Cryptography	1
1.2	Symmetric Cryptography	2
1.3	Asymmetric Cryptography	3
3.1	Structure Architecture	9
3.2	Proposed System	10
4.1	Class Diagram	15
4.2	Use Case Diagram	16
4.3	Sequence Diagram	17
4.4	Activity Diagram	18

TABLE OF CONTENTS

ABSTRACT

LIST OF FIGURES

1. INTRODUCTION

1.1 Introduction	1
1.1.1 Cryptography	1
1.1.2 Types of Cryptography	2
1.1.3 How does Cryptography works?	4
1.1.4 Examples of Cryptography	5
1.1.5 Applications of Cryptography	5
1.2 Motivation for the work	6
1.3 Problem Statement	6
1.4 Organizational of Thesis	7

2. LITERATURE SURVEY

3. METHODOOGY

3.1 System Architecture	9
3.2 Proposed System	10
3.2.1 Sender Side	11
3.2.2 Receiver Side	11
3.3 Module Division	12
3.3.1 Base64	12
3.3.2 RSA	13

4. DESIGN	14
4.1 Class Diagram	15
4.2 Use Case Diagram	16
4.3 Sequence Diagram	17
4.4 Activity Diagram	18
5. EXPERIMENTAL ANALYSIS AND RESULTS	
5.1 System Configuration	19
5.1.1 Software Requirements	19
5.2.2 Hardware Requirements	19
5.2 Sample Code	20
5.3 Results	22
6. CONCLUSION	23
7. REFERENCES	24

1. INTRODUCTION

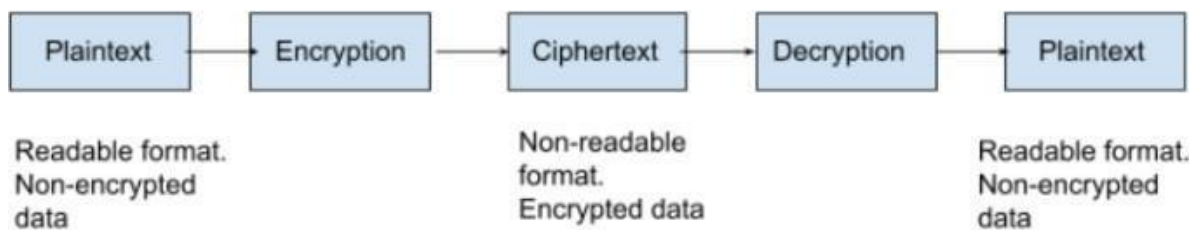
1.1 Introduction

Digital communication witnesses a noticeable and continuous development in many applications in the Internet. Hence, secure communication sessions must be provided. The security of data transmitted across a global network has turned into a key factor on the network performance measures. So, the confidentiality and the integrity of data are needed to prevent eavesdroppers from accessing and using transmitted data. Steganography and Cryptography are two important techniques that are used to provide network security.

The aim of this project is to develop a new approach to hiding a secret information in a message, by taking advantage of benefits of combining cryptography and steganography.

1.1.1 Cryptography

Cryptography is one of the traditional methods used to guarantee the privacy of communication between parties. This method is the art of secret writing, which is used to encrypt the plaintext with a key into ciphertext to be transferred between parties on an insecure channel. Using a valid key, the ciphertext can be decrypted to the original plaintext. Without the knowledge of the key, nobody can retrieve the plaintext. Cryptography plays an essential role in many factors required for secure communication across an insecure channel, like confidentiality, privacy, non-repudiation, key exchange, and authentication.



Cryptography

Fig 1.1

1.1.1.1 Symmetric / Secret Key Cryptography

The technique of Secret key encryption can also be known as the symmetric-key, shared key, single-key, and eventually private-key encryption. The technique of private key uses for all sides encryption and decryption of secret data. The original information or plaintext is encrypted with a key by the sender side also the similarly key is used by the receiver to decrypt a message to obtain the plaintext. the key will be known only by a people who are authorized to the encryption/decryption.

However, the technique affords the good security for transmission but there is a difficulty with the distribution of the key. If one stole or explore the key he can get whole data without any difficulty. An example of Symmetric-Key is DES Algorithm.

Because there is only one key for encryption and decryption, the symmetric key system has one major disadvantage: the two parties must exchange the key in a secure manner. An example of symmetric key cryptography is Blowfish.

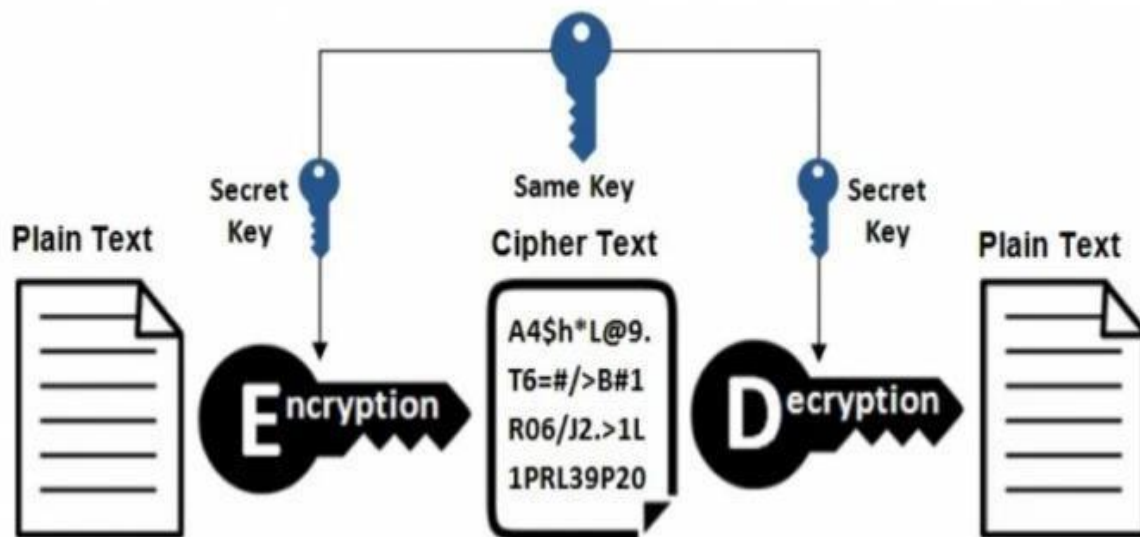


Fig 1.2

1.1.1.2 Asymmetric / Public Key Cryptography

We can call this technique as asymmetric cryptosystem or public key cryptosystem, this technique use, two keys which are mathematically associated, use separately for encrypting and decrypting the information. In this technique, when we use the private key, there are no possibilities to obtain the data or simply discover the other key.

The key used for encryption is stored public therefore it's called public key, and the decryption key is stored secret and called private key. An example of Asymmetric-Key Algorithm is RSA.

This cryptography differs from and is more secure than symmetric key cryptography. In this system, each user encrypts and decrypts using two keys or a pair of keys (private key and public key). Each user keeps the private key secret and the public key is distributed across the network so that anyone can use those public keys to send a message to any other user. You can use any of those keys to encrypt the message and can use the remaining key for decryption. An RSA algorithm is an example of asymmetric key cryptography.

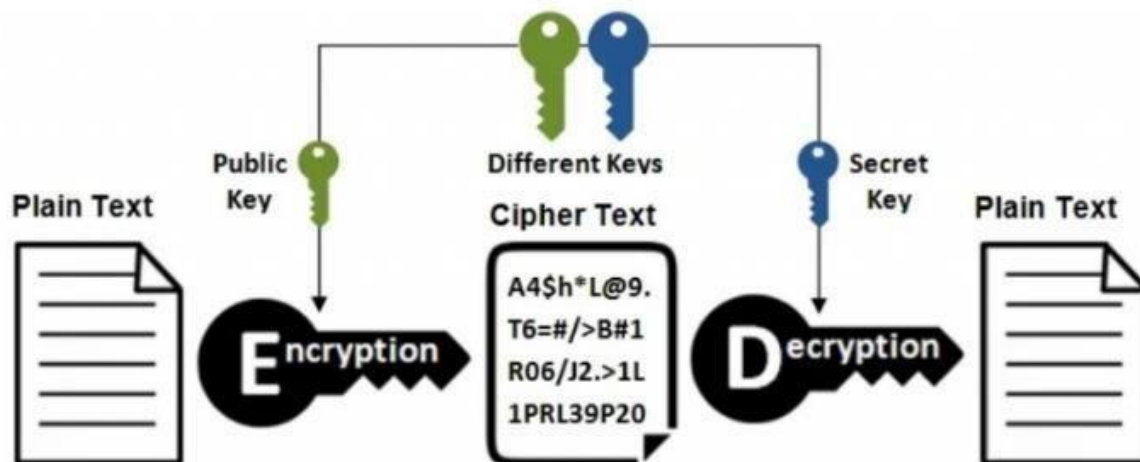


Fig 1.3

1.1.1.3 Hash Function

This algorithm makes no use of any keys. A hash value with a fixed length is calculated based on the plain text, making it impossible to recover the plain text's contents. Many operating systems encrypt passwords using hash functions.

1.1.2 Types of Cryptography Algorithm

Cryptographic algorithms are primarily of two types, and you can use them for critical tasks, such as authentication, data encryption, and digital signatures.

RSA: RSA is an asymmetric cryptographic algorithm based on the block cipher principle. It converts plain text to ciphertext at the receiver end and vice versa. If we use User A's public key for encryption, we must use the same user's private key for decryption.

DES: Data Encryption Standard (DES) is a symmetric cipher algorithm that encrypts and decrypts data using the block cipher method. The algorithm uses 48-bit keys to convert the plain text in 64-bit blocks into ciphertext. It operates on the Feistel Cipher Structure.

1.1.3 How Does Cryptography Work?

Cryptographic algorithms are central to how cryptography works. Cryptographic algorithms, also called ciphers, are mathematical functions that encrypt text by combining them with keys such as phrases, digits, words, and so on. You can define the effectiveness by the strength of the cryptographic algorithms and the level of key secrecy.

1.1.4 Examples of Cryptography

End-to-end encryption in WhatsApp is a prominent example of cryptography encryption these days. This feature is available in WhatsApp via the asymmetry model or public key methods. Only the intended recipient is aware of the actual message. After the WhatsApp installation, the server registers the public keys, and messages are transmitted.

Digital signatures are the next real-time application of cryptography. When two clients must sign documents for a business transaction. However, if two clients never meet, they may not believe each other. The use of encryption in digital signatures then ensures improved authentication and security.

1.1.6 Applications of Cryptography

There are various applications of cryptography. Some of those applications are:

Confidentiality: Cryptography allows users to store encrypted data, avoiding the major flaw of hacker circumvention.

Non-repudiation: The creator/sender of information cannot later deny his intent to send information.

Authentication: Helps to authenticate the sender and receiver's identities along with the destination and origin of the information.

Integrity: Information cannot be altered during storage or in transit between the sender and the intended receiver without any addition to the information being detected.

1.2 MOTIVATION FOR THE WORK

Motivation is very important function for any project. It is one of the methods to induce the man on the job to get the work done effectively to have the best results towards the common objectives. It is necessary for the better performance.

Motivation can be seen as the inner drive, which prompts people to act in a way either towards achieving their personal goals or organizational goals. To a large extent, motivation is “leadership” as it involves getting the whole staff to learn to work willingly and well in the interest of the business. A leader can influence his subordinate only when they are convinced.

Conviction can only come when the entire subordinate accepts those factors that propel actions of individuals, which are referred to as motivation. They may be highly paid, prestigious titles promotion, praises, bonus, etc. The word is an abstract noun applying to the entire class of desired need wishes and similar forces. Motivation has to do with action which results, to satisfaction closely associated with motivation is the word “miracle” it is injecting of moral and loyalty into the working team so that they will carry their duties properly and effectively with maximum economy.

1.3 PROBLEM STATEMENT

The purpose of this project is to provide the correct data with security to the users. For some of the users the data might be lost during the transmission process in the network and for some, the data might be changed by the unauthorized person in the network and there are some other security problems in the network. Our application will give you more Security to the data present in the network and there will be able to reduce the loss of data in the network which will be transmitted from the sender to the receiver using the latest technologies. Only the Authorized persons i.e., who are using our application will be there in the Network.

1.4 ORGANIZATION OF THESIS

The organization of this thesis is as follows:

Chapter-1: This chapter starts with an Introduction which highlights the problems under investigation by describing the status of problem conceptually and theoretically. It contains the introduction of the thesis, problem statement and scope of study, objective of the project, and the chapter organization.

Chapter-2: This chapter is a Literature Review that compiles the studies done by others based on the title of the project. Under the literature review, this chapter discussed on the features need to be include in designing the system.

Chapter-3: The methodology chapter describes the steps that has been taken while doing the project from the beginning until the end. The main content of the chapter are the flow charts and the description of each step of the process.

Chapter-4: This chapter presents the result of the algorithm and discussion observed. The results obtained are presented as a series of figures, tables, with textual description and discussion. The analysis outcome of the research is also discussed in relation to the evidences obtained from project work and theories reported in Literature Review .

Chapter-5: The chapter is the Conclusion of the thesis and which signalized the whole project a done

2. LITERATURE SURVEY

As we said the significance of network security is increased day by day as the size of data being transferred across the Internet. This issue pushes the researchers to do many studies to increase the ability to solve security issues. A solution for this issue is using the advantage of cryptography and steganography combined in one system. Many studies propose methods to combine cryptography with steganography systems in one system. This Project has been implemented on the basis of the requirements of security i.e authentication, confidentiality, and robustness.

There has been a continuous rise in the number of data security threats in the recent past and it has become a matter of concern for the security experts. Cryptography and steganography are the best techniques to nullify this threat. The researchers today are proposing a blended approach of both techniques because a higher level of security is achieved when both techniques are used together.

In proposed an encrypting technique by combining cryptography and steganography techniques to hide the data. In cryptography process, we proposed an effective technique for data encryption using one's complement method. It used an Asymmetric key method where both sender and receiver share the Secret key for encryption and decryption. In steganography part, we used the LSB method that is used and mostly preferred.

We present a method based on combining both the strong encrypting algorithm and steganographic technique to make the communication of confidential information safe, secure and extremely hard to decode. An encryption technique is employed for encrypting a secret message into a Cipher text using the Senders Private Key and receiver public key. The Cipher Text is finally embedded and transferred securely to deliver the secret information. They utilized a least significant bit method to accomplish the steganography.

At the receiver's side, the secret data is retrieved through the decoding process. Thus, a three-level security has been rendered for them a secret message to be transferred.

3. METHODOLOGY

3.1 SYSTEM ARCHITECTURE

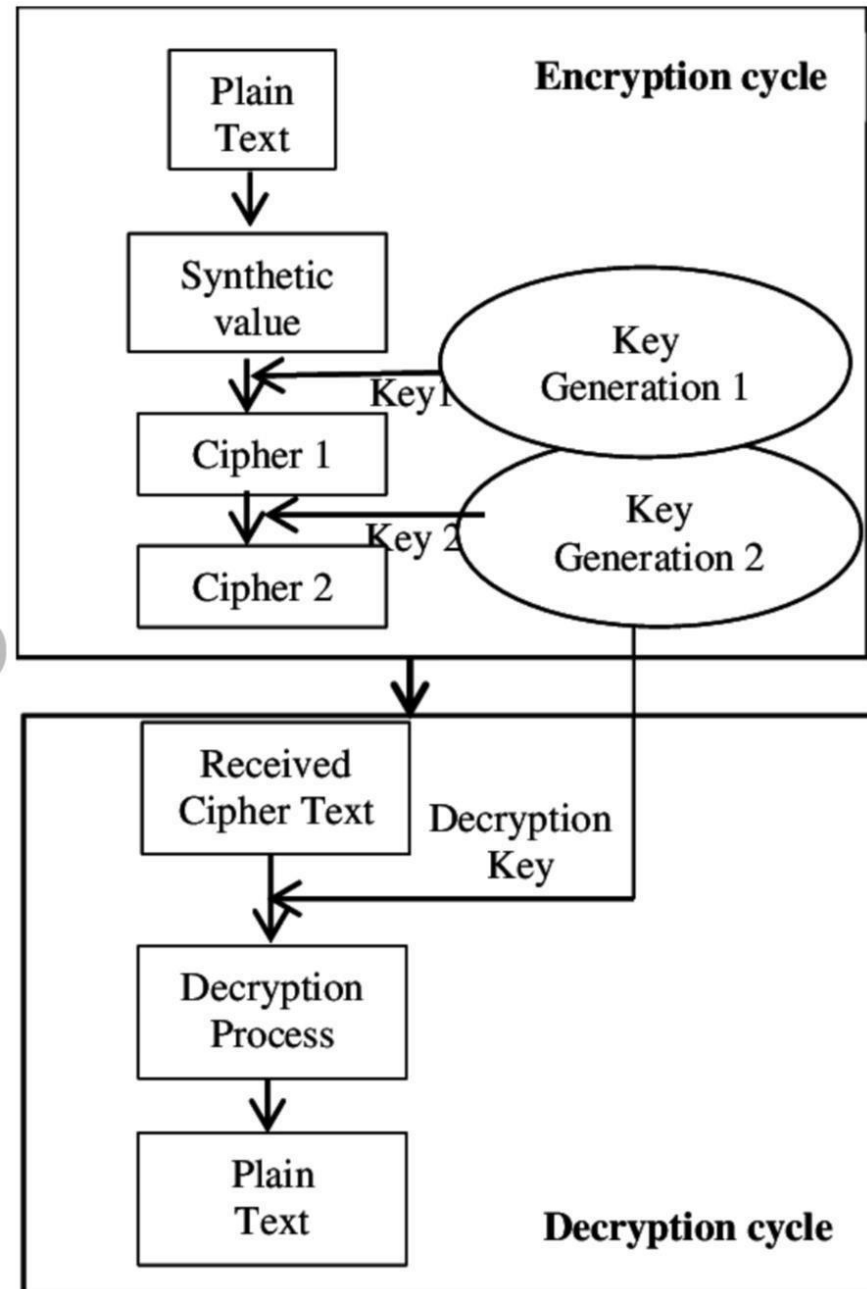


Fig 3.1 System Architecture

3.2 Proposed System

The proposed system suggests a new method of how the files are stored in the cloud by applying the existing encryption method and cloud computing system. Most users are not comfortable by knowing that their extremely private or confidential files can be accessed for various purposes by the cloud Server providers. This could be for maintenance purposes, security thread claims or even regular file backup processes. Normally, these reasons are complete valid in order to protect the cloud Server status and performance.

However, users are reluctant to upload their confidential files into cloud servers. This proposed system aims to fill this gap by providing an advanced level of file protection. RSA is known to be the strongest publicly available encryption method. This algorithm works with both private key and public key. The only way of decrypting the files which are encrypted with the public key is to use the private key. Users' file will be encrypted right before the upload process to the cloud Server. Only the encrypted file will be uploaded to the Server.

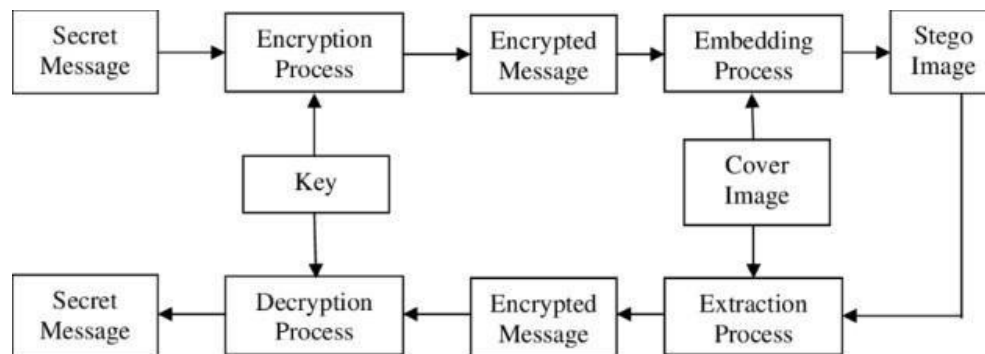


Fig 3.2

Before applying the cryptography, initially we convert our input to Base-64. And we save the obtained text in a text file. Then we proceed to cryptography.

3.2.1 Sender Side

The Sender side consists of cryptographic stages.

Cryptography Stage:

In encryption stage, we use RSA (Rivest Shamir Adelson) algorithm. This technique takes two prime numbers. The Encryption can be done using the Plain Text and with “e” values which was generated using the two prime numbers. Then we will get a cipher text, which is communicated to the receiving end for decryption. This encrypted data will be used in steganography stage.

Input= Message + Two Prime Numbers

Output= Encrypted Message

3.2.2 Receiver side

Receiver side consists of cryptography stages. In receiver side we will first extract embedded data then decrypt it.

Cryptography Stage:

In cryptography stage, we use the data which is extracted from file and use RSA. We will use the same steps which are used in sender side. The Decryption can be done using the Encrypted message, receivers private key and senders public key.

Input= Encrypted Message + 2 Prime Numbers

Output= Plain Text

Now the Plain Text is in the form of Base-64. After getting the plain text apply Base-64 conversion to change the Plain-text to given input, which can be Text.

3.3 MODULE DIVISION

3.3.1 Base-64

Base 64 is an encoding scheme that converts binary data into text format so that encoded textual data can be easily transported over network un-corrupted and without any data loss. Base64 is used commonly in a number of applications including email via MIME, and storing complex data in XML. Problem with sending normal binary data to a network is that bits can be misinterpreted by underlying protocols, produce incorrect data at receiving node and that is why we use this method. The term Base64 is taken from the Multipurpose Internet Mail Extension (MIME) standard, which is widely used for HTTP and XML, and was originally developed for encoding email attachments for transmission.

3.3.1.1 Why Do We Use Base64?

Base64 is very important for binary data representation, such that it allows binary data to be represented in a way that looks and acts as plain text, which makes it more reliable to be stored in databases, sent in emails, or used in text-based format such as XML. Base64 is basically used for representing data in an ASCII string format.

3.3.1.2 Base64 Encoding

Base64 encoding is the process of converting binary data into a limited character set of 64 characters. The characters are A-Z, a-z, 0-9, +, and / . This character set is considered the most common character set, and is referred to as MIME's Base64. It uses A-Z, a-z, 0-9, +, and / for the first 62 values, and +, and / for the last two values. The Base64 encoded data ends up being longer than the original data, so that, for every 3 bytes of binary data, there are at least 4 bytes of Base64 encoded data. This is due to the fact that we are squeezing the data into a smaller set of characters.

3.3.2 RSA

The RSA algorithm is the basis of a cryptosystem a suite of cryptographic algorithms that are used for specific security services which enables public key encryption and is widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet. RSA was first publicly described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology, though the 1973 creation of a public key algorithm by British mathematician Clifford Cocks was kept classified by the U.K.'s GCHQ until 1997.

In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm, It provides a method to assure the confidentiality, integrity, authenticity, and non-repudiation of electronic communications and data storage.

3.3.2.1 Why RSA Algorithm is used?

The public and private key generation algorithm is the most complex part of RSA cryptography. Two large prime numbers, p and q , are selected. N is calculated by multiplying p and q . This number is used by both the public and private keys and provides the link between them. Its length, usually expressed in bits, is called the key length.

The public key consists of the modulus n and a public exponent e . The e doesn't have to be a secretly selected prime number, as the public key is shared with everyone.

The private key consists of the modulus n and the private exponent d , which is calculated using the Extended Euclidean algorithm to find the multiplicative inverse with respect to the totient of n .

4. DESIGN

Project design is a major step towards a successful project. A project design is a strategic organization of ideas, materials and processes for the purpose of achieving a goal. Project managers rely on a good design to avoid pitfalls and provide parameters to maintain crucial aspects of the project. Project design is an early phase of the project where a project's key features, structure, criteria for success, and major deliverables are all planned out.

The point is to develop one or more designs which can be used to achieve the desired project goals. Stakeholders can then choose the best design to use for the actual execution of the project. The project design phase might generate a variety of different outputs, including sketches, flowcharts, HTML screen designs, and more.

So, the design can be implemented using Unified Modeling Language. diagrams such as class diagram, use case diagram, sequence diagram, activity diagrams.

UML offers a way to visualize a system's architectural blueprints in a diagram, including elements such as:

- Any activities
- Individual components of the system
- How the system will run
- How entities interact with others
- External user interface

UML is a common language for business analysts, software architects and developers used to describe, specify, design, and document existing or new business processes, structure and behaviour of artifacts of software systems.

The key to making a UML diagram is connecting shapes that represent an object or class with other shapes to illustrate relationships and the flow of information and data.

4.1 Class Diagram

A class diagram in the Unified Modelling Language 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. Class diagram is a static diagram. It represents the static view of an application. Class diagram is not only used for visualizing, describing, and documenting different aspects of a system but also for constructing executable code of the software application. Class diagram describes the attributes and operations of a class and also the constraints imposed on the system. The class diagrams are widely used in the modelling of object-oriented systems because they are the only UML diagrams, which can be mapped directly with object-oriented languages.

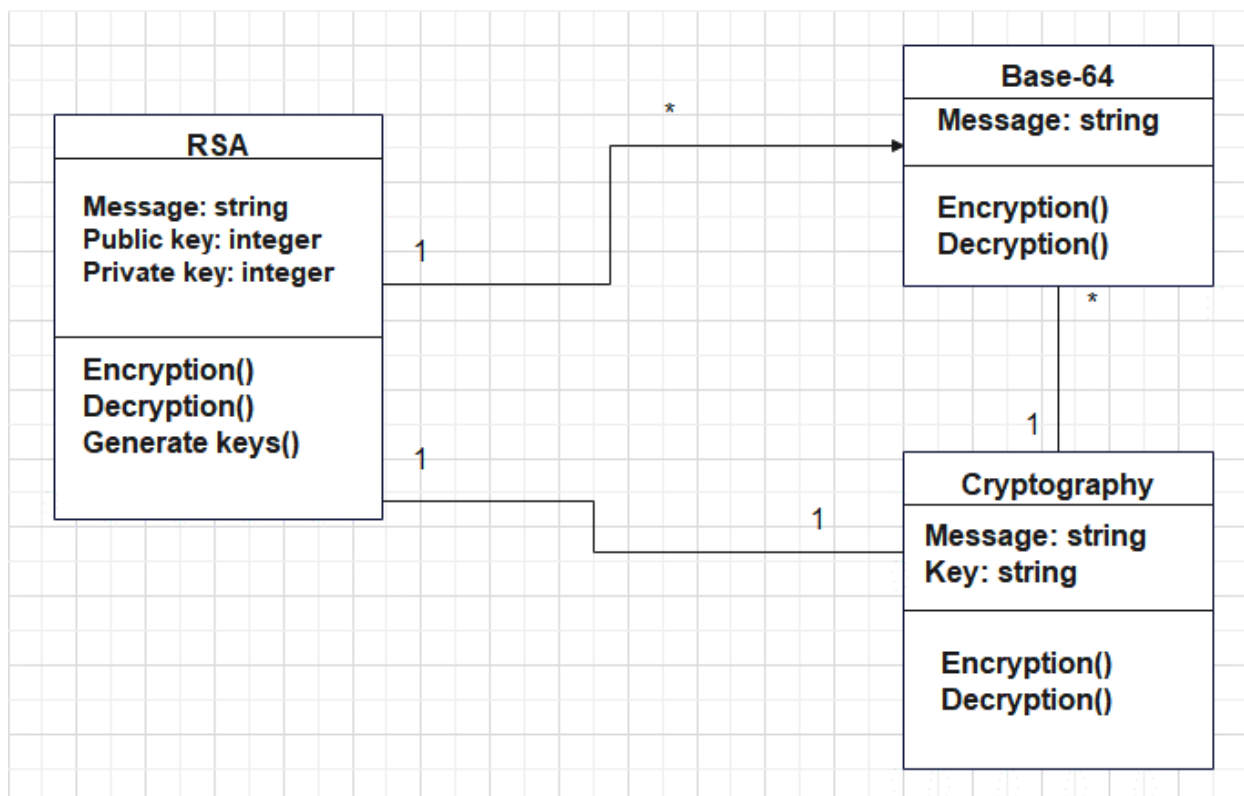


Fig 4.1 Class Diagram

4.2 Use Case Diagram

A use case diagram at its simplest is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved. A use case diagram can identify the different types of users of a system and the different use cases and will often be accompanied by other types of diagrams as well. The use cases are represented by either circles or ellipses.

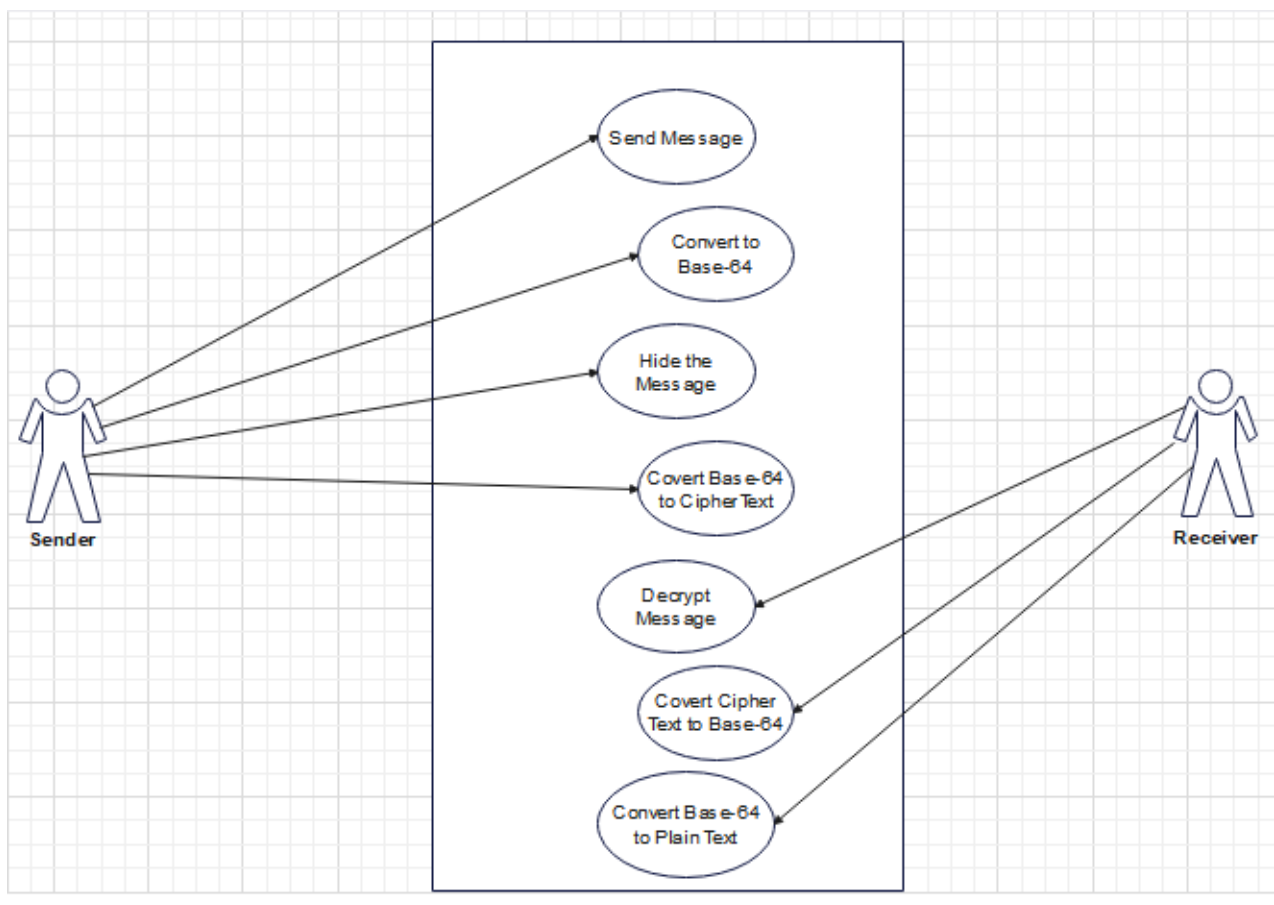


Fig 4.2 Use Case Diagram

4.3 Sequence Diagram

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams are typically associated with use case realizations in the Logical View of the system under development. Sequence diagrams are sometimes called event diagrams or event scenarios.

A sequence diagram shows, as parallel vertical lines, 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.

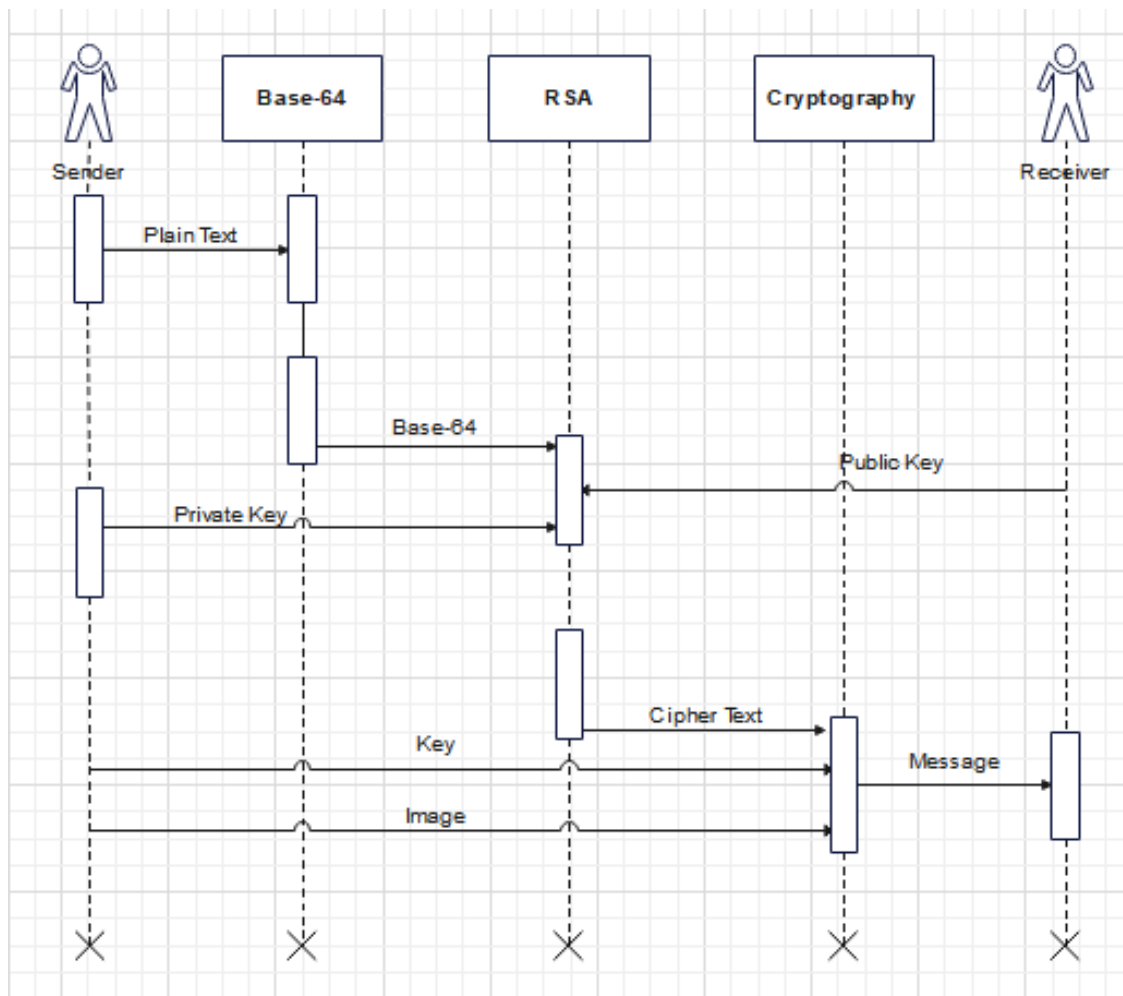


Fig 4.3 Sequence Diagram

4.4 Activity Diagram

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams are intended to model both computational and organizational processes (i.e., workflows) as well as the data flows intersecting with the related activities. Although activity diagrams primarily show the overall flow of control, they can also include elements showing the flow of data between activities through one or more data stores.

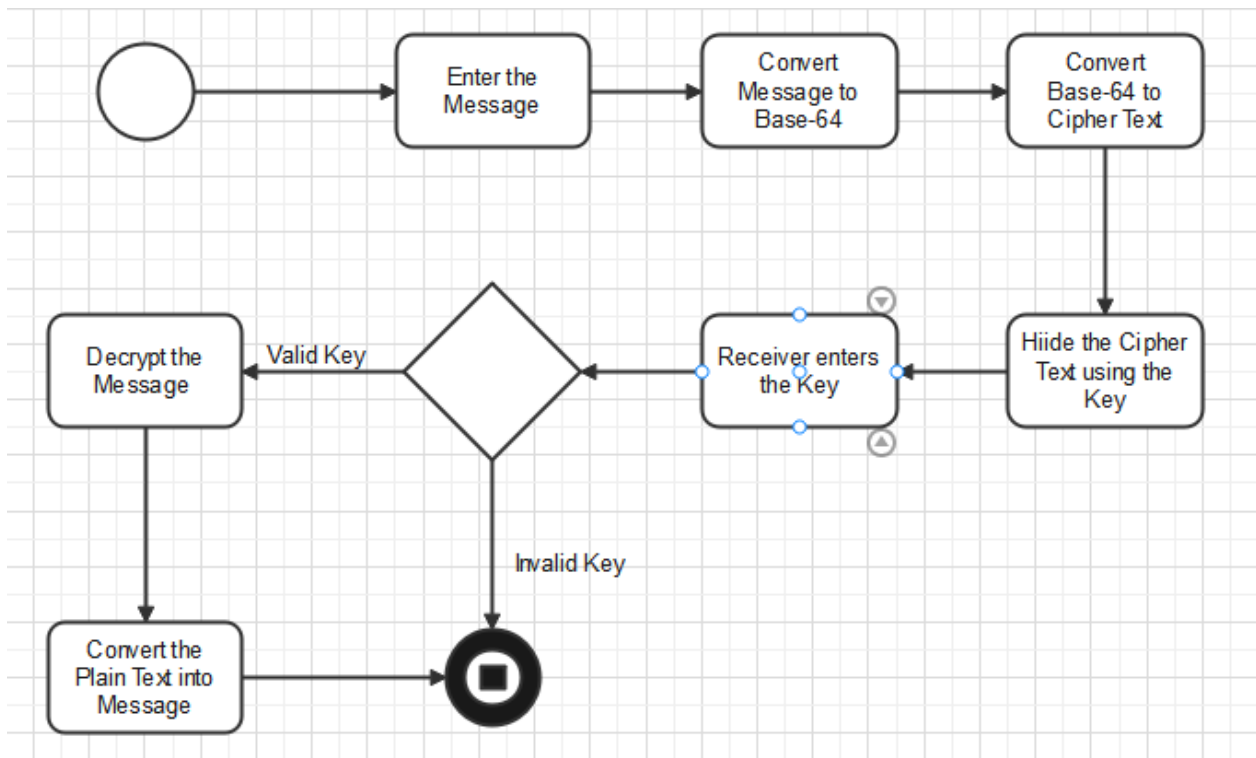


Fig 4.4 Activity Diagram

5. EXPERIMENTAL ANALYSIS AND RESULTS

5.1 SYSTEM CONFIGURATION

5.1.1 Software Requirements:

The software configurations used are

- Operating System: Windows 10
- Programming Language : Python
- Audio file format: m4a (any file format is accepted)

5.1.2 Hardware Requirements:

- Processor: INTEL
- RAM: Minimum of 256 MB or higher
- HDD: 10GB or higher
- Monitor: 15” or 17” color monitor
- Keyboard: Standard 110 keys keyboard.

5.2 SAMPLE CODE

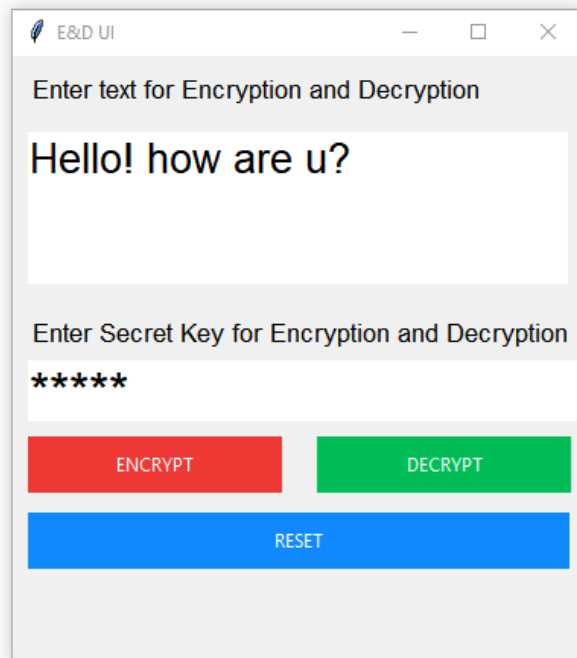
```
1 from tkinter import *
2 from tkinter import messagebox
3 import base64
4 import os
5
6
7 def encrypt():
8     password=code.get()
9
10    if password=="ENKEY":
11        screen1=Toplevel(screen)
12        screen1.title("Encryption")
13        screen1.geometry("400x200")
14        screen1.configure(bg="#ed3833")
15
16        message=text1.get(1.0,END)
17        encode_message=message.encode("ascii")
18        base64_bytes=base64.b64encode(encode_message)
19        encrypt=base64_bytes.decode("ascii")
20
21        Label(screen1,text="ENCRYPTED",font="arial",fg="white",bg="#ed3833").place(x=10,y=0)
22        text2=Text(screen1,font="Rpbote 10",bg="white",relief=GROOVE,wrap=WORD,bd=0)
23        text2.place(x=10,y=40,width=380,height=150)
24
25        text2.insert(END,encrypt)
26
27    elif password=="":
28        messagebox.showerror("Encryption","Input Password")
29
30    elif password!="ENKEY":
31        messagebox.showerror("Encryption","Invalid Password")
32
33
34 def decrypt():
35     password=code.get()
36
37    if password=="DEKEY":
38        screen2=Toplevel(screen)
39        screen2.title("Decryption")
40        screen2.geometry("400x200")
41        screen2.configure(bg="#00bd56")
42
43        message=text1.get(1.0,END)
44        decode_message=message.encode("ascii")
45        base64_bytes=base64.b64decode(decode_message)
46        decrypt=base64_bytes.decode("ascii")
47
48        Label(screen2,text="DECRYPTED",font="arial",fg="white",bg="#00bd56").place(x=10,y=0)
49        text2=Text(screen2,font="Rpbote 10",bg="white",relief=GROOVE,wrap=WORD,bd=0)
50        text2.place(x=10,y=40,width=380,height=150)
51
52        text2.insert(END,decrypt)
53
54    elif password=="":
55        messagebox.showerror("Decryption","Input Password")
56
57    elif password!="DEKEY":
58        messagebox.showerror("Decryption","Invalid Password")
59
60
61
62 def main_screen():
63
64     global screen
65     global code
66     global text1
67
68     screen=Tk()
69     screen.geometry("375x398")
70
71     screen.title("E&D UI")
```

```

72
73 def reset():
74     code.set("")
75     text1.delete(1.0,END)
76
77     Label(text="Enter text for Encryption and Decryption",fg="black",font=("calbri",13)).place(x=10,y=10)
78     text1=Text(font="Robote 20",bg="white",relief=GROOVE,wrap=WORD,bd=0)
79     text1.place(x=10,y=50,width=355,height=100)
80
81     Label(text="Enter Secret Key for Encryption and Decryption",fg="black",font=("Calabri",13)).place(x=10,y=170)
82
83     code=StringVar()
84     Entry(textvariable=code,width=20,bd=0,font=("arial",25),show="*").place(x=10,y=200)
85
86     Button(text="ENCRYPT",height=2,width=23,bg="#ed3833",fg="white",bd=0,command=encrypt).place(x=10,y=250)
87     Button(text="DECRYPT",height=2,width=23,bg="#00bd56",fg="white",bd=0,command=decrypt).place(x=200,y=250)
88
89     Button(text="RESET",height=2,width=50,bg="#1089ff",fg="white",bd=0,command=reset).place(x=10,y=300)
90
91
92     screen.mainloop()
93
94
95 main_screen()

```

5.4 Results



E&D UI

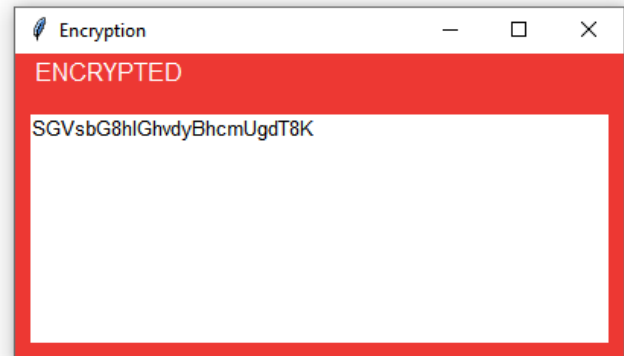
Enter text for Encryption and Decryption

Hello! how are u?

Enter Secret Key for Encryption and Decryption

ENCRYPT DECRYPT

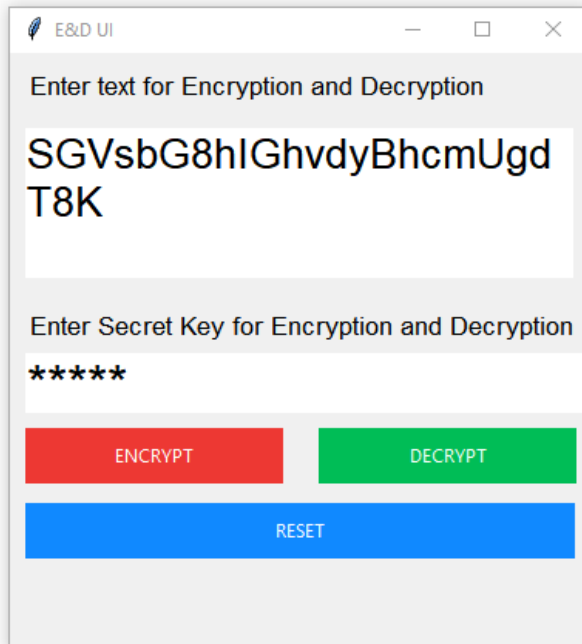
RESET



Encryption

ENCRYPTED

SGVsbG8hIGhvdvdyBhcmUgdT8K



E&D UI

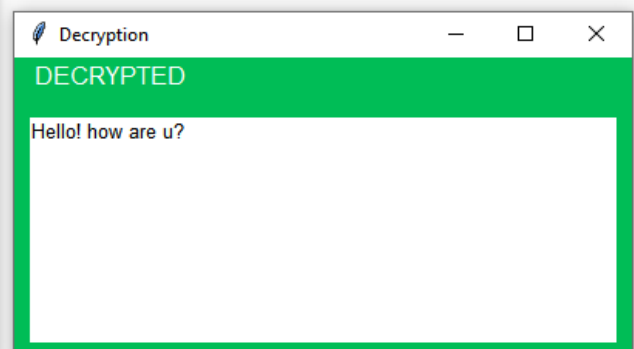
Enter text for Encryption and Decryption

SGVsbG8hIGhvdvdyBhcmUgdT8K

Enter Secret Key for Encryption and Decryption

ENCRYPT DECRYPT

RESET



Decryption

DECRYPTED

Hello! how are u?

6. CONCLUSION

In this project, we deal with the concepts of security of digital data communication across the network. This project is designed for combining the steganography and cryptography features factors for better performance.

We performed a new steganography method and combined it with RSA algorithm. The data is hidden in the image so there will be no chances for the attacker to know that data is being hidden in the image. We performed our method on image by implementing a program written in Python language. The method proposed has proved successful in hiding various types of text, images, audio and videos in color images. We concluded that in our method the Image files and RSA are better. Because of their high capacity.

This work presents a scheme that can transmit large quantities of secret information and provides secure communication between two private parties. Both steganography and cryptography can be woven in this scheme to make the detection more complicated. Any kind of text data can be employed as secret msg.

The secret message employing the concept of steganography is sent over the network. In addition, the proposed procedure is simple and easy to implement.

The Embedding of data is done such as Audio, Video, Image is done in the image, by choosing a distinct and new image, we can prevent the chance for the attacker to detect the data being hidden. Results achieved indicate that our proposed method is encouraging in terms of security, and robustness.

7. REFERENCES

- [1] D. Seth, L. Ramanathan, and A. Pandey, “Security enhancement: Combining cryptography and steganography,” *International Journal of Computer Applications* (0975–8887) Volume, 2010.
- [2] H. Abdulzahra, R. AHMAD, and N. M. NOOR, “Combining cryptography and steganography for data hiding in images,” *ACACOS, Applied Computational Science*, pp. 978–960, 2014.
- [3] J. V. Karthik and B. V. Reddy, “Authentication of secret information in image stenography,” *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 14, no. 6, p. 58, 2014.
- [4] M. H. Rajyaguru, “Cryptography-combination of cryptography and steganography with rapidly changing keys,” *International Journal of Emerging Technology and Advanced Engineering*, ISSN, pp. 2250–2459, 2012.
- [5] M. K. I. Rahmani and N. P. Kamiya Arora, “A crypto-steganography: A survey,” *International Journal of Advanced Computer Science and Application*, vol. 5, pp. 149–154, 2014.
- [6] Mr. Vikas Tyagi (2012), “Data Hiding in Image Using least significant bit with cryptography”, *International Journal of Advanced Research in computer science and Software Engineering*, Volume 2, Issue 4.
- [7] P. R. Ekatpure and R. N. Benkar, “A comparative study of steganography & cryptography,” 2013.
- [8] R. Poornimal and J. Iswarya (2013) “An Overview of Digital Image Steganography”, *International Journal of Computer Science & Engineering*