

CLOUD DATA SECURITY THROUGH CRYPTOGRAPHY

BY

MD. MUHIB SARKER
ID: 172-15-10008

SAMIRA ISHRAT ETI
ID: 172-15-9685

NURMAHAL KHATUN
ID: 172-15-9960

This Report Presented in Partial Fulfillments of the Requirements for the
Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Md. Abbas Ali Khan
Sr. Lecturer
Department of CSE
Daffodil International University

Co-Supervised By
Mr. Md. Sadekur Rahman
Assistant Professor
Department of CSE
Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

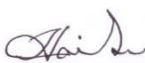
DHAKA, BANGLADESH

JANUARY 2021

APPROVAL

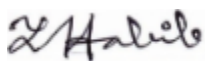
This project titled “**Cloud Data Security through Cryptography**”, submitted by * **Md.Muhib Sarkar***,* **Samira Ishrat Eti*** and * **Nurmahal Khatun** * to the department of Computer Science and Engineering, daffodil International University. Has been accepted as satisfactory for the partial fulfilment of the requirements for the B.Sc. in Computer Science and Engineering and Approved as to its style and contents. The presentation has been held on *05-01-2022*

BOARD OF EXAMINERS



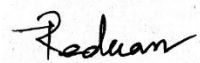
Dr. Sheak Rashed Haider Noori (SRH)
Associate Professor and Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman



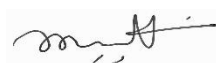
Md. Tarek Habib (MTH)
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Md. Reduanul Haque (MRH)
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Mohammad Shorif Uddin
Professor
Department of Computer Science and Engineering

External Examiner

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Mr. Md. Abbas Ali Khan, Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:



Mr. Md. Abbas Ali Khan

Sr. Lecturer

Department of CSE
Daffodil International University

Submitted by:



Md. Muhib Sarkar

ID: 172-15-10008

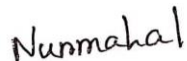
Department of CSE
Daffodil International University



Samira Ishrat Eti

ID: 172-15-9768

Department of CSE
Daffodil International University



Nurmahal Khatun

172-15-9960

Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to Almighty God for His Devine blessing that makes us possible to complete the final year project successfully.

We really grateful and wish our profound our indebtedness to Mr. Md. Abbas Ali Khan, Sr. Lecturer Department of CSE, Daffodil International University, Dhaka. Deep knowledge & keen interest of our supervisor in the field of “Blockchain” 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 all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to Prof. Dr. Touhid Bhuiyan, Head, Department of CSE, for his kind help to finish our project and also other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who participated in this discussion while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

Securing data encryption and decryption using Cryptography and ways. Due to recent developments in crypto analysis, furnishing security to particular contents, dispatches, or digital images using cryptography has come delicate. By using crypto analysis, one can fluently reveal the actuality of retired information in carrier lines. This design introduces a new cryptographic approach for communication between two private parties. The approach introduced in this design makes use of cryptographic ways. In Cryptography we're using RSA and others cryptography algorithm such as steganography, cipher. And we also use the Collective 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 the RSA algorithm, Steganography, cipher for securing the data and again on this we perform cryptography to hide the data in communication. Similar to that any other person in the network cannot pierce the data present in the network. Only the sender and receiver can recoup the communication from the data.

Keywords: Keywords: Security Key, Cryptography & its algorithm, Encryption, Decryption, Asymmetric key, key lengths.

TABLE OF CONTENTS

CONTENTS	PAGE
Board of examiners	i
Declaration	ii
Acknowledgements	iii
Abstract	iv
CHAPTER	
CHAPTER 1: INTRODUCTION	1-5
1.1 Introduction	1
1.2 Cryptography	2-3
1.3 Motivation	4
1.4 Objective	4
1.5 Organization of Report	5
CHAPTER 2: BACKGROUND	6-10
2.1 Introduction	6
2.2 Literature Review	6-10
CHAPTER 3: METHODOLOGY	11-16
3.1 System Architecture	11
3.2 Proposed System	11-12
3.2.1 Sender Side	12
3.2.2 Receiver Side	13

3.3 Model Division	13
3.3.1 Base-64	13-14
3.3.2 RSA	15-17
CHAPTER 4: DESIGN	18-21
4.1 Class Diagram	18-19
4.2 Use Case Diagram	19-20
4.3 Sequence Diagram	20-21
4.4 Activity Diagram	21-22
CHAPTER 5: EXPERIMENTAL ANALYSIS AND RESULTS	23-37
5.1 System Configurations	23
5.2 Software Requirements	23
5.3 Hardware Requirements	23
5.4 Sample Code	23-28
5.3 Testing	29
5.4 Results	30-32
CHAPTER 6: SUMMARY, CONCLUSION AND FUTURE WORK	33-34
6.1 Conclusion	33
6.2 Summary	33-34
REFERENCES	35-36

LIST OF FIGURES

FIGURES	PAGE NO
Figure 1.2 Cryptography as a flow Model	2
Figure 1.2.2 Steganography as a flow Model	3
Figure 3.1 System Architecture	11
Figure 3.2 Proposed Architecture System	12
Figure 4.1 Class diagram	19
Figure 4.2 Use Case Diagram	20
Figure 4.3 Sequential Diagram	21
Figure 4.4 Activity Diagram	22
Figure 5.3.1 Home Page and its key Channel	29
Figure 5.3.2 Home Page	30
Figure 5.3.3 Encrypted Bar	30
Figure 5.3.4 Decrypted Bar	31
Figure 5.3.5 Private Key	31
Figure 5.3.6 Public Key	32

CHAPTER 1

INTRODUCTION

1.1 Introduction

Digital communication substantiations a conspicuous and nonstop development in numerous operations on the Internet. Subsequently, secure correspondence meetings should be submitted. The security of the information communicated across a worldwide organization has transformed into a significant variable in the organization's execution measures. Thus, secrecy and the honesty of information are requested to help snoops from entering and utilizing communicated information. Cryptography is two significant ways that are utilized to give network security. The finish of this plan is to foster another way to deal with concealing a piece of restricted data in correspondence, by exploiting the advantages of cryptography.

1.2 Cryptography

Cryptography is one of the conventional styles used to ensure the sequestration of correspondence between parties. This framework is the craft of mystery writing, which is utilized to encode the plaintext with a key into ciphertext to be moved between parties on a shaky channel. Utilizing a substantial key, the ciphertext can be unraveled to the first plaintext. Without the information on the key, nothing can recover the plaintext. Cryptography has a fundamental impact on various variables required for secure correspondence across an uncertain channel, similar to classification, sequestration, non-disavowal, pivotal trade, and confirmation.

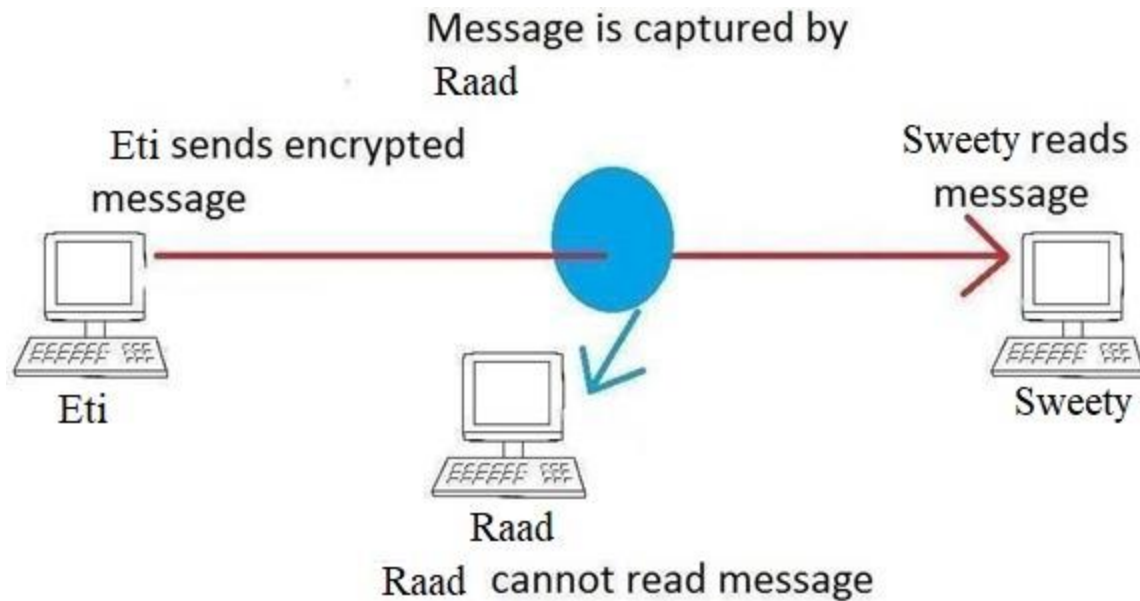


Fig. 1.2. Cryptography as a flow model.

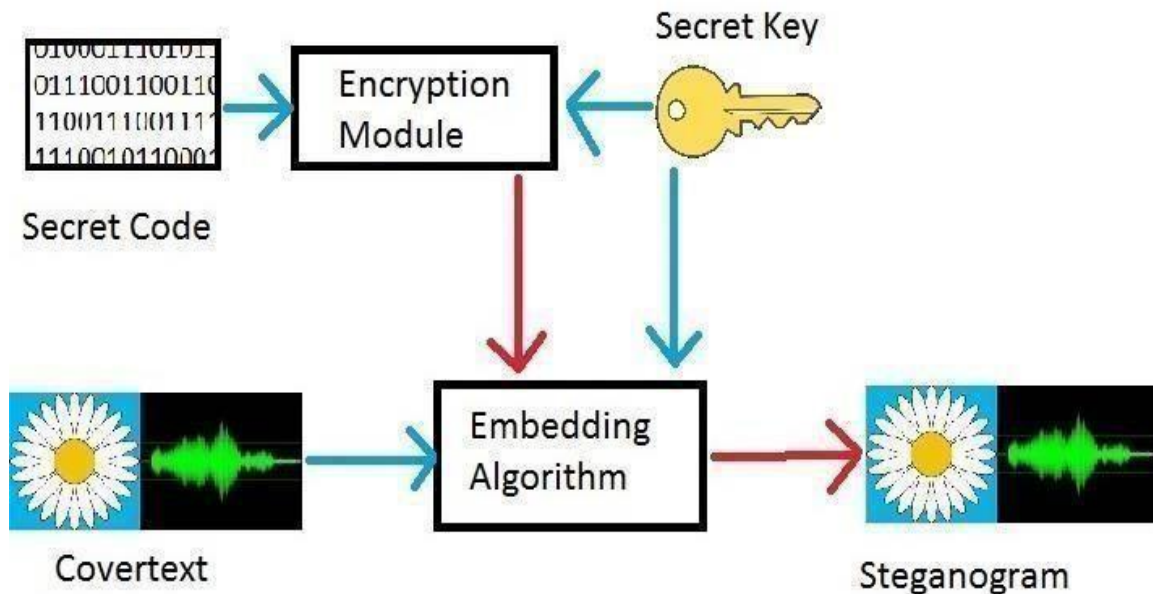
1.2.1 Symmetric / Secret Key Cryptography

The style of Secret significant encryption can likewise be known as the symmetric-key, took part vital, single-key, and at last private-critical encryption. The style of private significant uses for all side encryption and unscrambling of privileged information. The first data or plaintext is interpreted with a key by the source side likewise a closely resembling key is utilized by the recipient to unravel a correspondence to acquire the plaintext. The key will be known exclusively by individuals who are approved for the encryption/decoding. In any case, the style bears the cost of good security for transmission however there's trouble with the conveyance of the key. On the off chance that one takes or investigates the key, he can get entire information with practically no trouble. An outline of Symmetric-Crucial is DES Algorithm.

1.2.2 Asymmetric / Public Key Cryptography

We can call this design hilter kilter cryptosystem or public-essential cryptosystem, this style utilizes two keys that are numerically related, use autonomously for breaking and deciphering the data. In this design, when we utilize the private key, there are no potential outcomes to acquire the information or essentially find the other key. The key utilized for encryption is put away open subsequently it's known as the public key, and the

unscrambling key is put away confidential and called the private key. A representation of



an Asymmetric-Crucial Algorithm is RSA.

Fig 1.2.2: Steganography as a flow model.

1.2.3 Steganography versus Cryptography

Steganography and cryptography are used for the purpose of data transmission over an insecure network without the data being exposed to any unauthorized persons. Steganography embeds the data in a cover image while cryptography encrypts the data. The advantage of Steganography is that the look of the train isn't changed and this won't raise any mistrustfulness for the bushwhacker to suspect that there may be some data hidden, unlike cryptography that encrypts the data and sends it to network.

1.2.4 Benefits of Steganography and Cryptography

It's prominent that steganography and cryptography alone are lacking for the security of data, consequently assuming we join these frameworks, we can initiate a more trustworthy and solid methodology. The mix of these two techniques will improve the security of the data. This consolidation will satisfy the essentials, for the outline, memory space, security, and strength for significant data transmission across an open channel. Additionally, it'll be

a significant medium that empowers individuals to convey without sneaking around with Eavesdroppers to be sure knowing there's a style of correspondence in any case.

1.3 Motivation

Provocation is a veritably important function for any design. It's one of the styles to induce the man on the job to get the work done effectively to have the stylish results towards the common objects. It's necessary for better performance. Incitement should be visible as the inward drive, which prompts individuals to act in a way either towards accomplishing their specific assumptions or hierarchical assumptions. To a large extent, provocation 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 impact his inferiors only when they're convinced. A conviction can only come when the entire inferior accepts those factors that propel the conduct of individualities, which are appertained to as provocation. They may be largely paid, prestigious titles creation, praises, lagniappes, etc. The word is an abstract noun applying to the entire class of asked need wishes and analogous forces. Provocation has to do with action which results, in satisfaction nearly associated with provocation is the word “phenomenon” it's fitting moral and fidelity into the working platoon so that they will carry their duties duly and effectively with maximum frugality. The main reason and provocation for choosing this design are, Due to recent developments in crypto analysis, furnishing security to particular contents, dispatches cryptography has come delicate. By using crypto analysis, one can fluently reveal the actuality of retired information in carrier lines. So, after being exposed to similar problems it motivated us to do this design where the complete process of transferring information is done using two different ways. All that's needed is to elect a communication and transfer the information using that communication.

1.4 Objective:

In this work, our main thing is to make a software system in which we can partake our data with sequestration, currently, cryptography becomes a popular fashion for data security. In this work, we used the RSA model, steganography, cipher text with some others algorithms, we created our model to secure the data or dataset from any unauthorized access. The goal of every encryption algorithm is to make it as difficult as possible to

decrypt the generated ciphertext without using the key.

1.5 Organization of Report

The Report layout of this thesis is as follows.

Chapter-1 is about the preface which gives an idea about our design sphere. e Network Security and the title is explained i.e., Secure Data Encryption and Decryption Using Crypto, how the data is transmitted between two private parties.

Chapter- 2 is about Background Study where all former styles and being models are examined.

Chapter-3 contains methodology, where the algorithm is enforced for hiding the data in an image. Indeed the armature of the system is explained completely.

Chapter- 4 consists of a design that includes UML plates similar to a class illustration, use-case, sequence, and exertion illustration.

Chapter-5 consists of experimental analysis and results in this sample law, testing results, system configurations similar to software and tackle conditions, input and affair images are displayed.

Chapter-6 explains the conclusion and unborn work about our designs. e Secure Data Encryption and Decryption Using Crypto.

CHAPTER 2

BACKGROUND

2.1 Introduction

A set of IT services similar to network, storehouse, tackle, software, coffers are called pall computing. These services are handed to a client over a network. The benefits of pall storehouse are easy to pierce means access to your knowledge anyplace, anyhow, anytime, vacuity, and high trust ability of the data. For these benefits, each and every association is transferring its data to the pall. For this reason, is a need to cover the data against unauthorized access to our data? So security key is considered as one of the critical features for guarding data. Encryption is a well-known technology for guarding data. So will have to cipher the data & shoot it to the right receiver. The collector will translate it in his way. Cryptography is a design to accomplish the classification of dispatches. The term has particular importance in Greek "secret writing". At present, still, the sequestration of singularities and affiliations is given through cryptography at an elevated place, ensuring that data moved is secure such that the approved collector can penetrate this data. With strict roots, cryptography can be viewed as an old-style that is as yet being created. Embodiments reach back to 2000B.C. at the point when the antiquated Egyptians utilized "secret" hieroglyphics, just as other validation as mystery jottings in old Greece or the infamous Caesar code of old Rome. Billions of individuals all over the planet use cryptography on a diurnal premise to cover information and data, albeit most extremes don't realize that they're utilizing it. In addition to being extremely useful, it's also considered largely brittle, as cryptographic systems can come compromised due to a single programming or specification error.

2.2 Literature Review

Cryptography is a fashion to achieve the confidentiality of dispatches. The term has a specific meaning in Greek "secret jotting". Currently, still, the sequestration of individualities and associations is handed through cryptography at a high position, making sure that information transferred is secure in a way that the authorized receiver can pierce

this information (1). With literal roots, cryptography can be considered an old fashion that's still being developed. Exemplifications reach back to 2000B.C. when the ancient Egyptians used “secret” hieroglyphics, as well as other substantiation in the form of secret jottings in ancient Greece or the notorious Caesar cipher of ancient Rome (2). Billions of people around the globe use cryptography on a diurnal basis to cover data and information, although utmost don't know that they're using it. In addition to being extremely useful, it's also considered largely brittle, as cryptographic systems can come compromised due to a single programming or specification error (3). Susan et al. (4) pulled together out that organization and PC security is a new and quick innovation inside the PC insight field, with PC security coaching to be an objective that no chance quits moving. Algorithmic and precise angles, comparative as mincing ways and encryption, are the principle focal point of safety courses. As wafers track down ways of hacking network frameworks, new courses are made that cover the rearmost sort of assaults, however every one of these assaults becomes obsolete day by day because of the reactions from new security programming. With the constant development of safety language, security ways and cleaves keep on editing in the act of business, network improvement, security armature, and lawful establishment. Othman. Khalifa et al. (5) demonstrated the primary introductory generalities, characteristics, and pretensions of cryptography. They banded that in our age, i.e. the age of information, communication has contributed to the growth of technology and thus has an important part that requires sequestration to be defended and assured when data is transferred through the medium of communication. Nitin Jirwan et al. (6) appertained to data communication as depending substantially on digital data communication, in which data security has the loftiest precedence when using encryption algorithms in order for data to reach the intended druggies safely without being compromised. They also demonstrated the colorful cryptographic ways that are used in the process of data communication, similar to symmetric and asymmetric styles. In a review on network security and cryptography, Sandeep Tayal et al. (7) mentioned that with the emergence of social networks and commerce operations, huge quantities of data are produced daily by associations across the world. This makes information security a huge issue in terms of icing that the transfer of data through the web is guaranteed. With further druggies connecting to the internet, this issue further demonstrates the necessity of cryptography ways. This paper provides an

overview of the colorful ways used by networks to enhance security, similar to cryptography. Anjula Gupta et al. (8) showcased the origins and meaning of cryptography as well as how information security has come to a grueling issue in the fields of computers and dispatches. In addition to demonstrating cryptography as a way to ensure identification, vacuity, integrity, authentication, and confidentiality of druggies and their data by furnishing security and sequestration, this paper also provides colorful asymmetric algorithms that have given us the capability to cover and secure data. A study conducted by Callas, J. (9) appertained to motifs similar to cryptography, sequestration-enhancing technologies, legal changes concerned with cryptography, trust ability, and technologies used in sequestration improvement. He noticed that how society utilizes cryptography will decide the eventual fate of cryptography, which relies upon guidelines, current laws, and customs just as what society anticipates that it should accomplish. He demonstrated that there are various holes in the area of cryptography for unborn experimenters to fill. Also, the future of cryptography relies on an operating system generating strong keys to ensure that only the right people with the right keys can gain access, while others without the keys cannot. Eventually, Callas indicated that people's perspectives and studies about security and communication sequestration are a glass of the changes that do in-laws that came into actuality through events similar to the terrorist attacks of September 2001. In this manner, cryptography will forever have an influence on the security of information and data, for the present, and later on. Pushing ahead with the assumptions of cryptography, JamesL. Massey (10) pulled together out that there are two assumptions that cryptography intends to accomplish as their credibility as well as mystery. As far as the security that it manages (which can be either pragmatic or hypothetical), he talked about both Shannon's hypothesis of hypothetical mystery just and Simmon's hypothesis of hypothetical validness. Incipiently, Schneier (11) concluded that the secretiveness of security as a good thing is a myth and that it isn't good for security to be secret, as security fully counting on secretiveness can be fragile. However, recovering it would be insolvable, Assuming that mystery was lost. Schneier further communicated that cryptography grounded on short mystery keys that can be easily moved and changed should compute on an initial standard, which is for the cryptographic calculations to be contemporaneously solid and public to offer great security. The only dependable way to make further advancements in security is

to embrace public scrutiny. Varol, N. et al. (12) studied symmetric encryption which is used for the encryption of a certain textbook or speech. In this study, the content to be translated is first converted into an encapsulation cipher that cannot be understood by a cipher algorithm. Chachapara, K. et al. (13) examined secure sharing with cryptography in pall computing and demonstrated a frame that makes use of cryptography algorithms like RSA and AES, with AES being the most secure algorithm in cryptography. The pall druggies can induce keys for different druggies with different warrants to pierce their lines. Orman, H. (14) mentioned that numerous conversations and developments are generated about cryptography, as the author stated the hash functions are playing a vital part in cryptography by supplying nearly number to any piece of data and by the times that MD5's sins came given, it led to an unsettled feeling about how to design hash functions. Gennaro, R. (15) bandied randomness in cryptography and explained that an arbitrary process is one whose consequences are unknown, and mentioned that this is why randomness is vital in cryptography since it provides a way to produce information that an adversary can't learn or prognosticate it. Preneel, B. (16) exhibited cryptography and data security in the post-Snowden period, where he quibbled mass reconnaissance rehearses and the security of ICT frameworks just as known manners by which refined bushwhackers can sidestep or subvert cryptography. Sadhana, S.B. (17) pulled together on the fundamental interaction and patterns of the fields in cryptography from the hour of Julius Cesar till the ultramodern period, just as referencing the flow status of the Arabic counterfeit and scholastic sweats in this field in the set of experiences that are connected with the being cryptographic and look for new assessment styles for the security of data. The early-on origination of a cryptographic framework is to figure data or information to accomplish privacy of the data such that an unapproved individual would be unsuitable to choose its importance. Two of the most widely recognized employments of cryptography would utilize it to communicate information through a shaky channel, like the web, or icing that unapproved individuals fail to see what they're taking a gander at in a content wherein they've infiltrated the data. In cryptography, the hid data is for the most part named as "plaintext", and the method involved with camouflaging the plaintext is characterized as "encryption"; the interpreted plaintext is known as "ciphertext". This interaction is accomplished by various standards known as "encryption calculations". For the most part, the encryption interaction depends

on an "encryption key", which is additionally given to the encryption calculation as a contribution alongside the data. Utilizing an "unscrambling calculation", the entering side can recover the data utilizing the material "decoding key" (18). This is one of the most established and soonest instances of cryptography, created by Julius Caesar, the ruler of Rome, during the Gallic Wars. In this sort of calculation, the letters A through We are encoded by being addressed with the letters that come three spots in front of each letter in the letter set, while the excess letters A, B, and C are addressed by X, Y, and Z. This implies that a "shift" of 3 is utilized, despite the fact that by utilizing any of the numbers somewhere in the range of 1 and 25 we could acquire a comparable impact on the encoded text. In this way, these days, a shift is frequently viewed as a Caesar Cipher [18]. As the Caesar figure is perhaps the easiest illustration of cryptography, it is easy to break. For the ciphertext to be decoded, the letters that were moved return moved three letters once again to their past positions. Notwithstanding this shortcoming, it very well may be sufficient in verifiable occasions when Julius Caesar utilized it during his conflicts. Despite the fact that, as the moving letter in the Caesar Cipher is consistently three, anybody attempting to unscramble the code text has just to move the letters to decode it [19].

CHAPTER 3

RESEARCH METHODOLOGY

3.1 System Architecture

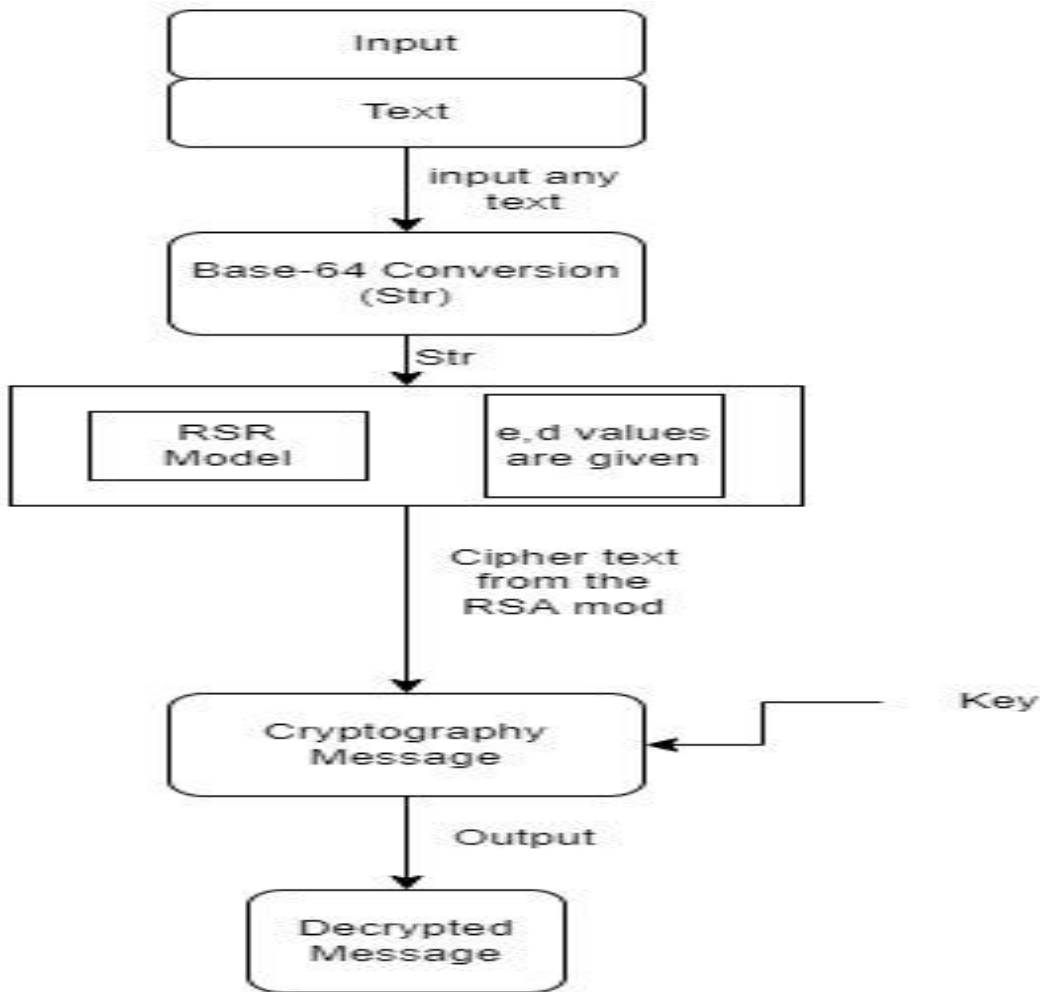


Fig 3.1 System Architecture

3.2 Proposed System

In this section, we will bandy the proposed system which is Cryptography. In this proposed system first, the communication is translated by using the RSA algorithm. After that, we use the modified LSB fashion to bed the translated information in the communication. So,

this cryptography provides a high position of security. It's better than either of the fashion used independently. There will be an arrangement between the shipper and the beneficiary with regards to the key for the covering calculation just as the key for the encryption calculation or these keys might be changed by a solid correspondence framework. Our framework begins with encryption first additionally conceals interpreted information. 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.

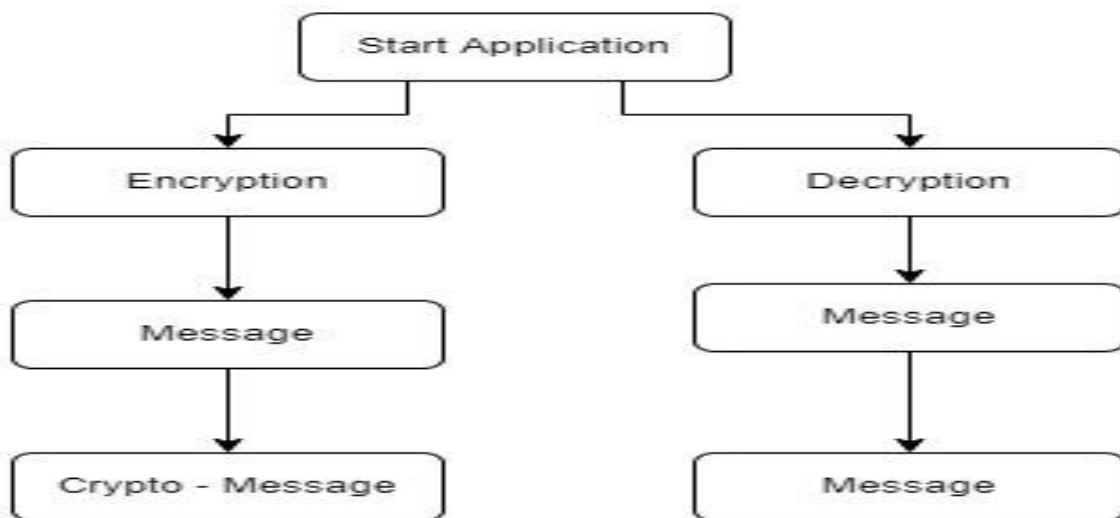


Fig: 3.2 Proposed Architecture System

3.2.1 Sender Side

The Sender side consists of cryptographic stages. This method starts with cryptographic.

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

The recipient side comprises of steganography and cryptography stages. On the collector side, we will initially separate implanted information then, at that point, decode it.

In the cryptography stage, we utilize the information which is extricated from the crypto record and use RSA. We will utilize similar advances which are utilized on the shipper side. The Decryption can be done using the Encrypted message, receiver's private key and sender's 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.

3.3 Module Division

3.3.1 Base-64

Base64 is a confusing plan that converts twofold information into a reading material organization so that decoded printed information can be smoothly moved over the organization ruined and with no information misfortune. Base64 is utilized commonly in various activities including the dispatch through MIME and putting away complex information in XML. The issue with moving ordinary twofold information to an organization is that pieces can be misjudged by supporting conventions, produce inaccurate information at entering hitch and that is the reason we utilize this framework. The term Base64 is taken from the Multipurpose Internet Correspondence Extension (MIME) standard, which is extensively used for HTTP and XML, and was firstly developed for garbling dispatch attachments for transmission.

3.3.2 Why Do We Use Base64?

Base64 is veritably important for double data representation, similar that it allows double data to be represented in a way that looks and acts as a plain textbook, which makes it more dependable to be stored in databases, transferred in emails, or used in a textbook- grounded format similar as XML. Base64 is principally used for representing data in an ASCII string format.

3.3.2.1 Base64 Encoding

Base64 encoding is the process of converting double 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 appertained 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 decoded data ends up being longer than the original data, so that, for every 3 bytes of double data, there are at least 4 bytes of Base64 decoded data. This is due to the fact that we're squeezing the data into a lower set of characters.

3.3.2.2 Base64 Decoding

Base64 decoding is the contrary of Base64 encoding. In other words, it's carried out by reversing the way described in the Encoding. So, each character in the string is changed to its Base64 decimal value. The decimal values attained are converted into double coequals. The first two bits of the double figures are abbreviated from each of the double figures attained, and the sets of 6 bits are combined, forming one large string of double integers. The large string of double integers attained in the former step is resolved into groups of 8 bits. The 8- bit double figures are converted into their decimal coequals. Eventually, the decimal values attained are converted into their ASCII fellow.

3.3.2.3 Usage

Base64 is most commonly used to deliver twofold information (for outline pictures, or sound lines) for implanting into HTML, CSS, EML, and other course book archives. What's more, Base64 is utilized to deliver information that might be unverified or harmed during move, storage facility, or issue. A portion of the activities of the calculation

3.3.1.4.1 Attach lines when transferring emails

3.3.1.4.2 Embed images in HTML or CSS via data URI

3.3.1.4.3 Save raw bytes of cryptographic functions

3.3.2 RSA

The RSA calculation is the foundation of a cryptosystem a set-up of cryptographic calculations that are utilized for explicit security administrations which empower public-critical encryption and are broadly used to get touchy information, especially when it's being moved over a shaky organization like the web. RSA was first personally depicted in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman of the Massachusetts Institute of Technology, however, the 1973 formation of a public key calculation by British mathematician Clifford Cocks was kept ordered by the U.K's. GCHQ until 1997. In RSA cryptography, both people in general and the private keys can encode correspondence; the opposite key from the one used to encode correspondence is utilized to translate it. This quality is one justification for why RSA has come to the most broadly utilized topsy-turvy calculation, It gives a framework to guarantee the privacy, trustworthiness, credibility, and non-disavowal of electronic dispatches and information storage facilities. RSA gets its security from the trouble of considering huge numbers that are the result of two huge high figures. Duplicating these two figures is simple, yet deciding the first high figures from the aggregate or calculating is thought of as infeasible because of the time it would take utilizing to be sure second's supercomputers.

3.3.2.1 Why RSA Algorithm is used?

The general population and private vital age calculation is the most intricate piece of RSA cryptography. Two enormous high figures, p , and q are named. N is determined by duplicating p and q . This number is utilized by both general society and private keys and gives the connection between them. Its length, for the most part, communicated in bits, is known as the urgent length. The public key comprises the modulus n and a public type e . You don't need to be a personally named big number, as the public key partakes with everybody. The private key comprises the modulus n and the private exemplified, which is determined utilizing the Extended Euclidean calculation to track down the multiplicative antipode regarding the totient of n .

3.3.2.2 RSA Security

RSA security depends on the computational trouble of figuring enormous numbers. As working out power increments and more compelling calculating calculations are found, the

capacity to factor in progressively large figures likewise increments. Encryption strength is immediate to a significant size, and multiplying urgent length can convey an outstanding expansion in strength, in spite of the fact that it vitiates execution. RSA keys are by and large 1024-bits or 2048-bits in length, however, specialists accept that 1024-cycle keys are presently not totally secure against all assaults. For this reason, the public authority and some ingenuity are moving to a base key length of 2048-bits. Notwithstanding an unlooked-for advance in sum processing, it'll be various occasions ahead longer keys are required, yet elliptic breeze cryptography (ECC) is acquired with various security specialists as volition to RSA to apply public-significant cryptography. It can create energetically, lower, and more compelling cryptographic keys. Ultramodern tackle and programming are ECC-prepared, and its popularity is probably going to develop, as it can convey unique security with lower figuring power and battery asset activity, making it more appropriate for portable applications than RSA. Ultimately, a company of experimenters, which included Adi Shamir, a demonstration innovator of RSA, has effectively made a 4096-piece RSA key utilizing aural cryptanalysis; still, any encryption calculation is powerless against assault.

3.3.2.3 RSA algorithm

a) Key Generation :

- Select p and q such that both are the prime numbers, $p \neq q$.
- Calculate $n = p \times q$
- Calculate $\phi(n) = (p-1)(q-1)$
- Select an integer e such that : $\text{gcd}(\phi(n), e) = 1$ & $1 < e < \phi(n)$
- Calculate d ; $de = 1 \pmod{\phi(n)}$
- Public Key, $PU = \{e, n\}$
- Private Key, $PR = \{d, n\}$

b) Encryption :

- Plaintext : M
- Ciphertext: $C = (M^e) \pmod n$

c) Decryption:

- Ciphertext: C
- Plaintext : $M = (C^d) \bmod n$
- Note 1 : $(n) \rightarrow$ Euler's totient function
- Note 2: Relationship between C and d is expressed as: $ed \bmod (n) = 1$

3.3.2.4 Algorithm

Inputs message, Key.

- 1) Originally Sender considers a Communication.
- 1) 2) Hide the Translated communication.
- 2) 3) Hiding can be done using a secret key for confidentiality.
- 3) 4) After Hiding the communication is considered a crypto- communication. Which consists of dispatches and data which is translated.
- 4) 5) The Receiver will admit the crypto communication.
- 5) 6) Using the Secret Key the receiver can view the data hidden in the communication.
- 7) Therefore the receiver can admit the communication safely.

CHAPTER 4

DESIGN

Project configuration is a significant stage towards a fruitful plan. A plan is an essential relationship of thoughts, accessories, and cycles to accomplish a thing. Plan chiefs ascertain a decent plan to stay away from dangers and give boundaries to keep up with critical parts of the plan. Project configuration is a beginning stage of the plan where a plan's vital highlights, structure, models for progress, and significant expectations are totally arranged out. The point is to foster one or further plans that can be utilized to accomplish the asked plan assumptions. Partners can likewise pick the sleek plan to use for the authentic indictment of the plan. The planning stage may actuate a wide range of works, including outlines, flowcharts, HTML screen plans, and the sky is the limit from there. So, the design can be enforced using Unified Modeling Language. Plates similar to a class illustration, use case illustration, sequence illustration, exertion plates. UML offers a way to fantasize a system's architectural arrangements in an illustration, including rudiments similar as

- . • Any conditioning
- Individual factors of the system
- How the system will run
- How realities interact with others
- External stoner interface

UML is a typical language for business judges, computer programmers, and creators used to depict, indicate plan, and archive being or new business cycles, structure, and gets of remnants of programming frameworks. The key to making a UML illustration is connecting shapes that represent an object or class with other shapes to illustrate connections and the inflow of information and data.

4.1 Class Diagram

A class diagram in the Unified Modeling Language is a sort of static construction chart that portrays the design of a framework by showing the framework's classes, their qualities, tasks (or styles), and the associations among objects. The class diagram is a static graph. It

addresses the fixed perspective on an activity. The class diagram isn't just utilized for imaging, depicting, and setting up various parts of a framework yet in addition to developing executable law of the product activity. The class chart portrays the characteristics and tasks of a class and furthermore the imperatives surveyed on the framework. The class plates are widely utilized in the demonstrating of item familiar frameworks since they're the main UML plates, which can be counterplotted straightforwardly with object-familiar dialects.

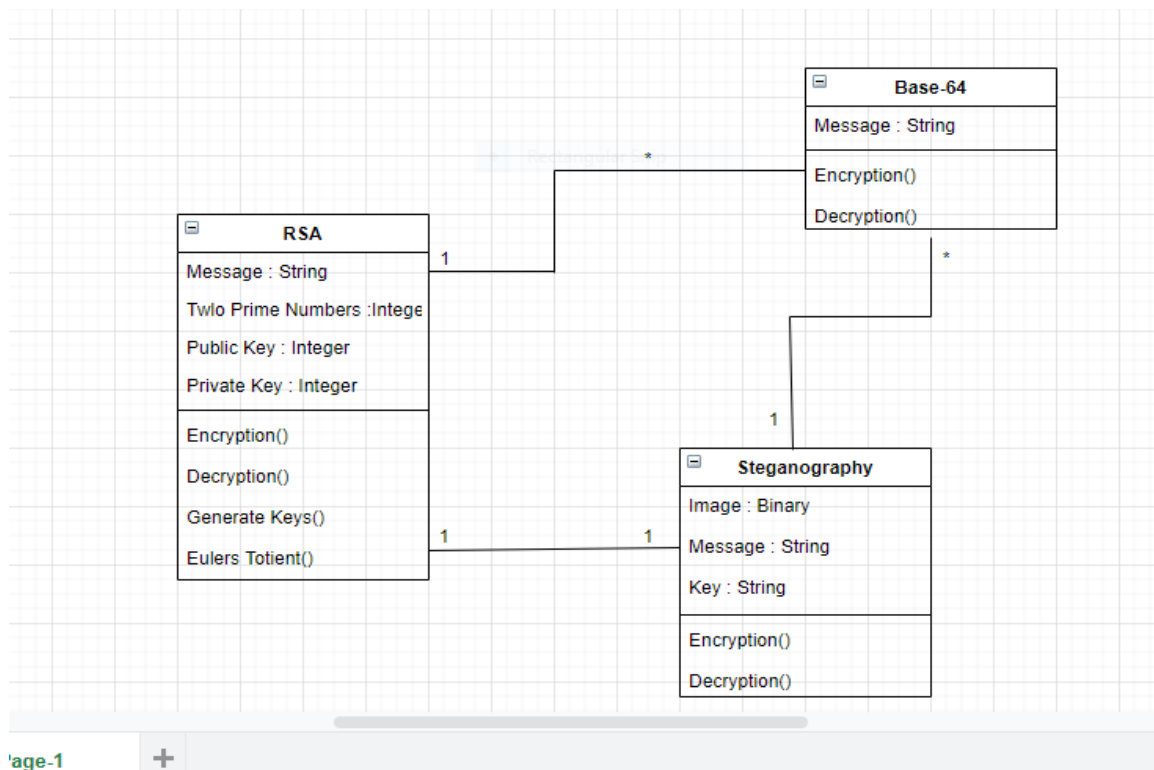


Fig 4.1 Class Diagram

4.2 Use Case Diagram

A use case diagram at its least difficult is a portrayal of a stoner's trade with the framework that shows the connection between the stoner and the distinctive use cases in which the stoner is involved. A use case diagram can distinguish the various kinds of addicts of a framework and the diverse use cases and will often be joined by different sorts of plates also. Use cases are addressed by either circles or circles.

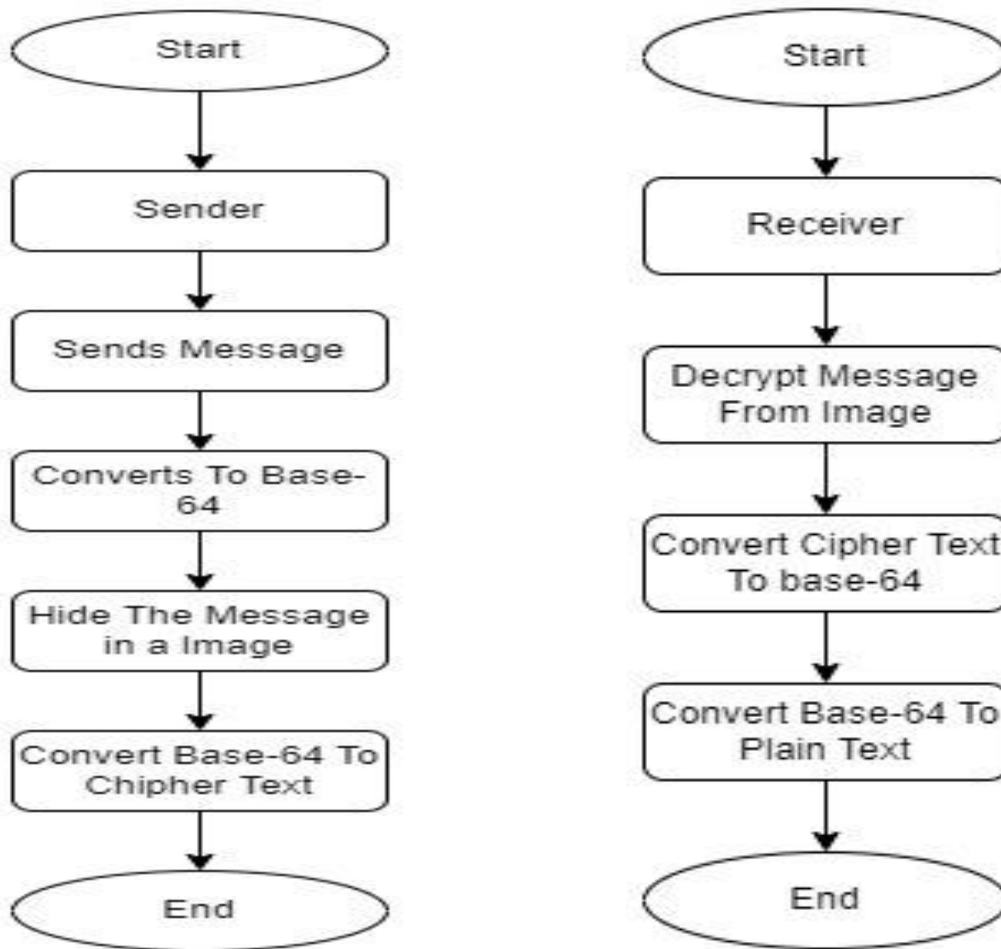


Fig 4.2 Use Case Diagram

4.3 Sequence Diagram

A grouping chart shows object relations organized in a period of succession. It portrays the articles and classes associated with the content and the succession of dispatches changed between the items requested to complete the usefulness of the content. Succession plates are by and large connected with use case culminations in the Logical View of the framework as a work in progress. Grouping plates are once in a while called occasion plates or occasion scripts. An arrangement graph shows, as taking after opposite lines, various cycles or articles that live contemporaneously, and as upward bolts, the dispatches changed between them, in the request wherein they do. This permits the determination of basic runtime scripts in a graphical way.

4.4 Activity Diagram

Effort plates are graphical portrayals of work processes of accretive molding and lead with help for decision, replication, and simultaneousness. In the Unified Modeling Language, effort plates are planned to display both computational and authoritative cycles (i.e., work processes), just as the information, streams cutting with the associated molding. Despite the fact that effort plates principally show the general inflow of control, they can likewise incorporate fundamentals showing the inflow of information between molding through one or further information stores.

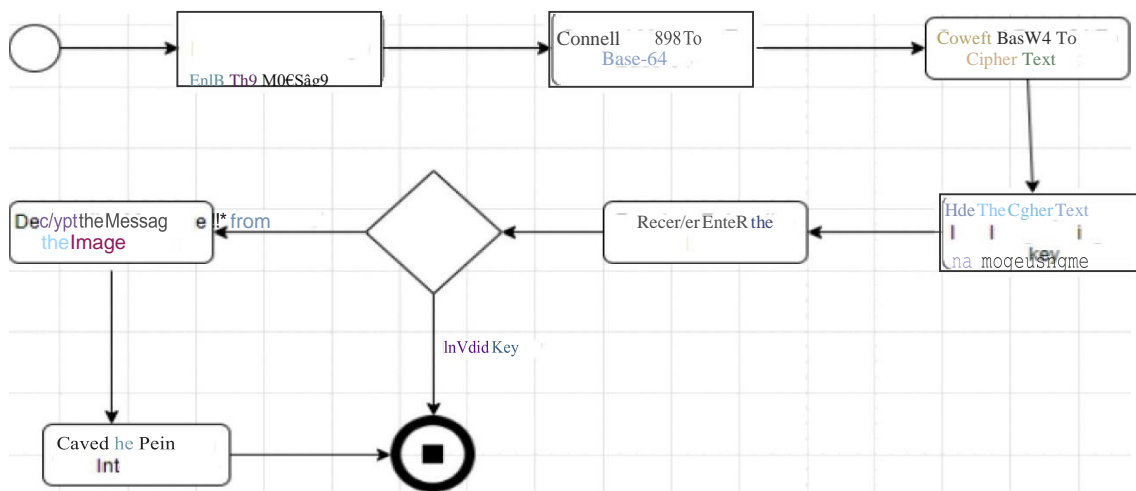


Fig: 4.4 Activity Diagram

CHAPTER 5

EXPERIMENTAL ANALYSIS AND RESULTS

5.1 SYSTEM CONFIGURATION

5.2 Software Requirements:

The software configurations used are:

Operating System: Windows 10

Programming Language: Python

5.3 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.

5.4 SAMPLE CODE

5.4.1 Home Page

```
6 # import tkinter module
  from tkinter import *

  # import other necessary modules
  import random

  # Vigenère cipher for encryption and decryption
  import base64

  # creating root object
  root = Tk()

  # defining size of window
  root.geometry("1000x5000")

  # setting up the title of window
  root.title("Message Encryption and Decryption Cryptography Project")
```

```

Tops = Frame(root, width=1400, relief=GROOVE)
Tops.pack(side=TOP)

f1 = Frame(root, width=700, relief=GROOVE)
f1.pack(side=LEFT)

# =====

lblInfo = Label(Tops, font=('Times New Roman', 25, 'bold'),
                text="MESSAGING ENCRYPTION & DECRYPTION BAR \n",
                fg="Black", bd=10, anchor='w')

lblInfo.grid(row=0, column=0)

```

5.4.2 Encryption

```

# Vigenère cipher
# Function to encode

def encode(key, msg):
    enc = []
    for i in range(len(msg)):
        key_c = key[i % len(key)]
        enc_c = chr((ord(msg[i]) +
                    ord(key_c)) % 256)
        enc.append(enc_c)
    print("enc:", enc)
    return base64.urlsafe_b64encode("".join(enc).encode()).decode()

```

5.4.3 Decryption

```

# Function to decode

def decode(key, enc):
    dec = []

    enc = base64.urlsafe_b64decode(enc).decode()
    for i in range(len(enc)):
        key_c = key[i % len(key)]
        dec_c = chr((256 + ord(enc[i]) -
                    ord(key_c)) % 256)

        dec.append(dec_c)
    print("dec:", dec)
    return "".join(dec)

```


5.4.4 Base-64

5.4.4.1 Encryption

```
6 #Encrypted Data
7 Import Base64
8 def encrypt_data(data):
9     with open(".\keyfile\moonpub.pem", "rb") as k:
10         key = RSA.importKey(k.read())
11         cipher = CPKCS.new(key)
12         return cipher.encrypt(data.encode())
13
```

5.4.4.2 Decryption

```
#Decrypted Data
Import Base64
def decrypt_data(data):
    with open(".\keyfile\moonprivate.pem", "rb") as k:
        key = RSA.importKey(k.read())
    decipher = CPKCS.new(key)
    return decipher.decrypt(data)
```

5.4.4.3 RSA

```
def convert(txt): if (txt == "A"): k = 1

elif (txt == "B"): k = 2
elif (txt == "C"): k = 3
elif (txt == "D"): k = 4
elif (txt == "E"): k = 5
elif (txt == "+"): k = 74
elif (txt == "/" ): k = 75
elif (txt == "!"): k = 63
elif (txt == "@"): k = 64
elif (txt == "#"): k = 65
elif (txt == "$"): k = 66
elif (txt == "%"): k = 67
elif (txt == "^"): k = 68
elif (txt == "&"): k = 69
elif (txt == "*"): k = 70
elif (txt == "("): k = 71
elif (txt == ")"): k = 72
elif (txt == "-"): k = 73
```

```

elif (txt == "+"): k = 74
elif (txt == "/"): k = 75
else:
k = "ERROR"
return k
def revconvert(num): if (num == 1):
k = "A"
elif (num == 2): k = "B"
elif (num == 3): k = "C"
elif (num == 4): k = "D"
elif (num == 5): k = "E"
elif (num == 6): k = "F"
elif (num == 63): k = "!"
elif (num == 64): k = "@"
elif (num == 65): k = "#"
elif (num == 66): k = "$"
elif (num == 67): k = "%"
elif (num == 68): k = "^"
elif (num == 69): k = "&"
elif (num == 70): k = "*"
elif (num == 71): k = "("
elif (num == 72): k = ")"
elif (num == 73): k = "-"
elif (num == 74): k = "+"
elif (num == 75): k = "/"
else:
k = "Error"

return k def gcd(a, b):
if b == 0:
return a else:
return gcd(b, a % b) if name == " main ":
p = int(input('Enter the value of p = ')) q = int(input('Enter the value of q = ')) #
Input Text.....

file = open("s1.txt", "r") text=file.read() file.close()
lk = []
#text = input('Enter the value of text = ') l1 = len(text)
k10 = ""
k20 = ""
for i in range(0, l1):
no = convert(text[i]) n = p * q
if (no > n):
print("Please enter correct text ")
else:

```

```

t = (p - 1) * (q - 1) for e in range(2, t):
if gcd(e, t) == 1:
break
for i in range(1, 10):
x = 1 + i * t if (x%e==0) d = int(x /e) break
ctt=Decimal(0) ctt = pow(no, e) ct = ctt % n lk.append(ct) ct1 = ct % 75
print('n = ' + str(n) + ' e = ' + str(e) + ' t = ' + str(t) + ' d = ' + str(d) + ' cipher
text = ' + str(ct1)) k1 = revconvert(ct1)
k10 = k10 + k1 print("Cipher Value", k10) print("Original Value : ",lk)
def get_lk():
return lk
file = open("sample1.txt","w") file.write(k10)
file.close()
file = open("sample2.txt","w") for i in lk:
file.write(str(i)+" ") file.close()

```

5.2.3.2 Decryption:

```

def convert(txt): if (txt == "A"): k = 1
elif (txt == "B"): k = 2
elif (txt == "C"): k = 3
elif (txt == "D"): k = 4
elif (txt == "E"): k = 5
elif (txt == "+"): k = 74
elif (txt == "/" ): k = 75
elif (txt == "!"): k = 63
elif (txt == "@"): k = 64
elif (txt == "#"):
k = 65
elif (txt == "$"):
k = 66
elif (txt == "%"): k = 67
elif (txt == "^"):
k = 68
elif (txt == "&"):
k = 69
elif (txt == "*"):
k = 70
elif (txt == "("):
k = 71
elif (txt == ")"): k = 72
elif (txt == "-"): k = 73
elif (txt == "+"): k = 74
elif (txt == "/" ): k = 75
else:
k = "ERROR"

```

```
return k
```

```
def revconvert(num): if (num == 1):  
k = "A"  
elif (num == 2): k = "B"  
elif (num == 3): k = "C"  
elif (num == 4): k = "D"  
elif (num == 5): k = "E"  
elif (num == 6):  
k = "F"  
elif (num == 63): k = "!"  
elif (num == 64): k = "@"  
elif (num == 65): k = "#"  
elif (num == 66): k = "$"  
elif (num == 67): k = "%"  
elif (num == 68): k = "^"  
elif (num == 69): k = "&"  
elif (num == 70): k = "*"  
elif (num == 71): k = "("  
elif (num == 72): k = ")"  
elif (num == 73): k = "-"  
elif (num == 74): k = "+"  
elif (num == 75): k = "/"  
else:  
k = "Error"  
return k
```

```
def gcd(a, b):  
if b == 0:  
return a else:  
return gcd(b, a % b)  
p = int(input('Enter the value of p = ')) q = int(input('Enter the value of q = ')) n  
= p * q  
file=open("sample2.txt","r") s=file.read() ct=list(map(int,s.split()))  
for i in range(0, len(ct)):  
t = (p - 1) * (q - 1) for e in range(2, t):  
if gcd(e, t) == 1:  
break  
for j in range(1, 10):  
x = 1 + j * t if(x%e ==0) d = int(x / e) break  
dtt =Decimal(0) print(ct[i])  
dtt = pow(ct[i], d) dt = dtt % n  
print('n = '+str(n)+' e = '+str(e)+' t = '+str(t)+' d = '+str(d)+'decrypted text =  
'+str(dt)) k2 = revconvert(dt)  
k20 = k20 + k2
```

```
print("Original Message: ", k20)
```

5.5 Testing

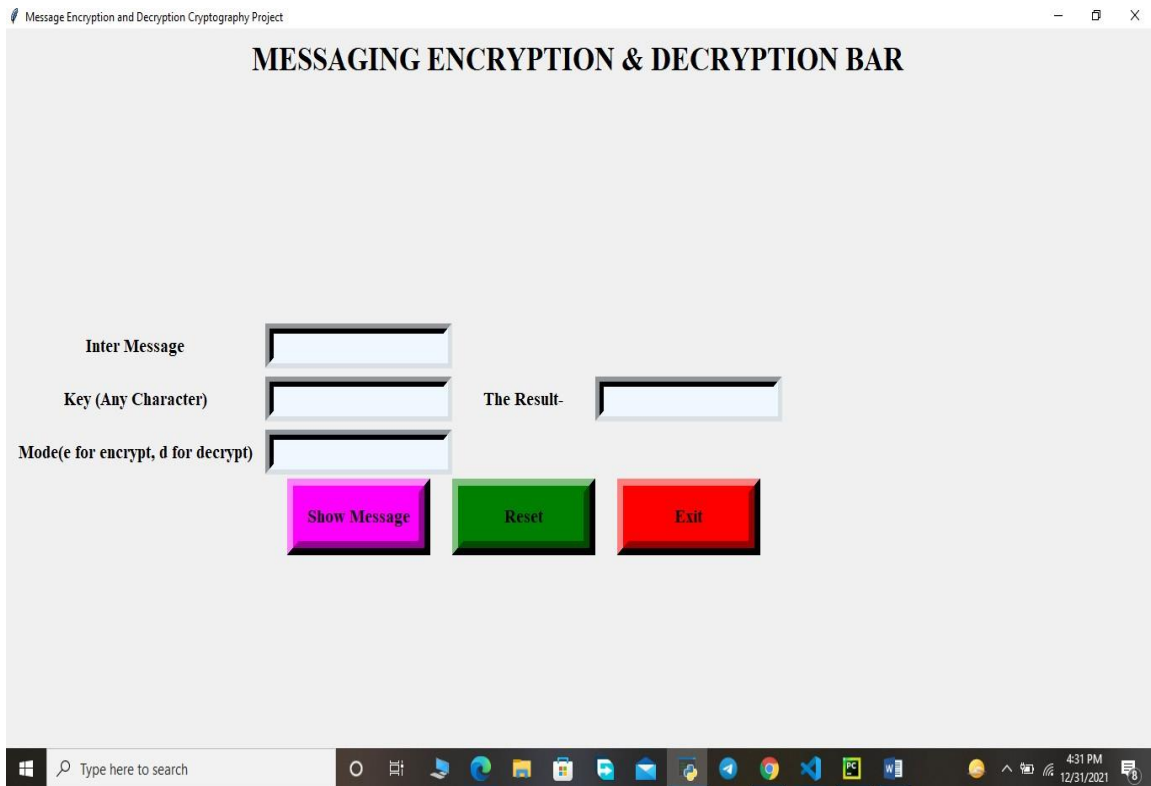


Fig 5. Home Pages in its key Channel

5.6 Results

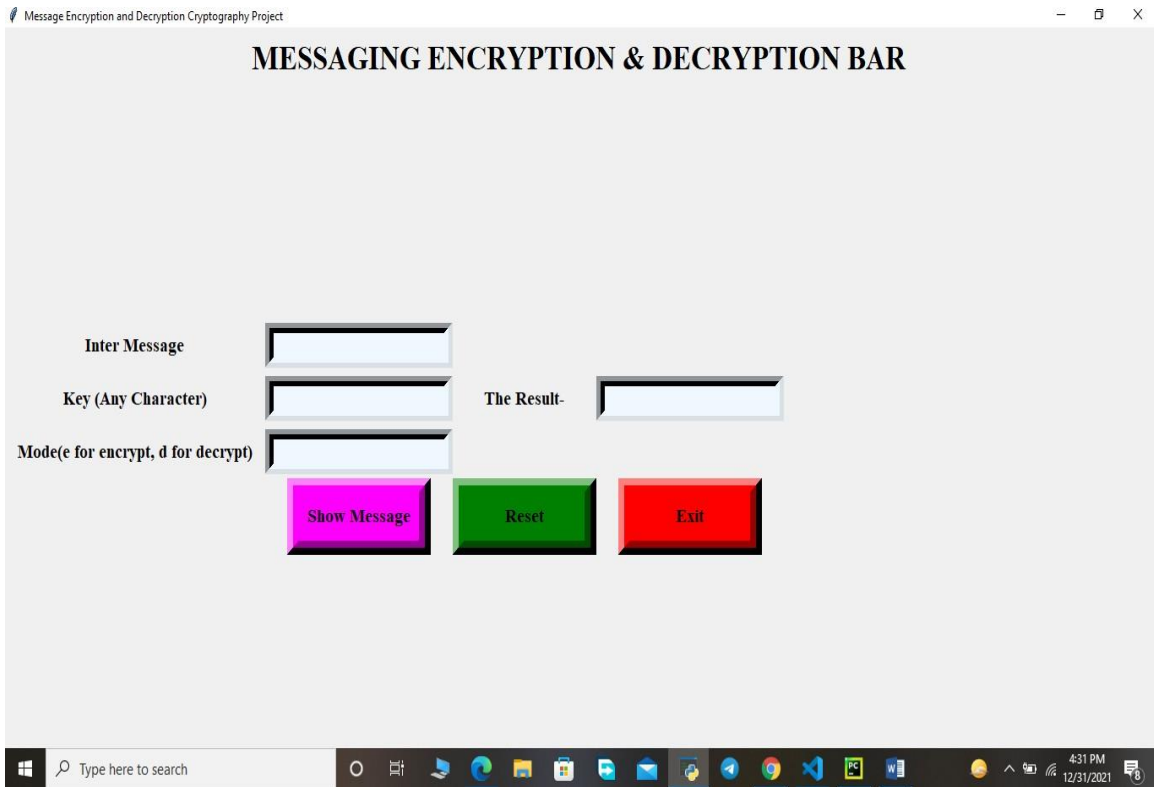


Fig 5.6.1: Home Page

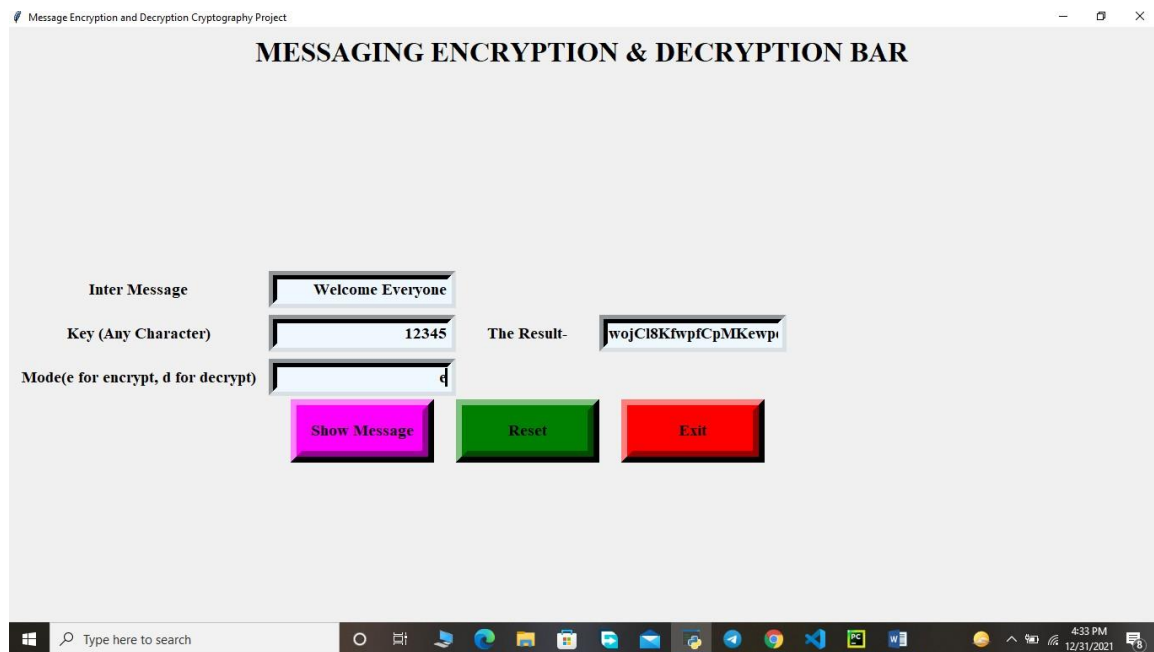


Fig 5.6.2: Encrypted Bar

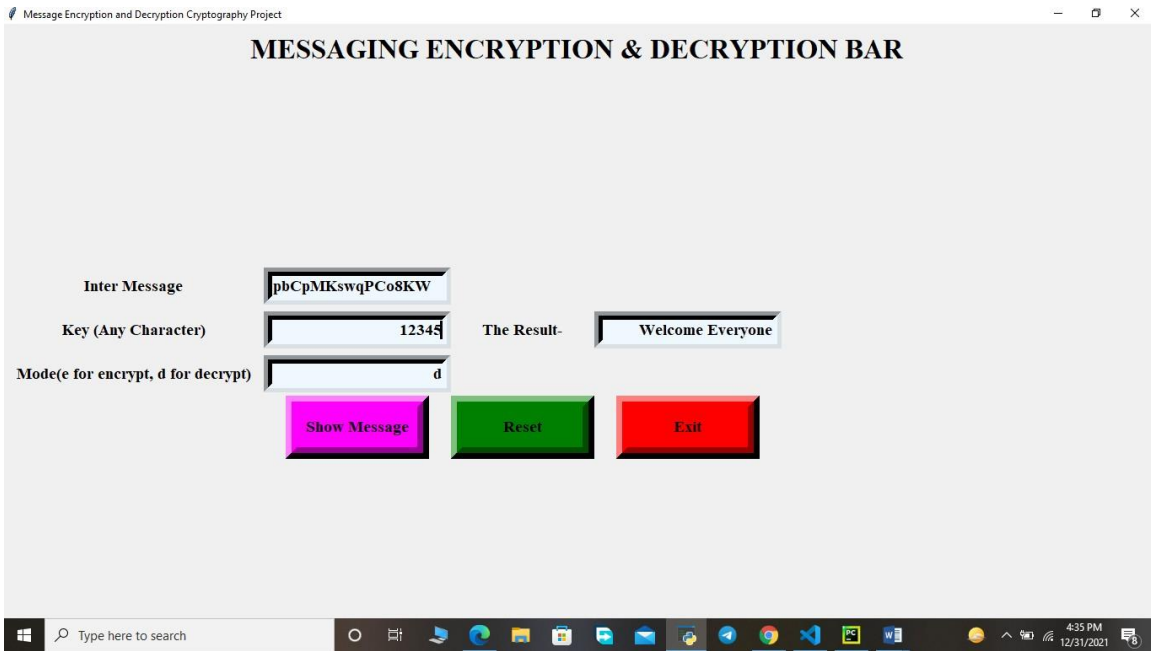


Fig 5.6.3 Decrypted Bar

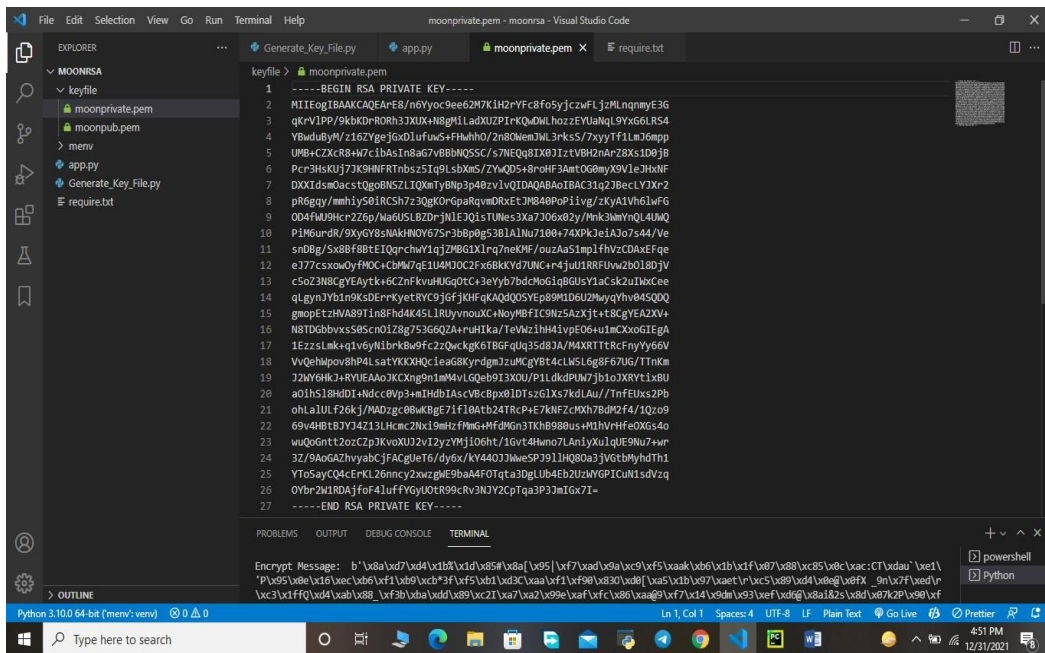


Fig 5.6.4 Private Key

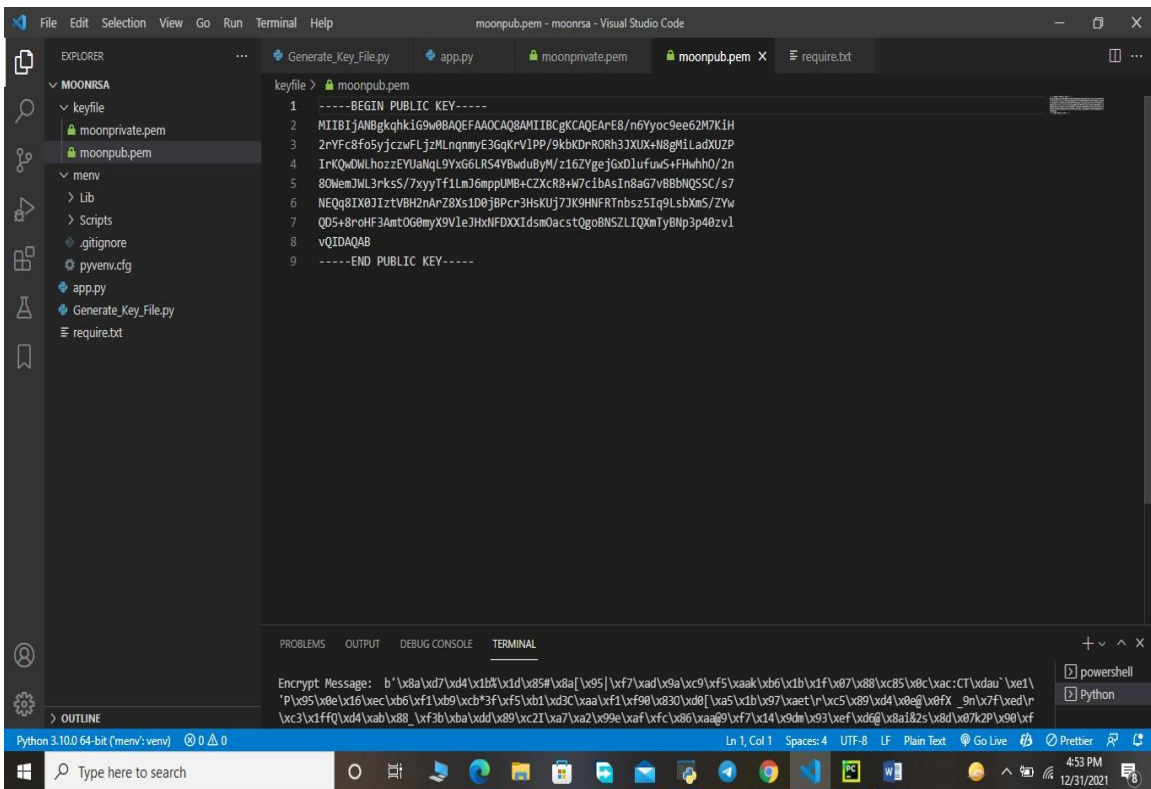


Fig 5.6.5 Public Key

CHAPTER 6

SUMMARY, CONCLUSION AND FUTURE WORK

6.1 Conclusion

Effort plates are graphical portrayals of work processes of accretive molding and lead with help for decision, replication, and simultaneousness. In the Unified Modeling Language, effort plates are planned to display both computational and hierarchical cycles (i.e., work processes), just as the information, streams cutting with the subsidiary molding. Despite the fact that effort plates essentially show the general inflow of control, they can likewise incorporate fundamentals showing the inflow of information between molding through one or further information stIn this plan, we manage the over-simplifications of the safety of computerized information correspondence across the organization. This plan is intended for cryptography highlights factors for better execution. We played out our framework on correspondence by upholding a program written in Python language. The framework proposed has demonstrated fruitfully secluded from everything brilliant kinds of course readings. Because of their high capacity. This work presents a scheme that can transmit large amounts of secret information and provides secure communication between two private parties. Any kind of textbook data can be employed as a secret msg. The secret communication employing the conception of steganography is transferred over the network. In addition, the proposed procedure is simple and easy to apply. The Embedding of data is done similarly as communication is done in the textbook, and we can help the chance for the bushwhacker to descry the data being hidden. Results achieved indicate that our proposed system is encouraging in terms of security, and robustness.

6.2 Summary

As we said the meaning of organization security is expanded step by step as the size of information is being moved across the Internet. This issue pushes the experimenters to do various investigations to expand the ability to break security issues. A consequence of this issue is involving the upside of cryptography in one framework. Various investigations propose styles to join cryptography with steganography frameworks in a single framework. This Design has been upheld based on the states of safety for example verification, privacy,

and vigor. There has been a relentless ascent in the quantity of information security traps in ongoing history and it has come to a question of worry for security specialists. Cryptography is the polished design to decrease this difficulty. The experimenter's second is proposing an amalgamated methodology of the two different ways in light of the fact that a high-level place of safety is accomplished when the two different ways are utilized together. In proposing a breaking style by joining cryptography and steganography ways of concealing the information. In the cryptography interaction, we proposed a compelling design for information encryption utilizing one's supplement framework. It utilized an Asymmetric essential framework where both shipper and collector share the Secret key for encryption and decoding. We present a framework grounded on consolidating both the solid breaking calculation to make the correspondence of nonpublic data protected, secure, and amazingly difficult to break. An encryption style is utilized for breaking a mysterious correspondence into a Ciphertext utilizing the Sender's Private Key and beneficiary public key. The Cipher Text is in the long run slept within an appropriate cover.

REFERENCE

- [1] N. Sharma, Prabhjot and H. Kaur, "A Review of Information Security using Cryptography Technique," *International Journal of Advanced Research in Computer Science*, vol. 8, no. Special Issue, pp. 323-326, 2017.
- [2] B. Preneel, *Understanding Cryptography: A Textbook for Students and Practitioners*, London: Springer, 2010.
- [3] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, London: Taylor & Francis Group, LLC, 2008.
- [4] S. J. Lincke and A. Hollan, "Network Security: Focus on Security, Skills, and Stability," in *37th ASEE/IEEE Frontiers in Education Conference*, Milwaukee, 2007.
- [5] O. O. Khalifa, M. R. Islam, S. Khan and M. S. Shebani, "Communications cryptography," in *RF and Microwave Conference, 2004. RFM 2004. Proceedings*, Selangor, 2004.
- [6] N. Jirwan, A. Singh and S. Vijay, "Review and Analysis of Cryptography Techniques," *International Journal of Scientific & Engineering Research*, vol. 3, no. 4, pp. 1-6, 2013.
- [7] S. Tayal, N. Gupta, P. Gupta, D. Goyal and M. Goyal, "A Review paper on Network Security and Cryptography," *Advances in Computational Sciences and Technology*, vol. 10, no. 5, pp. 763-770, 2017.
- [8] A. Gupta and N. K. Walia, "Cryptography Algorithms: A Review," *INTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH*, vol. 2, no. 2, pp. 1667-1672, 2014.
- [9] J. Callas, "The Future of Cryptography," *Information Systems Security*, vol. 16, no. 1, pp. 15-22, 2007.
- [10] J. L. Massey, "Cryptography—A selective survey," *Digital Communications*, vol. 85, pp. 3-25, 1986.
- [11] B. Schneier, "The Non-Security of Secrecy," *Communications of the ACM*, vol. 47, no. 10, pp. 120-120, 2004.
- [12] N. Varol, F. Aydoğan and A. Varol, "Cyber Attacks Targeting Android Cellphones," in *The 5th International Symposium on Digital Forensics and Security (ISDFS 2017)*, Turgu Mures, 2017.
- [13] K. Chachapara and S. Bhadlawala, "Secure sharing with cryptography in cloud," in *2013 Nirma University International Conference on Engineering (NUiCONE)*, Ahmedabad, 2013.
- [14] H. Orman, "Recent Parables in Cryptography," *IEEE Internet Computing*, vol. 18, no. 1, pp. 82-86, 2014.
- [15] R. GENNARO, "IEEE Security & Privacy," *IEEE Security & Privacy*, vol. 4, no. 2, pp. 64 - 67, 2006.
- [16] B. Preneel, "Cryptography and Information Security in the PostSnowden Era," in *IEEE/ACM 1st International Workshop on TEchnical and LEgal aspects of data pRivacy and SEcurity*, Florence, 2015.
- [17] S. B. Sadkhan, "Cryptography: current status and future trends," in *International Conference on Information and Communication Technologies: From Theory to Applications*, Damascus, 2004.

[18] F. Piper and S. Murphy, *Cryptography: A Very Short Introduction*, London: Oxford University Press, 2002.

[19] J. P. Aumasson, *SERIOUS CRYPTOGRAPHY A Practical Introduction to Modern Encryption*, San Francisco: No Starch Press, Inc, 2018.

CLOUD DATA SECURITY THROUGH CRYPTOGRAPHY

ORIGINALITY REPORT



PRIMARY SOURCES

1	Submitted to King Fahd University for Petroleum and Minerals Student Paper	4%
2	Submitted to University of West London Student Paper	2%
3	Submitted to Daffodil International University Student Paper	2%
4	Submitted to colorado-technical-university Student Paper	2%
5	Submitted to Edith Cowan University Student Paper	1%
6	Submitted to Hofstra University Student Paper	1%
7	Submitted to Graphic Era University Student Paper	1%
8	Submitted to CSU, San Jose State University Student Paper	1%
9	Submitted to ABES Engineering College Student Paper	1%