SC402 Introduction to Cryptography

Dhirubhai Ambani
Institute of Information and Communication Technology

Secure data Using Cryptography and Steganography

Assigned by : Professor Manish K Gupta

DA-IICT
GANDHINAGAR

Made by:

Keval Savaliya *ID:201901006*
Arik Dholiya *ID:201901009*
Sanny Dhameliya *ID:201901031*
Kenil Bhingradiya *ID:201901066*
Aditya Ramanuj *ID:201901138*

Abstract

We can secure our data by using encryption and decryption methods. Currently, providing security to personal messages and contents has become difficult. By using steganalysis, one can easily reveal hidden information. This project describes the steganographic approach for communication between two private files. The approach that is used in this project is steganographic and cryptographic. We are using RSA in Cryptography, and we are using image steganography to hide the data. We also have an authentication process that makes the data more secure like access control, Integrity, Authentication. Any other person in the network cannot access the data present in the network. Only the sender and receiver can see the message.

1 INTRODUCTION

Nowadays, Digital communication has made noticeable development in many applications on the internet. So, the security of the data should also be provided across the globe that is using the data in the network. The integrity of data should be maintained from accessing across the network. Cryptography and Steganography are two main techniques that can be used to provide network security.

The purpose of this project is to develop a new design by hiding the secret information in the picture, by combining steganography and cryptography. With the help of cryptography, we can encrypt the plaintext with the help of a key into cipher text, using a valid key, the cipher text can be decrypted. Without a key no one can retrieve the plaintext. this idea also known as symmetric key.The plaintext can be encrypted with a key by the sender side. Similarly as we know there is always use a key to encryption and also use for decription. If the key is stolen then all the data will be lost. An example of Symmetric-Key is Data Encryption Standard Algorithm. The technique of two keys which are used for encrypting and decrypting the information is known as asymmetric key. By using this technique, it is nearly impossible when we use primary key to get orignal data or discover other key. Example of an Asymmetric-Key Algorithm is RSA. With the help of the Stego system encoder and certain algorithms we can hide the information into cover media. The types of secret message can be plaintext, an image, ciphertext, or anything which can be represented in the form of a bitstream. After the restricted information is installed in the cover object, the cover article will be known as a stego object.

2 Problem Statement

The aim of this project is to provide the correct data to the receiver which is sent by the sender with securly. In some cases users' data might be changed during the transmission process or in other cases the data might be changed by an unauthorized person in the network and this is the security problem in the network. so our application will give you more security for the data present in the network and also be able to reduce the loss of data during transmission using the latest technologies. The primary target of the project is the quality of covering information should not be lost.we used technique for hiding data in different image file instead of the network.

3 LITERATURE SURVEY

As we already know that the data transmitted in the network is increasing day by day so the significance of network security is also increased.since researchers have to work with many studies and researches to improve the skill to solve the security problem. The main idea for this is to combine steganography and cryptography in one system. In recent past time, there has been many cases related to data inconsistency and increment in the number of data security threats and fraud, it has turned into an issue of worry for the security specialists. The combinathion of Cryptography and steganography are the best techniques to nullify this situation. In Today's time , the specialists are proposing a mixed methodology of the two strategies in light of the fact that a more significant level of safety is accomplished when the two procedures are utilized together. In the cryptography process, we have used one's complement method in which sender and receiver both share the secret key to encrypt and decrypt. In the steganography process, we used the most popular and most preferred method LSB. We present a technique primarily based on combining each sturdy encrypting set of rules and steganographic approach to make information safe, secure and extraordinarily difficult to decode. An encryption method is utilized for scrambling a mystery message into a Cipher message utilizing the Sender's Private Key and recipient public key.The Ci-

pher Text is at long last implanted in an appropriate cover picture and moved safely to convey the restricted data. They used a most un-critical piece technique to achieve the computerized picture steganography. And at the recipient's side, restricted information is recovered by decoding process. In this way, a three-level security has been delivered for them a secret message to be transferred.

4 METHODOLOGY

4.1 Proposed System

Now, we are going to discuss about the method which we call proposed method. In this method we use two different techniques like Cryptography and Stenography. As mention here, this method RSA algo. to encrypt messages and then using LSB technique it convert it into image. Thus, this method use combine techniques of two different hiding method and provide highly secure system. In this we get different type of input so first we convert it into Base-64 and then apply cryptography and stenography.

4.1.1 User Side

As, we discuss above, user side have to stage first cryptography and second stenography.

Cryptography Stage:

In this, we are going to use Rivest Shamir Adelson (RSA) algorithm. This method is simple to understand. First we take plain text and one 'e' value which is made by to big prime numbers. By this, we get cipher text. this text will be used in next stage.

Input = user's message + Two Prime numbers.
Output = Encrypted Message.

Stenography stage:

As per we discuss above in this method we are going to use Least Significant Bit (LSB) algorithm with modification to encrypt information inside a image. we use here image as a cover but this method applied on other files format to like audio and video. In general LSB method, we hide information into the last bit in each pixel or sample or frame sequentially into the cover image file.

Input = Encrypted Message + cover image + Key.
output = stego-image.

4.1.2 Client Side

In this side , we do same things which we did in users side but in reverse order. First we do Stenography stage and get text file from image and then using cryptography we decrypt it.

Stenography Stage:

In this, we will extract text from cover image file and then send it to the second step to decrypt it.

Input = Stego-image + key.
output = Encrypted user's message.

Cryptography stage:

Now, we are going to use this encrypted message and users public key and client private key to get our original message back.

Input = Encrypted message + users public key + client private key.
output = Plain text(user's message).

Now, remember in starting we convert our message in form of Base64. So, now we convert it back to change plain text into given file format like image,audio,video,Text.

4.2 Modules Division

4.2.1 Base64

What is Base64 ? Why do we use it? now we are going to answer this type of questions in this section.
Base64 is used to covert binary data into text format so that data can be transported without any data loss and without any corrupted data.In binary data it is easy to misinterpreted bit during transported.It is impotent for binary data because it convert binary data into plain looking text data.Basically Base64 used to represent binary data in an ASCII string format.

4.2.2 RSA

The RSA algorithm is widely used to secure data when it send over an network. this algorithm is basis of cryptography.In this method we use to key. one is public key and second one is private key. we can encrypt message using any of this key. That why this algorithm has become this much popular and most used asymmetric algorithm. Security of RSA come from the difficulty of factoring large number in proper prime factor. If we know prime number than multiplying in easy but finding this prime number in no possible because of time it takes.

In this, we use two large prime number p and q. then calculate N by multiplying p and q. the public key content the mod n and a public exponent e. e can not have selected prime number , as the this key is shared with public. the privat key content mod n and private exponent d.

Description of RSA Algorithm

- Plain text is taken from the file and then encrypted using RSA Algorithm.
- here Plain text is denoted using M and Cipher text is C.
- $C = (M^e)$mod n
- $M = (C^d)$mod n

- $M = ((M^e)^d)$mod n
- $M = (M^e d)$mod n
- value of n is known by user and reciver.
- user know the value of e as well as reciver also know the value of d.
- public key for encryption part is c,n and private key is d,n.

Key Generation

- Select p and q such that both are the prime numbers, $p \neq q$.
- Calculate $N = p * q$
- Calculate $q(N) = (p-1) * (q-1)$
- Select an integer e such that :
  $gcd((N), e)) = 1, 1 < e < N$
- Calculate d:
  de = 1 mod (q(N))
- Public Key: $PU = (e, N)$
- Private Key: $PR = (d, N)$

Encryption Using RSA:

- Plaintext = M
- Ciphertext: C = (M^e) mod n

Decryption Using RSA:

- Ciphertext = C
- Plaintext: M = (C^d) mod n

- Note 1 : (N) $->$ Euler's Totient Function
- Note 2 : Relationship between C and d is expressed as:

$ed(mod(N)) = 1$
$ed = 1mod(N)$
$d = e^{-}1mod(N)$

4.2.3 STENOGRAPHY

Most Of the application most important thing is data hiding. for data hiding basic method are : cryptography,steganography,watermarking.In cryptography the information to be hidden is encoded using certain techniques.But hear data appears is nonsensical.Main use of Steganography hiding the information.detection of steganography is called Stego analysis.
Steganography is of 4 diffrent types:

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography

In all this method basic principle is that a encryted message be embedded in some another cover object like image and audio etc.so it cannot easily detected.
Steganography consists of three components:

- Cover Object
- Message object
- Resulting Steganographic object

Here we define Image Steganography type which we use in our project.

Image Steganography

Image Steganography warp up the data using image. here data can be any thing like image,audio,test or another file.we have to make sure that image must be accountable for the data that is being embedded.best solution for hiding the data is 24-bit format,since it hold large memory space and convenient to hide a big amount of data.In our project Image Steganography apply using LSB positioning Method.

LSB Positioning Method

LSB Positioning Method is the simplest method of hiding data within the given image.when convert image to digital formt we usually choose b/w three diffrent ways of represnting colors:

- 24-bit color : every pixel can have one in (2^24) colors, and these are represented as different quantities of three basic colors : red(R), green(G), blue(b) given by 8 bits (256) each.
- 8-bit color : every pixel can have one in 256 (2^28) colors, chosen from a palette, or a table of colors.
- 8-bit gray-scale : every pixel can have one in 256 (2^28) shades of gray

Image Steganography we are using Spatial Methods.spatial methods most common method which is used is LSB substitution. since every image has three components (RGB).Every pixel infomation of Image are store in encoded format. When the LSB bit is Modified then intensity of pixel and change in colour cannot detect by human visual system.

Algorithm of Image Steganography

Inputs: Image,Encrypted-Message,Key.

1. Sender choose a cover object(here it is Image) .
2. Hide the Encrypted Message in the Image.

3. Hidding done using secrete Key.
4. After Hidding Image is called Stego-Image which is consists image and data which is encrypted
5. Receiver will receive the Stego-Image.
6. Now at receiver side, we can see secret message by secret key.
7. Thus the receiver can receive the message safely.

4.3 Algorithm Illustration

Encryption:

Inputs: User-Message, Two Prime Numbers,Image,Secret Key.

1. analysis of User-Input it can be Text,age,audio or Video anything.
2. convert this User-Input into Base-64 using Base-64 conversion algorithm.
3. after applying Base-64 algorithm we get a String.
4. Store the entire string in a Text File and save the file.
5. from this file take each char and apply RSA.
6. after applying RSA on every char of files get Text is called Cipher text.
7. Let the Cipher text be encrypted message.
8. Using Image Stegnography Algorithm choose secret key.Using this secret key we can hide our encrypted data over chosen image.After applying this Algorithm on image,this image is called Stego-Image.
9. Now send the Stego-Image to the Receiver.

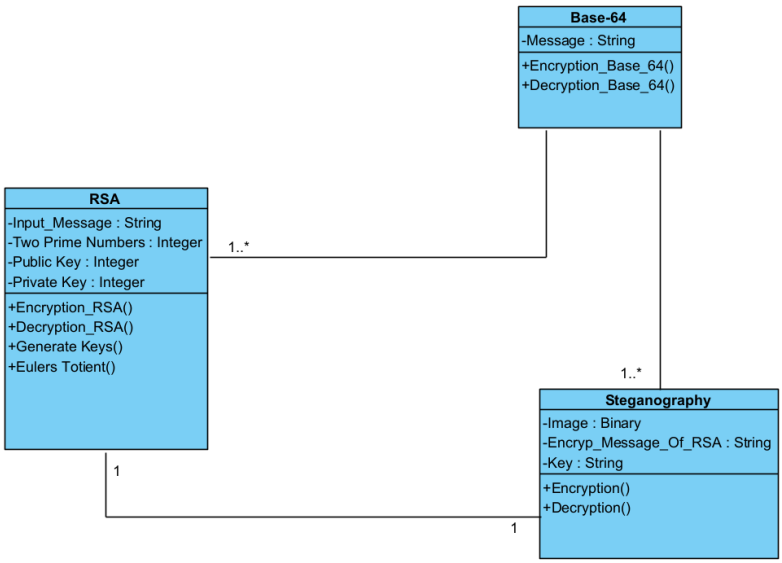
DECRYPTION:

Inputs : Cipher Text , Two Prime Numbers,Image,Secret Key.

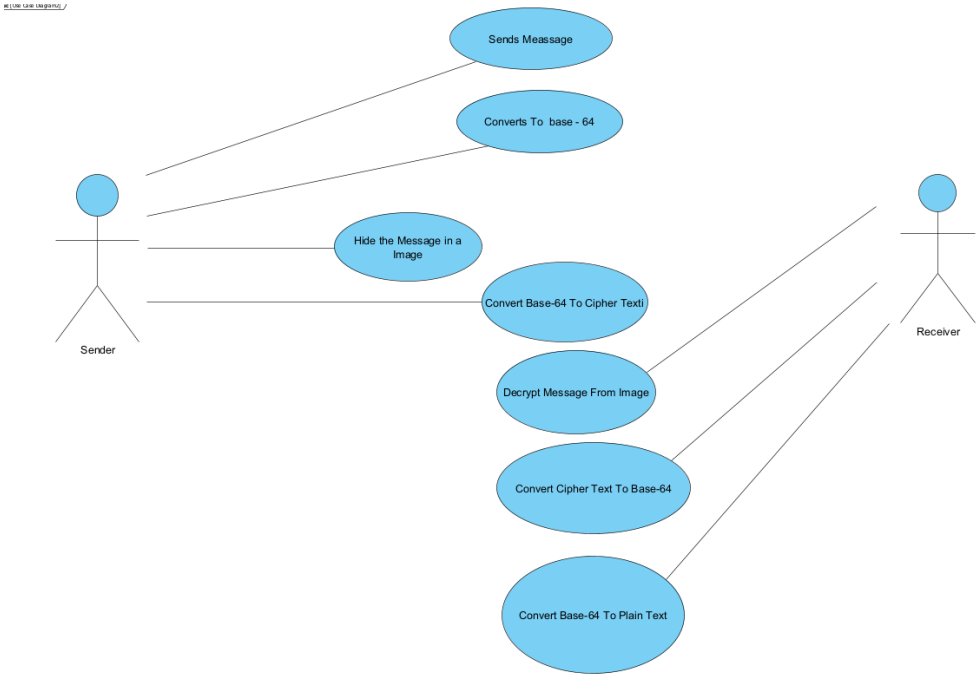
1. Stego-Image is work as input for receiver side .
2. Now at receiver side, we use secret key to get message from Stego-Image.
3. hear we obtain message is cipher text,but we want actual message. we must decrypt this message.
4. The decryption of the message can be done using RSA algorithm.
5. By applying RSA decryption Algorithm we getting Plain Text.
6. And also receiver convert this BASE64 message into simple text format.So,finally applying Base64 algorithm convert the Message into original input,which can be Text,Image,Audio or Video.

5 DESIGN

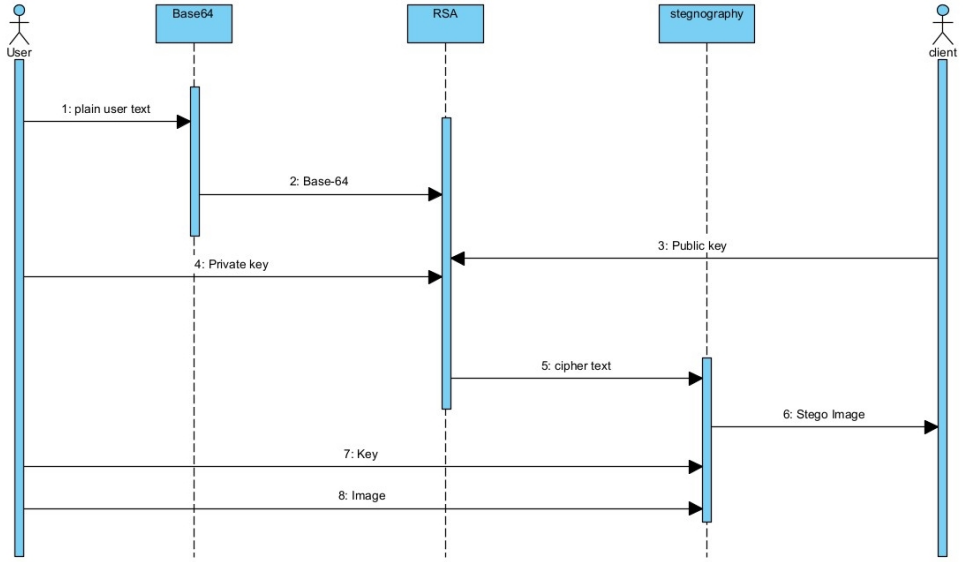
Class Diagram



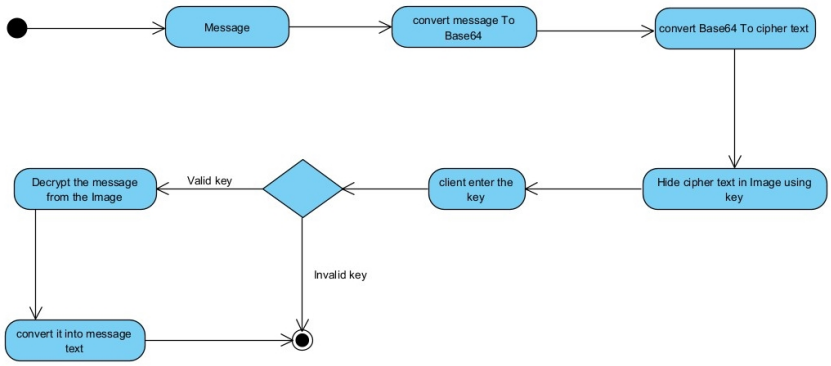
Use Case Diagram



Sequence Diagram



Activity Diagram



6 EXPERIMENTAL ANALYSIS AND RESULTS

Results of website

Link for this web application is https://github.com/kenil-bhingradiya/secure-data-using-cryptogrphy-and-steganography [**3**]

Figure 1: Home Page

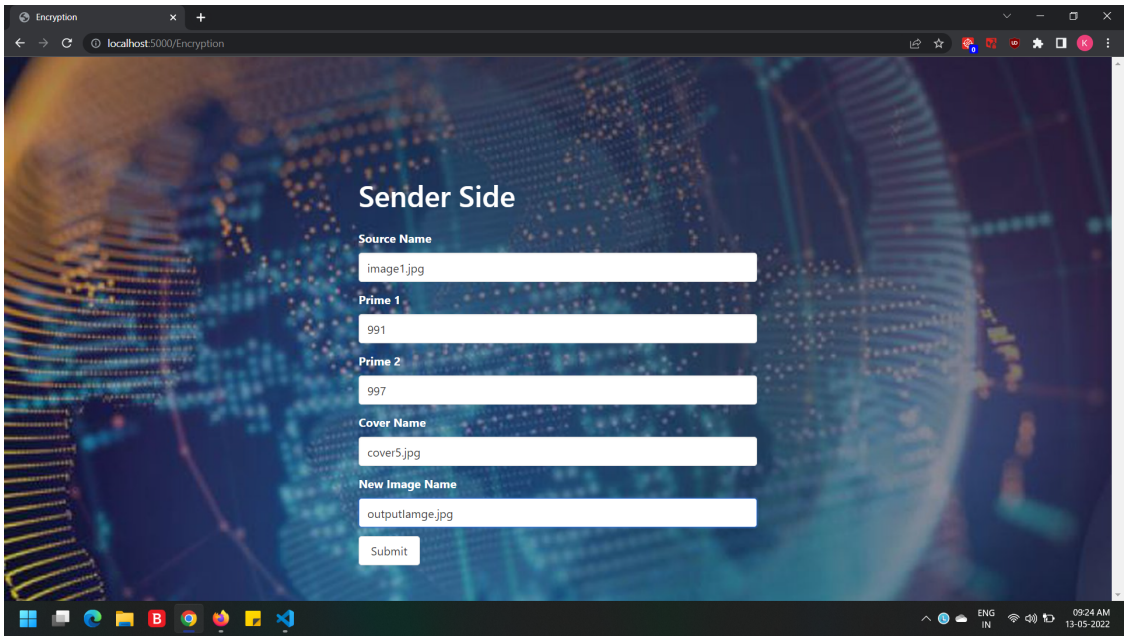


Figure 2: encryption page

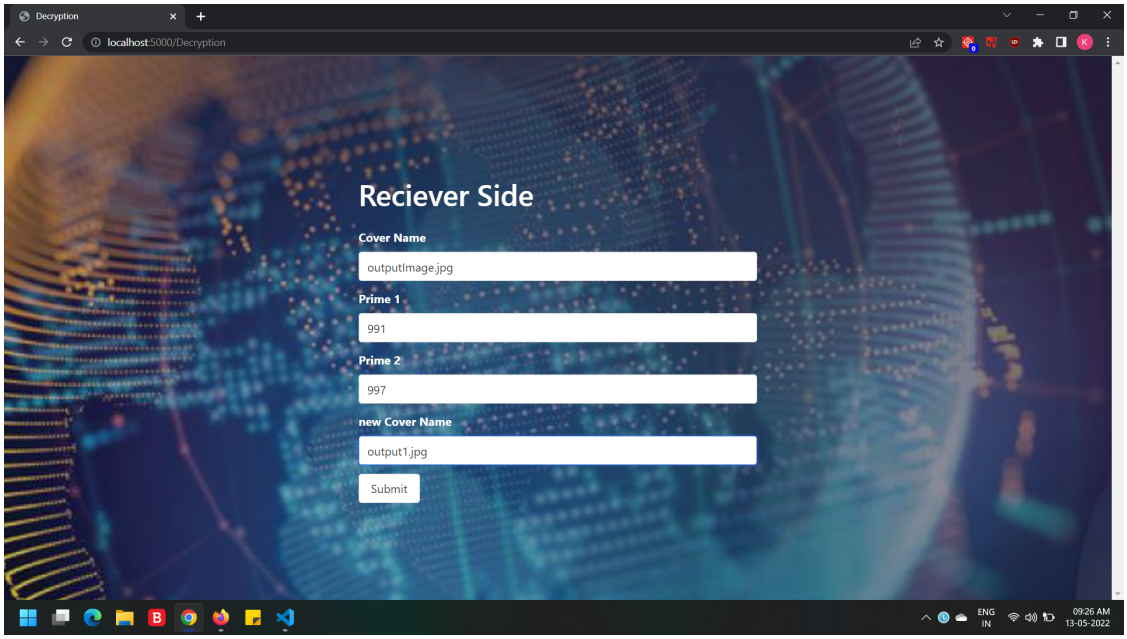


Figure 3: decryption Page

Testing analysis

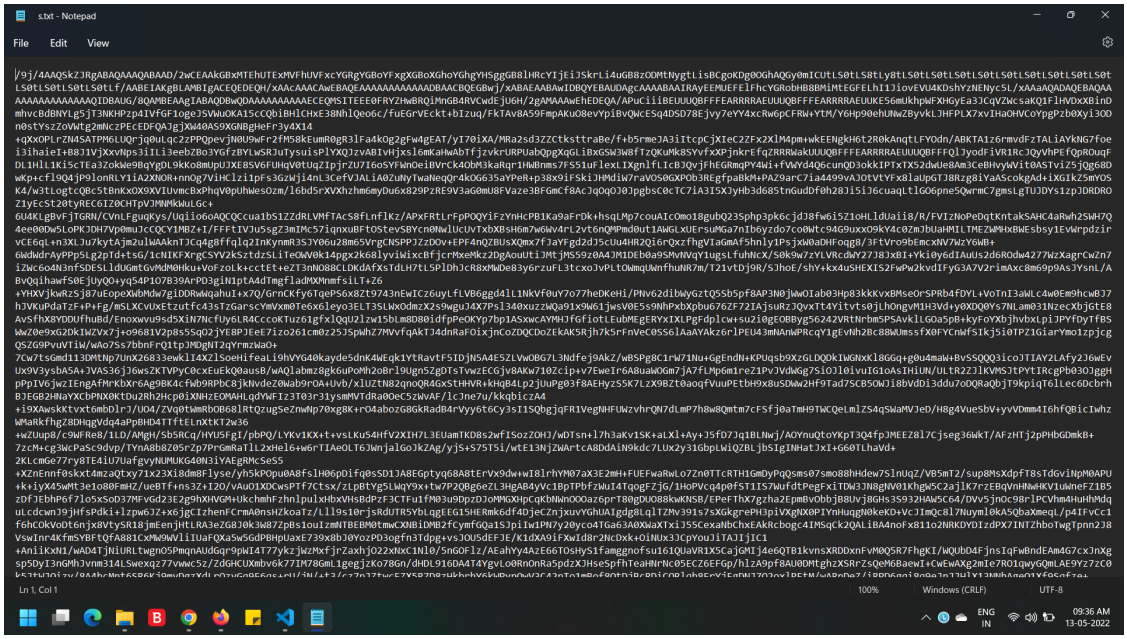


Figure 4: Image encryption data

Figure 5: Image Decryption

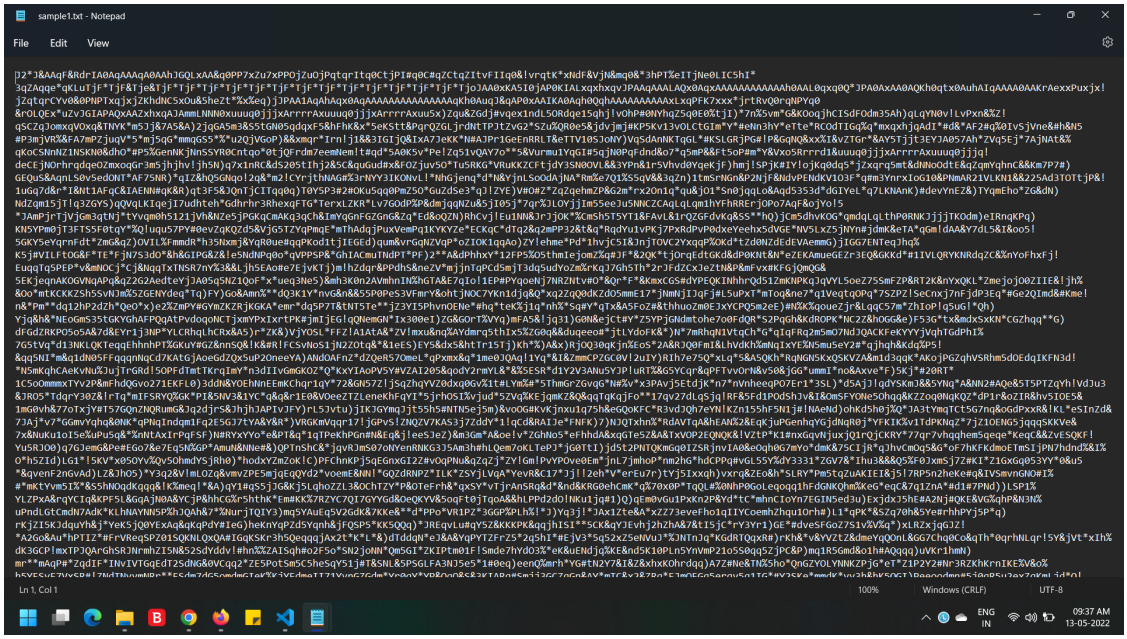


Figure 6: RSA encryption

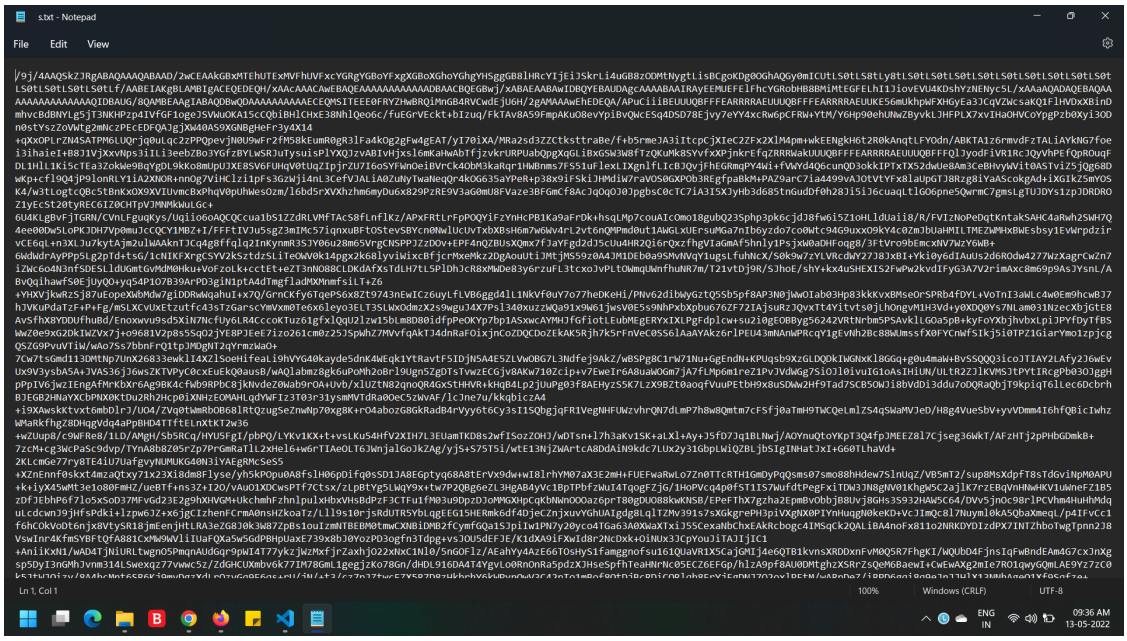


Figure 7: RSA decryption

7 CONCLUSION AND FUTURE SCOPE

Here, we deal with security required while digital data communication on network. This project is on designing combined steganography and cryptography features for better performance. Also, we performed Steganography with RSA key algorithm.Here data is in image so attacker will not able to find that data. We implemented it using python program. This method successful hide image, audio, video or colour image. By this we observed that in this method image with RSA is batter because of its high capacity.

Using this scheme, we can transmit big size of secret data and provide secure communication between two nodes across network. The embedding data like image, audio, video done in image prevent hance for attacker to detect data being hiden. Results achieved show that our proposed method is encouraging in terms of security, and robustness.

References

[1] Sangivalasa, bheemili mandal, visakhapatnam dist.(A.P), SECURE DATA ENCRYPTION AND DECRYPTION USING CRYPTO-STEGO, International Journal of Research and Analytical Reviews (IJRAR), 2019 - 2020

[2] Data security using cryptography and steganography techniques, Saleh, Marwa E and Aly, Abdelmgeid A and Omara, Fatma A, 2016, (IJACSA) International Journal of Advanced Computer Science and Applications

[3] https://github.com/kenil-bhingradiya/secure-data-using-cryptogrphy-and-steganography

[4] https://www.youtube.com/watch?v=Te8Cao2Smsk

[5] H.Abdulzahra, R. AHMAD, and N. M. NOOR, "Security enhancement; Combining cryptograhy and steganography for data hiding in images," ACACOS, Applied Computational Science,pp.978-960,2014.