***Image Cryptography using RSA and AES Algorithm***

## 

## B.Tech. Report Submitted

**In partial fulfilment for VIII-semester, course PRT-S402**

**of Bachelor of Technology**

**In**

**Computer Science and Engineering**

**Submitted by**

**Aditya Kumar Singh (CSJMA14001390004)**

**Supriya Singh (CSJMA14001390045)**

**Department of Computer Science and Engineering**

**University Institute of Engineering and Technology**



**Chhatrapati Shahu Ji Maharaj University, Kanpur**

**CERTIFICATE**

This is to certify that the project report entitled **Image Cryptography using RSA and AES** **Algorithm**  submitted by Aditya Kumar Singh (CSJMA1400139004) Supriya Singh(CSJMA14001390045) to the Department of Computer Science and Engineering, University Institute of Engineering and Technology, CSJM University, Kanpur, in partial fulfilment for VIII-semester course PRT-S402, their work is original and has been carried out under my supervision. The contents of this report, in full or part, has not been submitted to any other Institute or University for the award of any degree or diploma.

**Date: 22 APRIL 2018 Signature of Project Supervisor**

**Er. Mohd. Shah Alam**

**Counter Signature of Head of Department**

Computer Science and Engineering Department

University Institute of Engineering and Technology

CSJM University, Kanpur,

**DECLARATION**

We declare that this project report **Image Cryptography using RSA and AES Algorithm** submitted in partial fulfilment for VIII semester course PRT-S402 of B.Tech. program in Computer Science and Engineeringis an original work carried out by us under the supervision of Er. Mohd. Shah Alamand has not formed the basis for the award of any other degree, in this or any other Institution or University.

**Aditya Kumar Singh Supriya Singh**

**(CSJMA14001390004) (CSJMA14001390045)**

**ACKNOWLEDGEMENT**

We would like to express my sincere gratitude to my supervisor Er. Mohd Shah Alam for providing her invaluable guidance, comments and suggestions throughout the course of the project. we wish to express my indebtedness to her for introducing the present topic, providing me with the required data and analysing the work done by me on regular intervals.

Above all no words can express my feelings to my friends and all those persons who supported me during the project. we are also thankful to all the respondents whose cooperation & support has helped me a lot in collecting necessary information.

**Aditya Kumar Singh (CSJMA14001390004)**

**Supriya Singh (CSJMA14001390045)**

Computer Science and Engineering Department

University Institute of Engineering and Technology

CSJM University, Kanpur, U.P.

**OPERATING ENVIRONMENT**

**SOFTWARE REQUIRED**

Visual studio

**PROGRAMMING LANGUAGE**

C#

**ABSTRACT**

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication. In data and telecommunications, cryptography is necessary when communicating over any unreliable medium, which includes any network particularly the internet. In today’s era it is a crucial concern that proper encryption decryption should be applied to transmit the data from one place to another place across the internet in order to prevent unauthorized access. Image Cryptography is a special kind of encryption techniques to hide data in an image for encryption and decryption of original message based on some key value. Very few algorithms, provides computational hardness and it makes difficult to break a key to find the original message. Here we use RSA and AES algorithm used to encrypt the image files to enhance the security in the communication area for data transmission. An image file is selected to perform encryption and decryption using key generation technique to transfer the data from one destination to another.

|  |
| --- |
| TABLE OF CONTENT  1 INTRODUCTION  1.1 WHAT IS CRYPTOGRAPHY ………………………………………………….………………...9  1.2 SYMETRIC KEY CRYPTOGRAPHY…….....……………… …………………………….…..10  1.3 PUBLIC KEY CRYPTOGRAPHY……………………………………….………...…………...10  1.4 GOALS OF CRYPTOGRAPHY………………….……………………...……………………...11  1.5 PUBLIC -PRIVATE KEY……………………………………………….………………………11    2 LITERATURE STUDY OF RSA  2.1 IMAGE CRYPTOGRAPHY USING RSA…………………….……………………….……….12  2.2 STEPS IN RSA……………………………………………………………….………………….13    3 MEHODOLOGY USED IN RSA  3.1 ENCRYPT THE IMAGE…………………..……………………………..……………………….14  3.2 DECRYPT THE IMAGE……………………..……………………………..…………………….15  4 IMAGE CRYPTOGRAPHY USING AES  4.1 INTRODUCTION.…………………………………………………………...…………..……….16  5 LITERATURE STUDY OF AES  5.1 ENCRYPTION…………………………………….………………………………………………17  5.1.1 Sub bytes transformation……………………………………………………………...………..18  5.1.2 Shift Row………………………………………………………………………………...……..18  5.1.3 Mix Columns……………...……………………………………………….…………………...19  5.1.4 Add Round Key……………..………………………………………………………………….19  5.1.5 Key Expansion…………………………………………………………………….…………...20  5.2 DECRYPTION ….……………………………………………………………..…………………..20  5.2.1 Inverse Shift Row Transformation….………………………………………..………………...22  5.2.2 Inverse Sub-Byte Transformation….………………………………………...………………...22  5.2.3 Inverse Mix Column….………………………………………..………….….………………..22  5.2.4.Inverse Add Round Key….……………………………..……..………….….……….………..23  6 MEHODOLOGY USED IN AES  6.1 ENCRYPTING THE IMAGE…………………………………………………………………….24  6.2 DECRYPT THE IMAGES……………………………………………………………………..…25  7. RESULT and CONCLUSION  7.1-RESULT……………………………………………………………………...…………………...27  7.2-Issue In RSA Algorithm During Implementation…………………………….…………………..28  7.2-Issue In AES Algorithm During Implementation……………………..…….……………………28  7.3-CONCLUSION…………………………………………………………………………………...28 |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| FIG NO | NAME OF THE FIGURE | PAGE NO |
| Fig-1.1 | A Simple cryptographic model | 07 |
| Fig-1.2.a | Asymmetric key cryptographic model | 08 |
| Fig-1.2.b | Public key cryptography | 08 |
| Fig-2.1 | RSA algorithm phase | 10 |
| Fig-2.2 | RSA algorithm steps | 11 |
| Fig-3.1.1 | Select operation | 12 |
| Fig-3.1.2 | RSA encryption of images | 12 |
| Fig-3.2.1 | Load cipher for decryption | 13 |
| Fig-3.2.2 | RSA decryption of images | 13 |
| Fig-5.1 | General structure of encryption | 15 |
| Fig-5.1.2 | Box operation on individual byte | 16 |
| Fig-5.1.3 | Affine transformation | 16 |
| Fig-5.1.4 | Left rotation used for decryption | 16 |
| Fig-5.1.5 | Mix column operator | 17 |
| Fig-5.1.6 | Round byte key XOR with data byte | 18 |
| Fig-5.1.7 | Key expansion operation | 19 |
| Fig-5.2.1 | General structure of decryption | 19 |
| Fig-5.2.2 | Inverse sub byte transformation | 20 |
| Fig-5.2.3 | Inverse matrix column | 21 |
| Fig-6.1.1 | Select operation | 22 |
| Fig-6.1.2 | Encryption open page | 23 |
| Fig-6.1.3 | Encryption done | 23 |
| Fig-6.1.4 | Decryption done | 24 |
| Fig-6.1.5 | Error while decryption | 25 |
| Fig-7.2.1 | Image Set Original and after decryption | 27 |

**Chapter 1**

1. **INTRODUCTION**



**1.1 WHAT IS CRYPTOGRAPHY**

The word cryptographyhas come from a Greek word, which means *secret writing*. In the present day it refers to the tools and techniques used to make messages secure for communication between the participants and make messages immune to attacks by hackers. For private communication through public network, cryptography plays a very crucial role.

**Plain text-**

The message to be sent through an unreliable medium is known as plaintext*,* which is encrypted before sending over the medium.

**Cipher text-**

The encrypted message is known as ciphertext, which is received at the other end of the medium.

Decrypted to get back the original plaintext message.

Cryptography divided into two broad categorize –

1. Symmetric key cryptography
2. Public key cryptography**.**

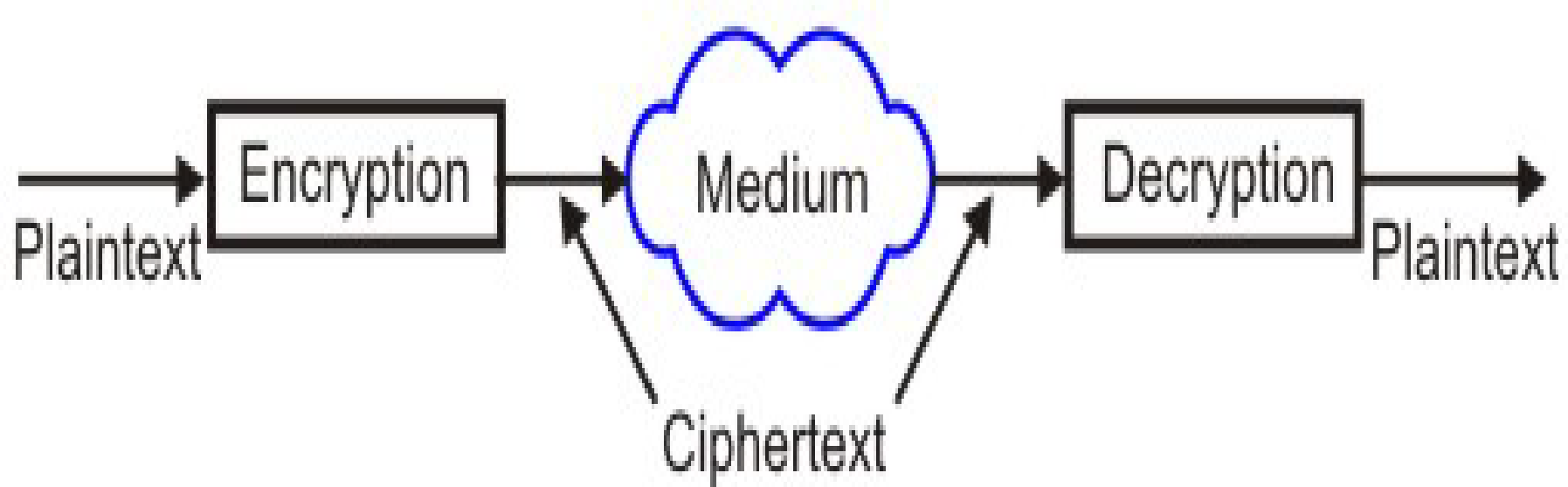


Fig 1.1 A Simple Cryptography Model

**1.2 SYMMETRIC KEY CRYPTOGRAPHY**

Secret key cryptography is also known as symmetric key cryptography. In this type both the sender and the receiver know the same secret key. The sender is encrypted the data or the information using the secret key and the receiver is decrypt the information using the same secret key. In the symmetric cryptography the key is playing a very important role which is depends on the nature of key.

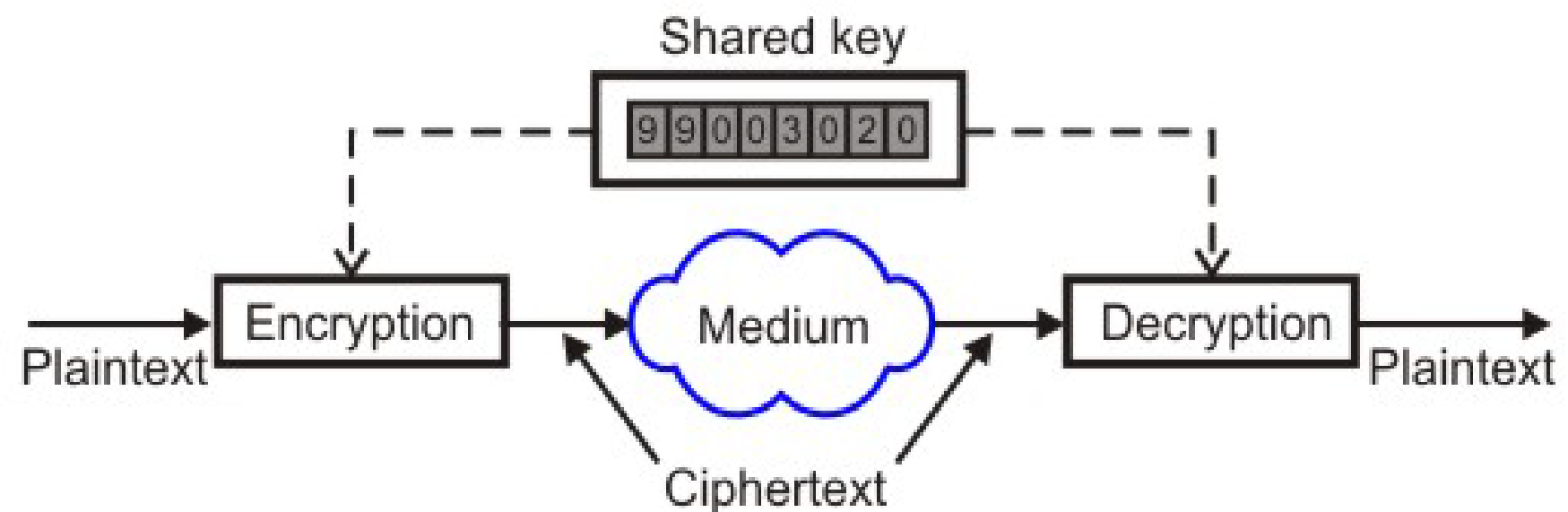


Fig – 1.2A Symmetric Key Cryptography

**1.3-PUBLIC KEY CRYPTOGRAPHY**

Asymmetric cryptography is used encryption and decryption algorithm pair. With public key cryptography, keys work in pairs of matched public and private keys. Public key cryptography, also called asymmetric key cryptography which is using a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys. The cryptography technique is using the secret message transfer from one place to another place over the networks. The cryptography technique is requiring some algorithms for encrypt the data.

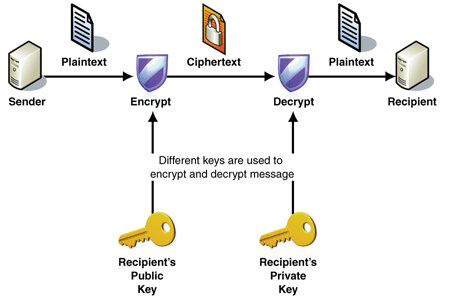


Fig – 1.2B Public Key Cryptography

**1.4 GOAL OF CRYPTOGRAPHY**

**1. Confidentiality**

The transmission of data from one computer to another computer has to be accessed by an authorized user and it not access by anyone else.

**2. Authentication**

The transmission of data from one computer to another computer has to be accessed by an authorized user and it not access by anyone else.

**3. Integrity**

Only the authorized party is allowed to modify the transmitted information. And an unauthorized person should not allow to modify in between the sender and receiver.

**4. Non-Repudiation**

Ensures the message that sender or the receiver should be able to deny the transmission.

**5. Access control**

The authorized persons only able to access the information while in transfer.

**1.5 PUBLIC AND PRIVATE KEY**

Every host have both its own public and private key. On those keys the public key can be know everyone and it is use for encrypting messages. Messages encrypted with the public key can decrypt using the private key. It means every host have database of public key of other host, suppose A want send data to B so A have a public key of B

so, he encrypts the message through A’s public key. Now that message is decrypted by B’s public key which is kept only by B.It means private key is not spread everywhere. Every host have its private key, which cannot access by everyone, but public key is totally opposite, public key are spread over the network and easily accessed by other host.

**Chapter 2**

**2.LITERATURE STUDY (RSA)**



**2.1 IMAGE CRYPTOGRAPHY BY USING RSA**

The RSA is a cryptographic algorithm which is useto encrypt and decrypt the data. This algorithm developed in1977 by Ron Rivest, Adi Shamir, and Leonard Adelman. RSA cryptosystem is also known as the public-key cryptosystems. RSA is normally used for secure data transmission. The encryption is starting on the RSA algorithm with the selection of two large prime numbers, along with an auxiliary value, as the public key. The prime numbers are keep in secret. The public key is used to encrypt a message, and private key is used to decrypt a message or information.

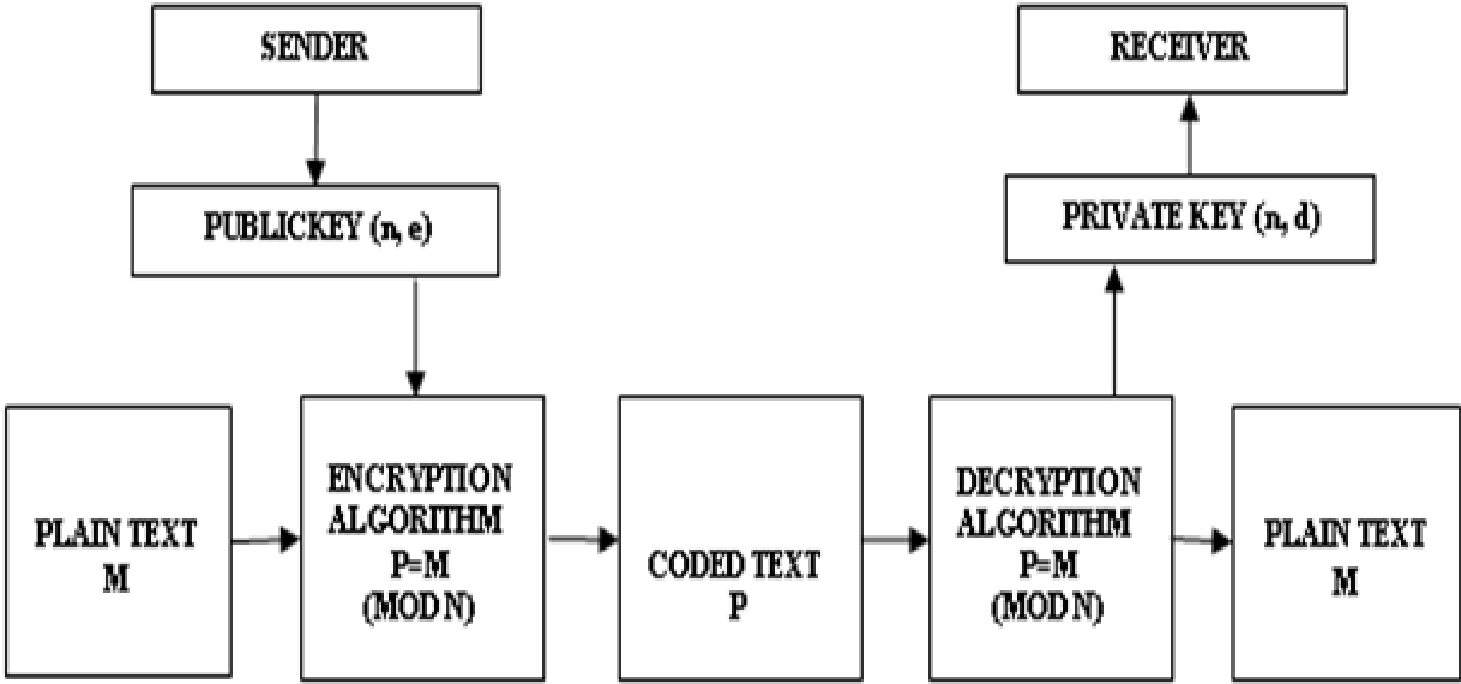


Fig – 2.1 RSA Algorithm Phases

The RSA algorithm is also called as an asymmetric cryptographic algorithm. Asymmetric cryptosystem means two different keys are using in the encryption and decryption.

**2.2 Steps in RSA**

1. Key Generation

2. Encryption

3. Decryption

1. **Key Generation**

The key generation is the first step of RSA algorithm. The RSA involves a public key and a private key. On those keys the public key can be know everyone and it is use for encrypting messages. The keys for the RSA algorithm is generated by the following steps,

1. First choose the two distinct prime numbers p and q.

2. For security purposes, the integer p and q should be chosen, and it should be the similar bit-length. Prime integers can be efficiently found by a primality testing.

3. Then compute the n value, n = pq.

4. n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

5. Compute φ(n) = φ(p)φ(q) = (p − 1)(q − 1) = n - (p + q -1), where φ is Euler's totient function. This value is kept private.

6. Choose an integer e such that 1 < e < φ(n) and gcd (e, φ(n)) = 1; i.e., e and φ(n) are co-prime. e is the released as the public key. e has a short bit-length and small Hamming weight results in more efficient encryption. However, much smaller values of e have been shown to be less secure in some settings.

7. Determine d as d ≡ e−1 (mod φ(n)); i.e., d is the modular multiplicative inverse of e (modulo φ(n)). This is stated as, solve the d given d⋅e ≡ 1 (mod φ(n)). This is computed using extended Euclidean algorithm. It using the pseudo code in the Modular integers section, inputs a and n correspond to e and φ(n), respectively.

8. d value is keep as the private key. The public key consists of the modulus n and the

public key e. The private key have the modulus n and the private key d, and it keep in secret. p, q, and φ(n) values are keep in secret, because they can be used to calculate value of d.

1. **Encryption**

CIPHER TEXT = (PLAIN TEXT) ^e MOD N

After encryption image get converted into hex image.

1. **Decryption**

PLAIN TEXT= (CIPHER TEXT) ^d MOD N

In decryption again, the hex code is preserved as image.

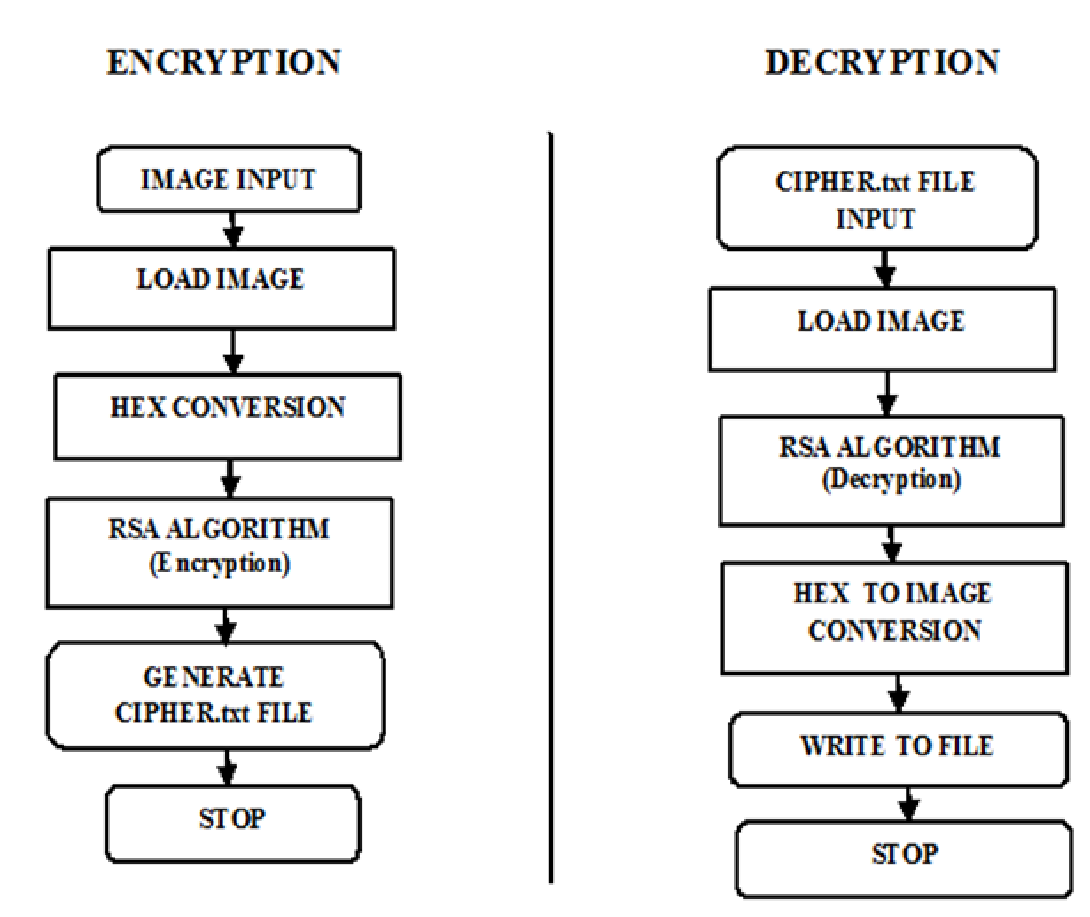


Fig – 2.2 RSA Algorithm Steps

**Chapter 3**

**3. METHODOLOGY (RSA)**

The following steps are used to Encrypt and Decrypt an image using the RSA Algorithm in the applied project work.

**3.1 Encrypting the Image**

STEP-1

Select encryption option.

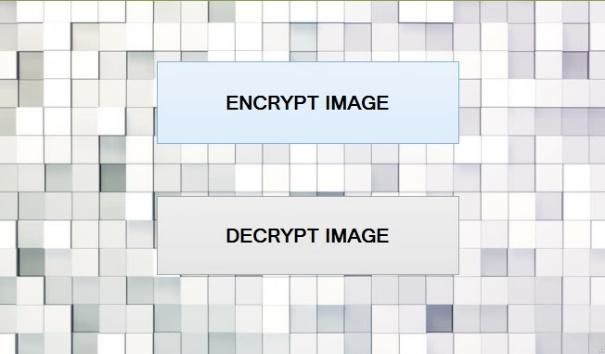


Fig – 3.1.1 Select Operation

STEP-2

load image that we want to encrypt.by click on open file

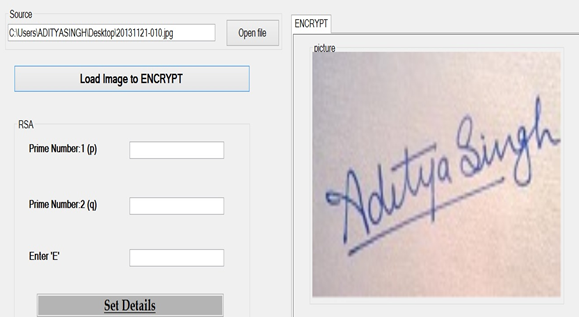


Fig –3.1.2 RSA Encryption of Image

STEP-3

Enter the valve of p and q as prime number

Click on set detail.on click the image convert in Hex form.

STEP-4

now image is encrypted.This hex image is called as cipher text.

**3.2 Decrypting the Image**

STEP-1

Decrypt the image by load cipher

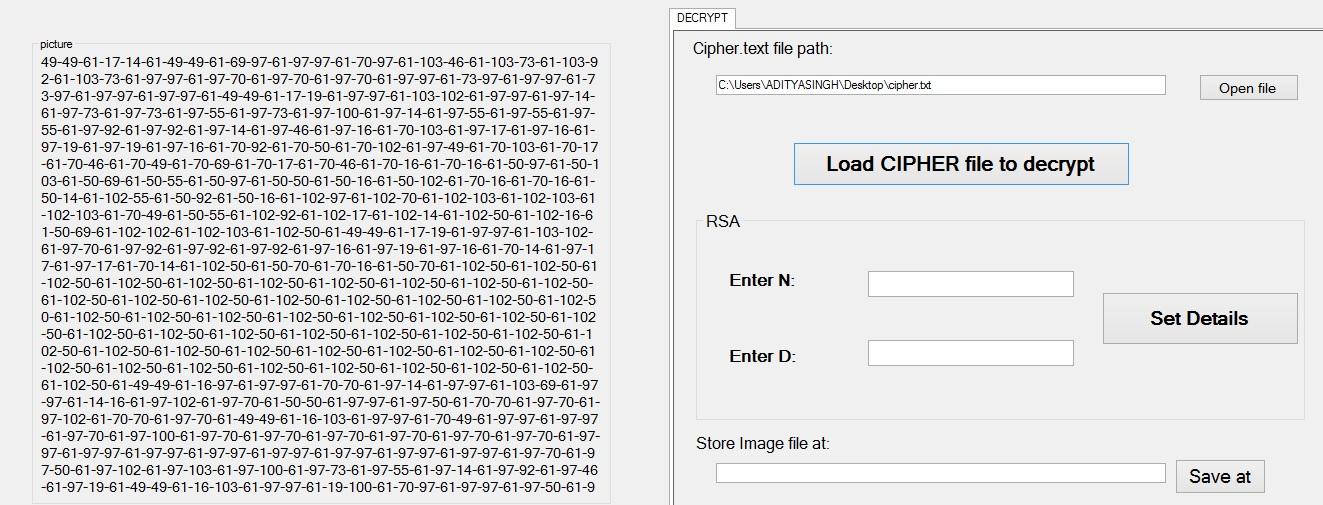


Fig –3.2.1 Load Cipher for Decryption

STEP-2

Enter the suitable valve of n and d.acc to algo and set detail if we give any wrong input then it always send you message” access denied”.

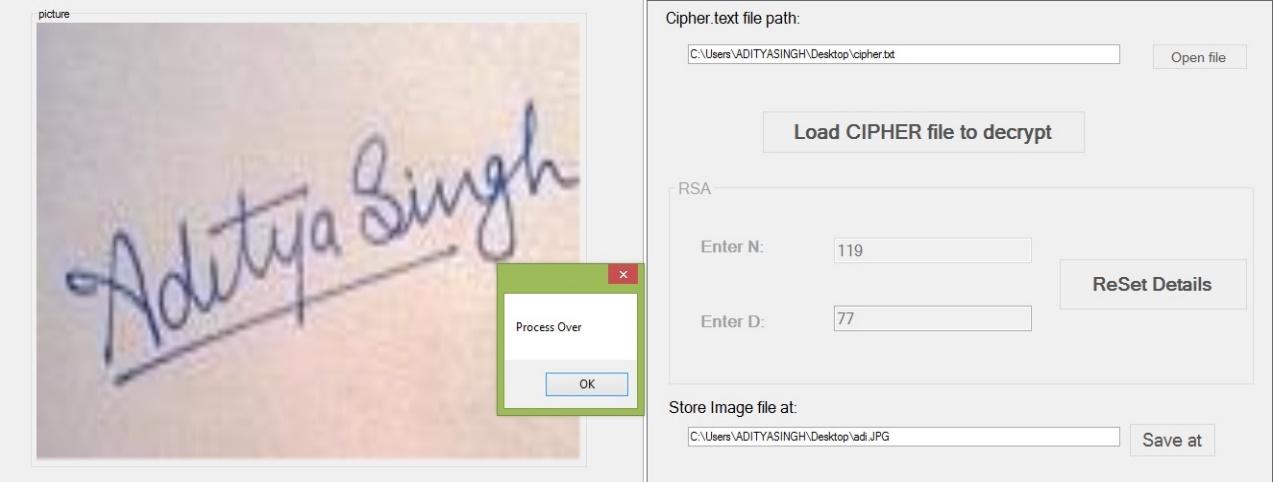


Fig –3.2.2 RSA Decryption of Image

**IMAGE CRYPTOGRAPHY BY USING AES (ADVANCED ENCRYPTION ALGORITHM)**

**Chapter 4**

**4. INTRODUCTION**

AES is a symmetri*c* encryption algorithm processing data in block of 128 bits. AES is symmetric since the same key is used for encryption and the reverse transformation, decryption. The only secret necessary to keep for security is the key. AES may have configured to use different key-lengths, the standard defines 3 lengths and the resulting algorithms are named AES-128, AES-192 and AES-256 respectively to indicate the length in bits of the key.

In our project work we study and work on AES-128 for Encryption and Decryption of the Image Data. The Encrypted data is stored in the disk in the form of Cipher text which is used for transmitting over the network or to share with privacy, this Cipher Text is again converted to Image form using Decryption process and the authentic key values.

For both its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations:

1. Byte substitution using a substitution table (S-box),

2. Shifting rows of the State array by different offsets,

3. Mixing the data within each column of the State array, and

4. Adding a Round Key to the State.

**Chapter 5**

**5.LITERATURE STUDY (AES)**



**5.1 Encryption**

In encryption mode, the initial key is added to the input value at the very beginning, which is called an initial round. This is followed by 9 iterations of a normal round and ends with a slightly modified final round, as one can see in Figure 5.1. During one normal round the following operations are performed in the following order: Sub Bytes, Shift Rows, Mix Columns, and Add Round key. The final round is a normal round without the Mix Columns stage.

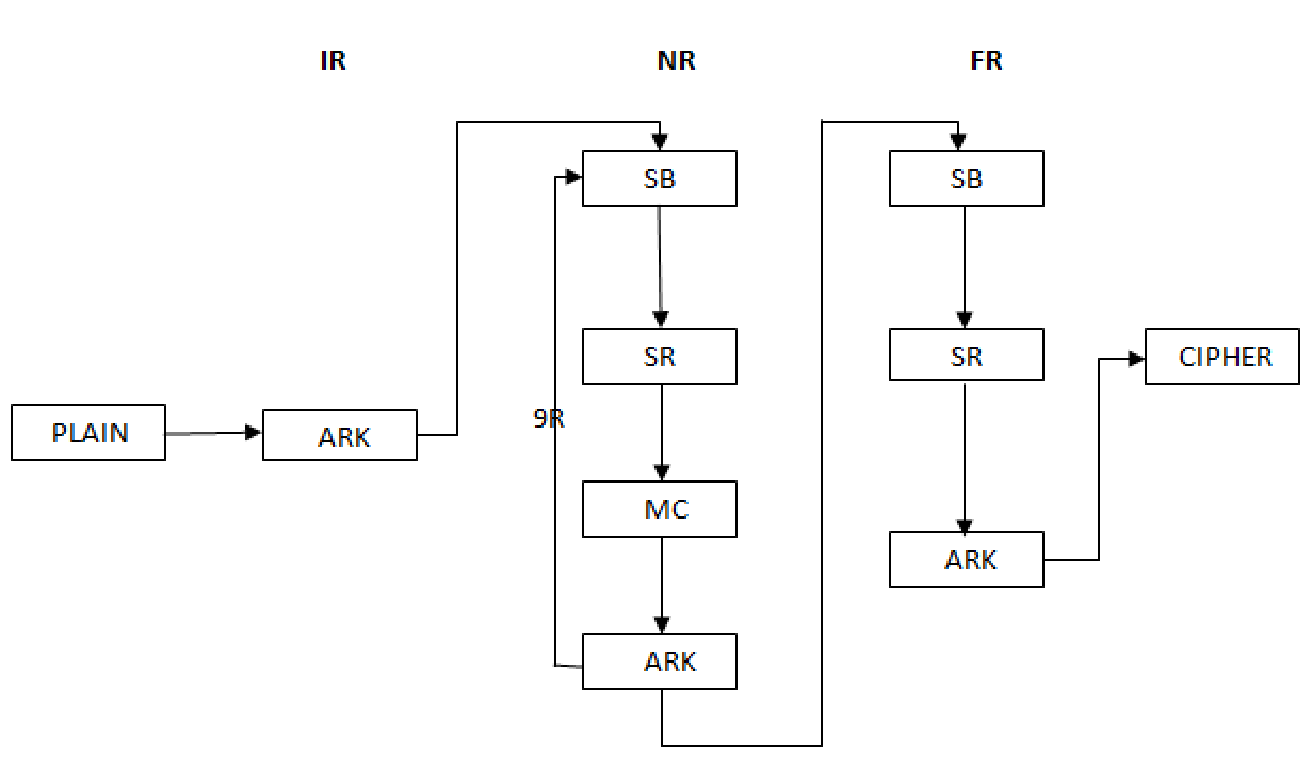
****

Fig-5.1 General structure of encryption

**Steps in AES Encryption**

Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.

Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column

Add Round Key—each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

**5.1.1 Sub bytes transformation**

The Sub Bytes transformation is a non-linear byte substitution that operates independently on each byte of the State using a substitution table (S-box). This S-box which is invertible is constructed by composing two transformations:

Take the multiplicative inverse in the finite field GF (28), the element {00} is mapped to itself.

Apply the following affine transformation.

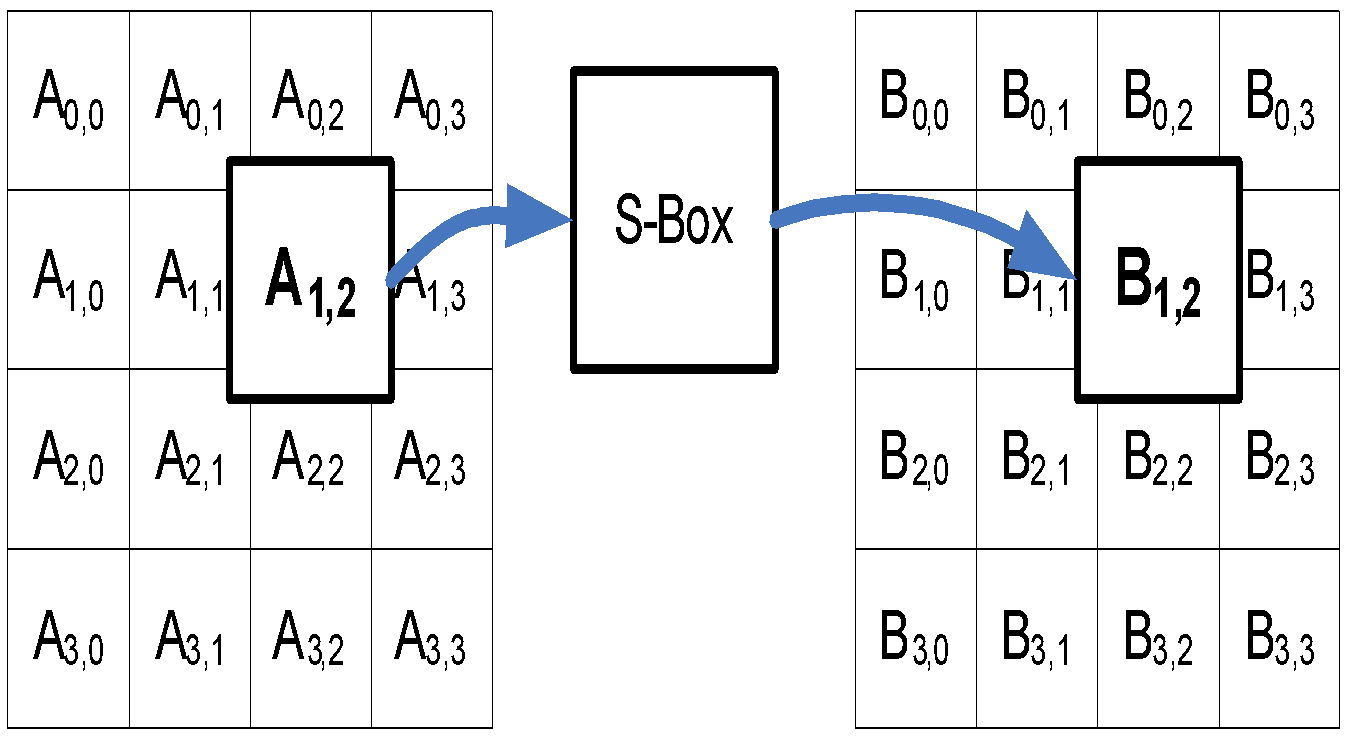
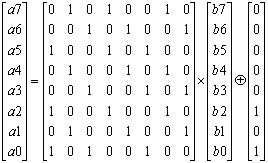
 

Fig 5.1.2 S-box operation on individual bytes Fig 5.1.3 Affine Transformation

**5.1.2 SHIFT ROW**

The Shift Row operation affects each of the four rows of data individually. Each row is rotated by a different amount. The first row is unchanged and rows two through four are rotated by one, two, and three bytes respectively. For encryption a right rotation is performed while for decryption a left rotation is used. The result of the shift on the data matrix representing the data.

The shift value shift(r,Nb) depends on the row number, *r*, as follows (recall that Nb = 4): shift(1,4) shift(2,4) shift(3,4) .This has the effect of moving bytes to lower‖ positions in the row (i.e., lower values of *c* in a given row), while the lowest‖ bytes wrap around into the top of the row (i.e. higher valves of c in given row)

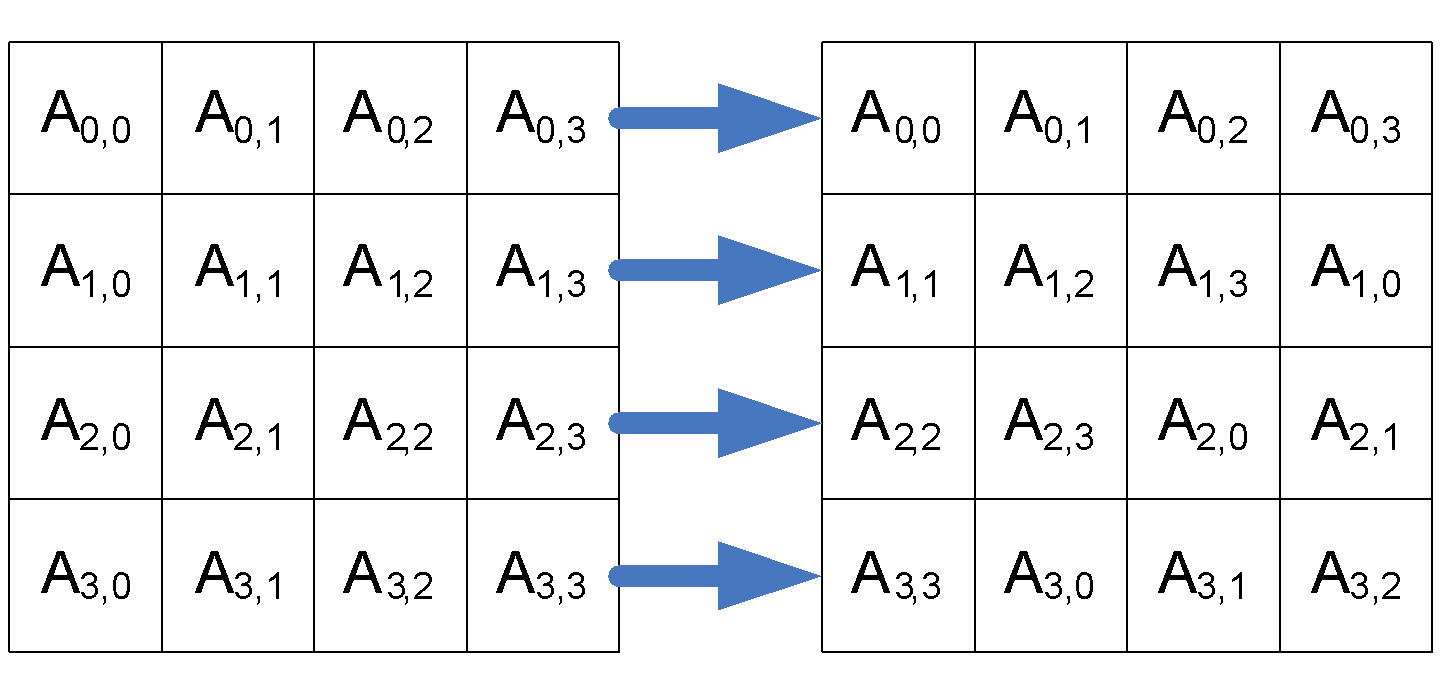


Fig5.1.4 Left Rotation Used For Decryption

**5.1.3 MIX COLUMNS**

The Mix Columns operation transforms the data in the current state by operating on each of the four columns independently. For this operation each column of the data is treated as a polynomial over GF(256). The polynomial is multiplied by a fixed polynomial and the result is taken modulo x4 + 1. The fixed polynomial used for decryption is the inverse of the polynomial used for encryption in the field GF(256) modulo x4 + 1. The encryption polynomial is 3x3 + 1x2 + 1x + 2. The inverse of this polynomial is 11x3 + 13x2 + 9x + 14.

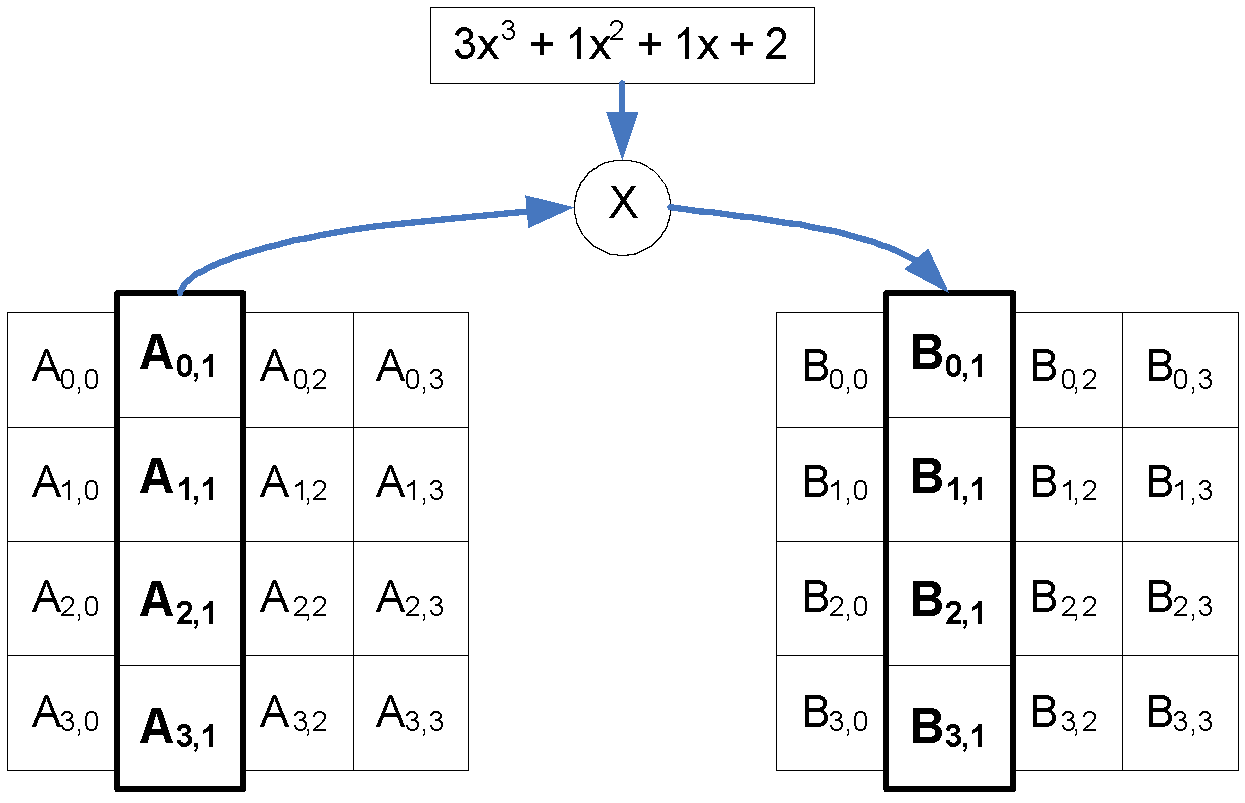


Fig-5.1.5 Mix Column Operator

The encryption and decryption for the Mix Columns operation were implemented in different ways. The polynomial used for encryption was specifically selected to make the computation very easy to implementThis implementation requires the use of memory which has a higher space requirement but is easier to implement and operates much faster.

**5.1.4 ADD ROUND KEY**

The Add Round Key operation performs a simple XOR between the current state data values and the round key for the current round. The round key is obtained from the key selector block based on the value of the expanded key and the current round.

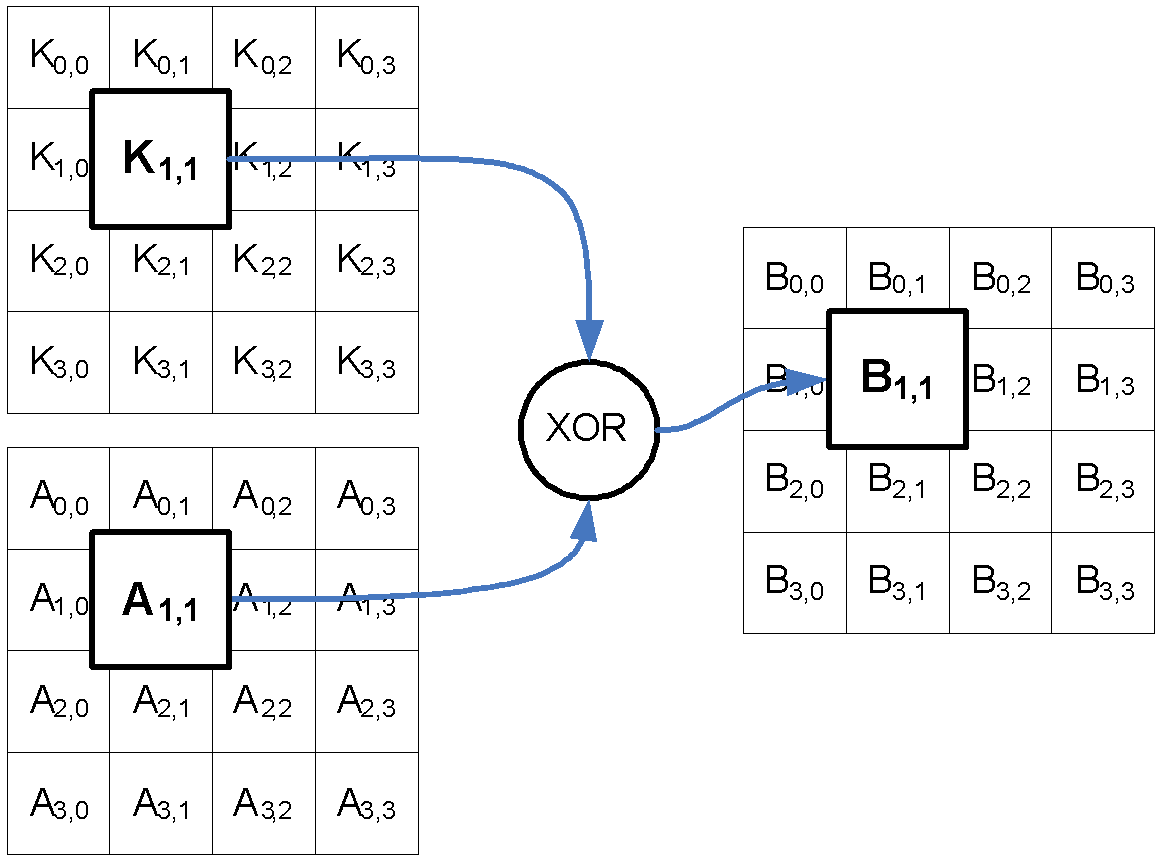


Fig-5.1.6 Round Byte Key (K) Xor With Data Byte (A)

**5.1.5 KEY EXPANSION**

The AES algorithm takes the Cipher Key, *K*, and performs a Key Expansion routine to generate a key schedule. The Key Expansion generates a total of Nb (Nr + 1) words: the algorithm requires an initial set of *Nb* words, and each of the Nrrounds requires Nbwords of key data. The resulting key schedule consists of a linear array of 4-byte words, denoted [wi], with *i* in the range 0 < i < Nb(Nr + 1). The expansion of the input key into the key schedule proceeds according to the pseudo code. SubWord is a function that takes a four-byte input word and applies the S-box to each of the four bytes to produce an output word. The function Rot Word takes a word [*a*0,*a*1,*a*2,*a*3] as input, performs a cyclic permutation, and returns the word [*a*1,*a2,a3,a0*It is important to note that the Key Expansion routine for 256-bit Cipher Keys (Nk= 8) is slightly different than for 128- and 192-bit Cipher Keys. If Nk= 8 and i-4 is a multiple of Nk, then SubWord () is applied to w [i-1] prior to the XOR.

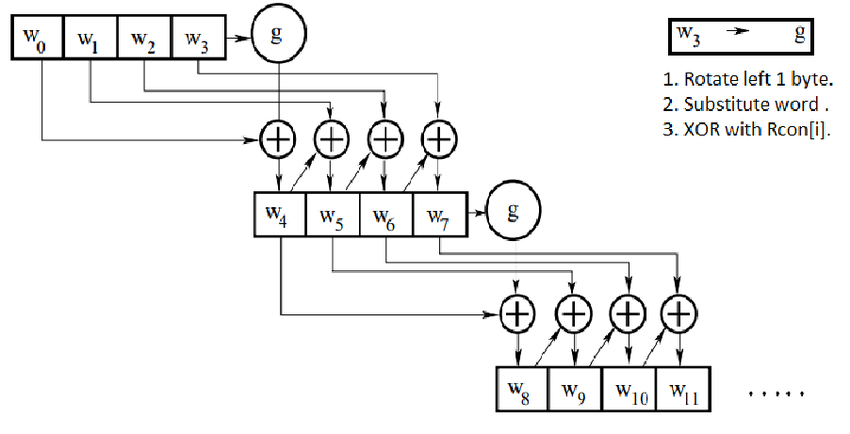


Fig-5.1.7 Key Expansion Operation

**5.2 DECRYPTION**

In decryption mode, the operations are in reverse order compared to their order in encryption mode. Thus, it starts with an initial round, followed by 9 iterations of an inverse normal round and ends with an Add Round Key. An inverse normal round consists of the following operations in this order: Add Round Key, Inv Mix Columns, Inv Shift Rows, and Inv Sub Bytes. An initial round is an inverse normal round.

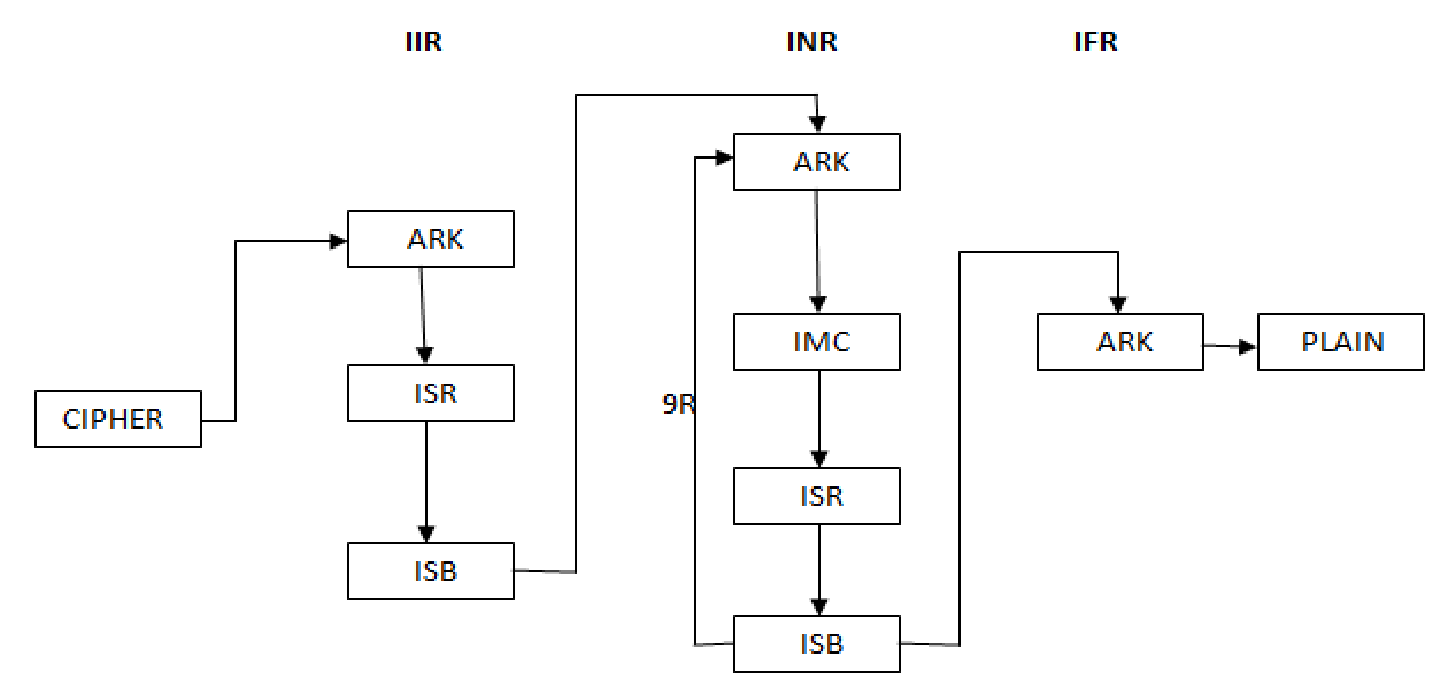
****

Fig-5.2.1 General Structure of Decryption

**STEP INVOLVED IN DECRYPTION**

**5.2.1 Inverse Shift Row Transformation**

Inv Shift Rows is the inverse of the Shift Rows transformation. The bytes in the last three rows of the State are cyclically shifted over different numbers of bytes (offsets). The first row, *r* = 0, is not shifted. The bottom three rows are cyclically shifted by Nb shift(r, Nb) bytes, where the shift value shift(r,Nb*)* depends on the row number.

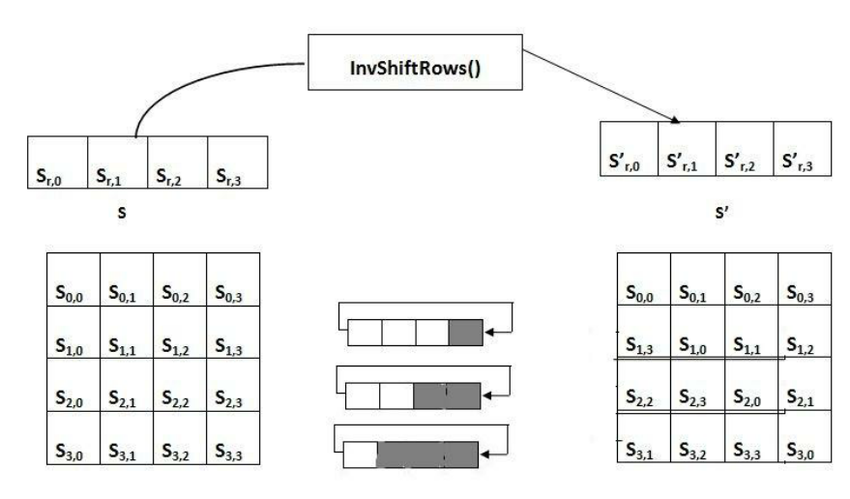


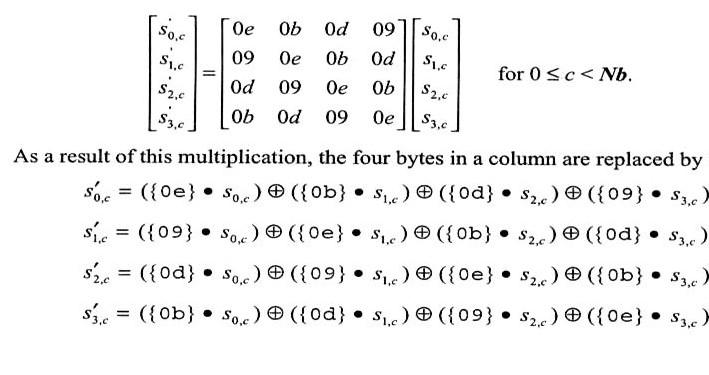
Fig-5.2.2 Inverse Shift Row Transformation

**5.2.2 Inverse Sub-Byte Transformation**

InverseSubBytes is the inverse of the byte substitution transformation, in which the inverse Sbox is applied to each byte of the State. This is obtained by applying the inverse of the affine transformation followed by taking the multiplicative inverse in GF (28).The inverse S-box used in the InvSubBytes () transformation.

**5.2.3 Inverse Mix Column**

InverseMixColumns is the inverse of the Mix Columns transformation. Inv Mix Columns operates on the State column-by-column, treating each column as a four term polynomial. The columns are considered as polynomials over GF (28) and multiplied modulo *x*4 + 1 with a fixed polynomial *a*-1(*x*), given by *a*-1(*x*) = {0b} *x3* + {0d} *x2* + {09} *x* + {0e}, this can be written as a matrix multiplication. Let As a result of this multiplication, the four bytes in a column are replaced by the following:



**5.2.4.INVERSE ADD ROUND KEY**

Add Round Key is its own inverse since it only involves an application of the XOR operation. Equivalent Inverse Cipher transformations differ from that of the Cipher, while the form of the key schedules for encryption and decryption remains the same. However, several properties of the AES algorithm allow for an Equivalent Inverse Cipher that has the same sequence of transformations as the Cipher (with the transformations replaced by their inverses). This is accomplished with a change in the key schedule. The two properties that allow for this Equivalent Inverse Cipher are as follows: The Sub Bytes and Shift Rows transformations commute; that is, a Sub Bytes transformation immediately followed by a Shift Rows transformation is equivalent to a Shift Rows transformation immediately followed by a Sub Bytes transformation.

The same is true for their inverses, Inv Sub Bytes and Inv Shift Rows. The column mixing operations – Mix Columns and Inv Mix Columns – are linear with respect to the column input, which means Inv Mix Columns (state XOR Round Key) =Inv Mix Columns(state) XOR InverseMixColumns(Round Key).

**Chapter 6**

**6. METHODOLOGY (AES)**

The following steps are used to Encrypt and Decrypt an image using the AES Algorithm in the applied project work.

**6.1 Encrypting the Image**

STEP-1

Select encryption option.

****

Fig – 6.1.1 Select Operation

STEP-2

load image that we want to encrypt.by click on open file**.**

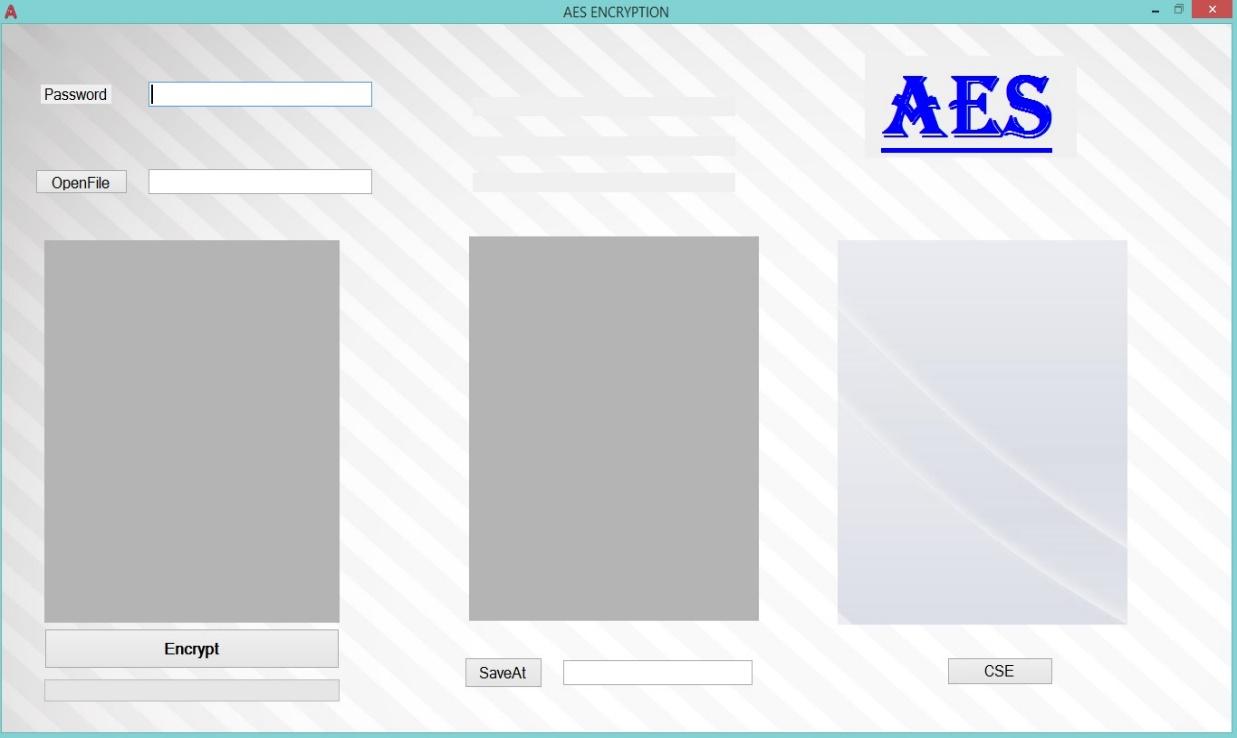
****

Fig – 6.1.2 Encryption Operation Page

STEP-3

Enter the value of the Password for Encryption

Click on saveAt to save text file.

STEP-4

Encrypt the Image as cipher text.



Fig – 6.1.3 Encryption Done

**6.2 Decrypting the Image**

STEP-1

Load the cipher text and enter the password value same as used in Encryption of the Image.

STEP-2

Choose the destination where image is to be saved.

Decrypt the Cipher text. If the given password field value is different from the initial given value used during Encryption, then it gives Error Message.

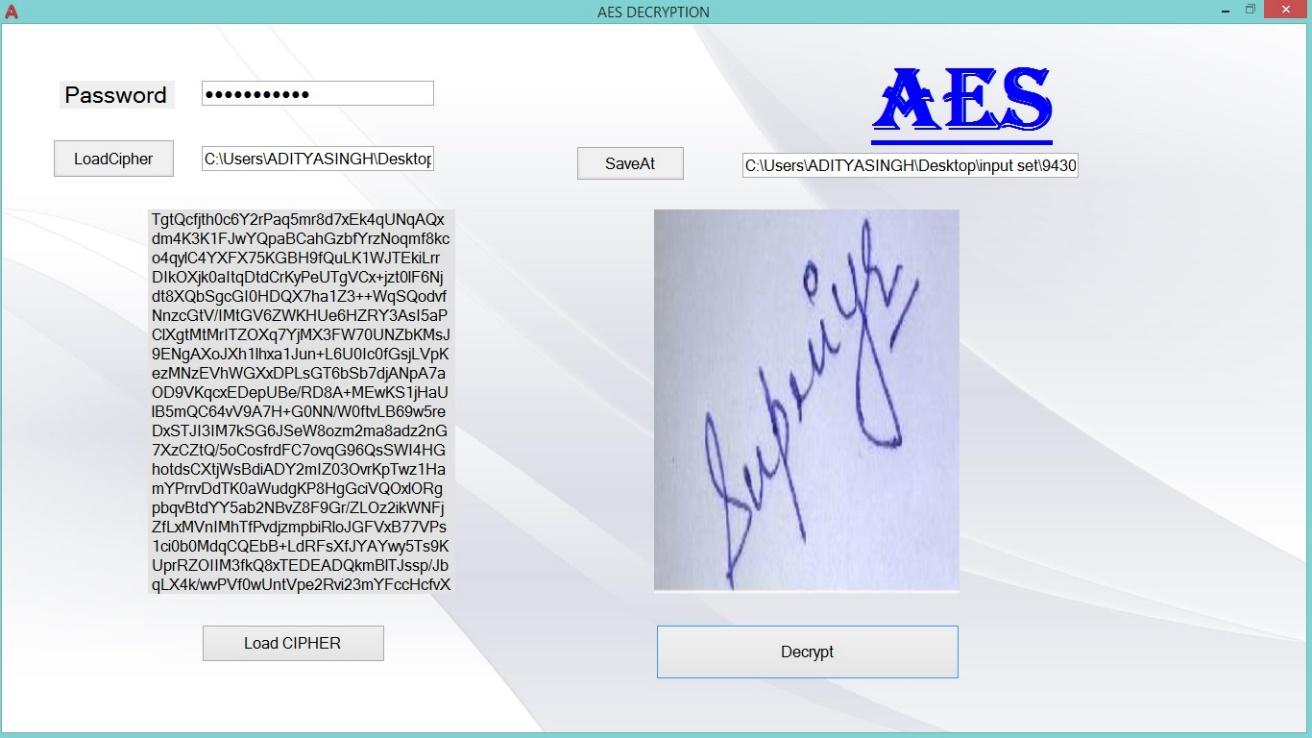
****

Fig – 6.1.4 Decryption Done

if the wrong password value is provided then the “Wrong Input Given “ message is viewed and the image shown as ACCESS DENIED.

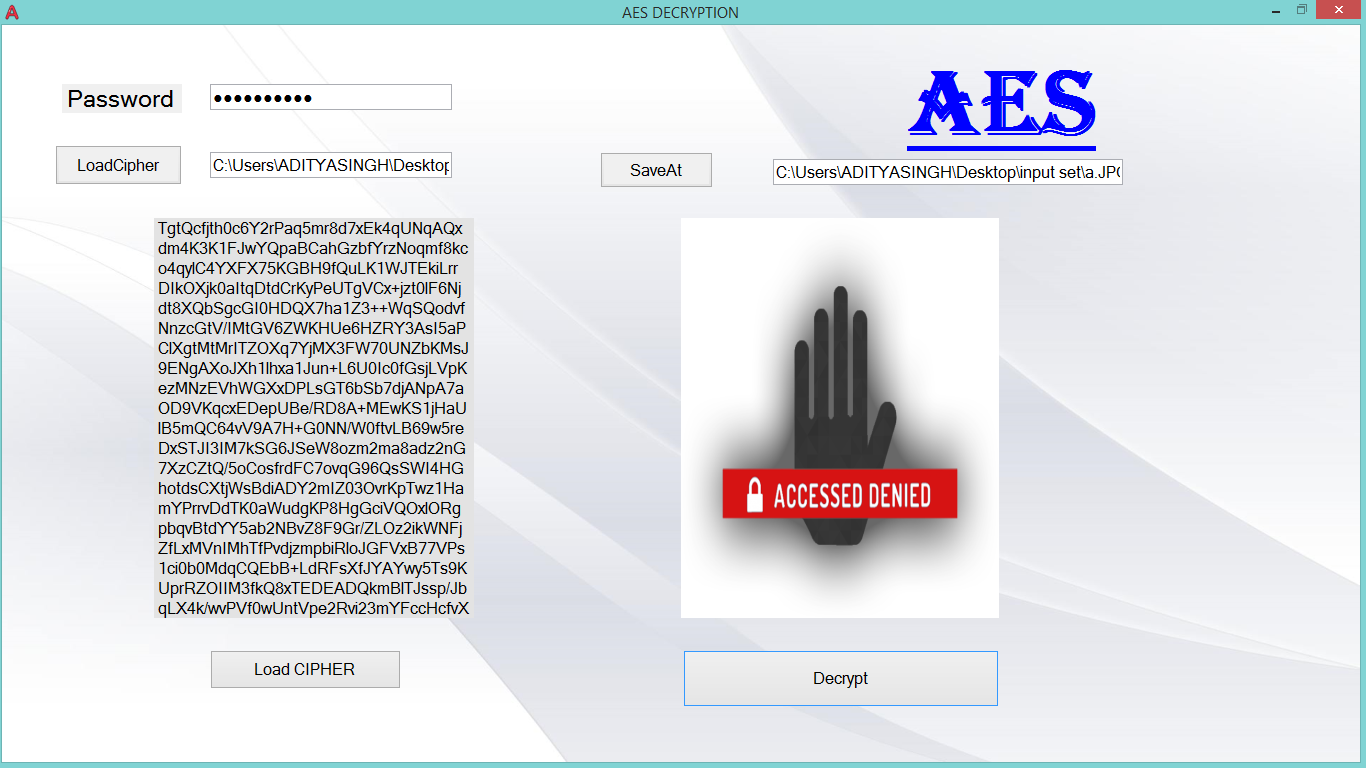


Fig – 6.1.5 Error in Decryption Process

**Chapter 7**

**7. RESULT and CONCLUSION** 

**7.1-RESULT**

For this, an experimental with the different raw images with the different sizes are encrypted and decrypted.

We implement cryptography mechanism by using the RSA algorithm and AES Algorithm with the public key encryption is to increase the security levels of the encrypted. Here one key is needed to encrypt and another key is needed to decrypts the image. Finally, the image cryptography experiment is provided the feasibility of security to the image in network security. The data is not view by no one without the knowledge of cryptography.

If we take image of dimension 250\*250 pixels, then number of times RSA algorithm executes is equals to 3\*250\*250,

1. Execution time of the process increases with the size of the image in both the algorithms but AES performs better in this case.

2. Size of the cipher file is greater than original image size but the increase in size is more in case of RSA Algorithm then AES.

.

Example: Time Elapsed Approximate Result

|  |  |  |
| --- | --- | --- |
| **Image Size** | **RSA Algorithm** | **AES Algorithm** |
| 50 KB | 17 sec | 2 sec |
| 100 KB | 1 min 40 sec | 3 sec |
| 250 KB | 3 min 50 sec | 5 sec |
| 500 KB | 10 min | 6 sec |
| 1.1 MB | 20 min | 10 sec |

Table 7.1 Time Taken

Example: Encrypted data size Approximate Result

|  |  |  |
| --- | --- | --- |
| **Image Size** | **RSA Algorithm** | **AES Algorithm** |
| 50 KB | 186 KB | 85 KB |
| 100 KB | 415KB | 190 KB |
| 250 KB | 600 KB | 344 KB |
| 500 KB | 900 KB | 720 KB |
| 1.1 MB | 2.7 MB | 1.8 MB |

Table 7.2 Encrypted Data size

**7.2-ISSUE IN RSA ALGORITHM DURING IMPLEMENTATION**

The efficiency of RSA Algorithm is about 77.88%. Now a day RSA Algorithm is used to prevent from unauthorized access on data. But during implementation, two main challenge introduce-

Quality of image does not preserve.

Size of image after encryption get change or approximately double of the actual size.

It takes lot of time to encrypt and decrypt the data.

**7.3-ISSUE IN AES ALGORITHM DURING IMPLEMENTATION**

AES Algorithm is lossy image encryption technique i.e. the image which we get after decryption is of smaller size which gives some less details. Although the information from the image is not loose but the quality gets degraded.

Images after Decryption using the RSA Algorithm and AES Algorithm

**Original RSA AES**

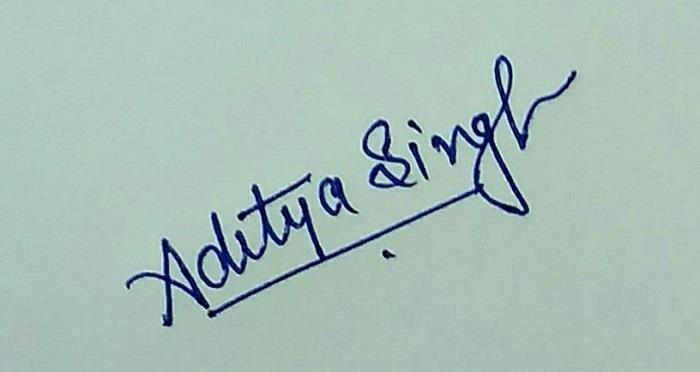
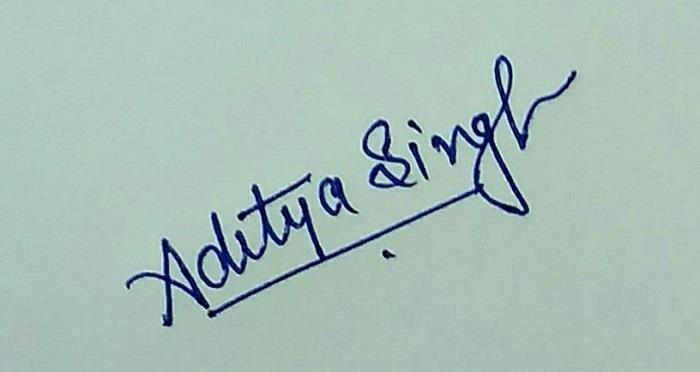


Fig – 7.2.1 Image Set Original and after decryption

**7.4 CONCLUSION**

AES Algorithm can be used in more effective manner instead of RSA Algorithm for Encryption of large data such as images, video etc.

AES perform better then RSA Algorithm for the image data.

**Which is better for what type of data:**

Size of Encrypted data- AES

Time taken to Encrypt and Decrypt – AES

AES is good for large Data (Image, video etc.)

RSA is good for small Data (text, numbers etc.)