GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

Comparative Study of Security algorithm for Data Transfer

A Report for the Evaluation 3 of Project 2

Submitted by

SHUBHAM MAURYA

(1613107059 / 16SCSE107005)

in partial fulfillment for the award of the degree of

Bachelor of Technology

IN

Computer Science and Engineering with Specialization of Business Analytics

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

Under the Supervision of

Mr.Ashutosh Upadhyay, M.Tech.
Assistant Professor

APRIL / MAY- 2020

SCHOOL OF COMPUTING AND SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Certified that this project report "**COMPARATIVE STUDY OF SECURITY ALGORITHM FOR DATA TRANSFER"** is the bonafide work of **"SHUBHAM MAURYA (1613107059)"** who carried out the project work under my .

SIGNATURE OF HEAD

Dr.PRASHANT JOHRI,

PhD (Management), PhD (CS)

Professor & Dean,

School of Computing Science & Engineering

SIGNATURE OF SUPERVISOR

Mr. ASHUTOSH UPADHYAY, M.Tech.

Assistant Professor

School of Computing Science $ Engineering

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	FrontPage	3
1	Abstract	4
2	Introduction	6
3	Existing System	8
4	Proposed system	9
5	Implementation or architecture diagrams	10
6	Output / Result / Screenshot	14
7	Conclusion/Future Enhancement	17
8	References	18

1. ABSTRACT

Encryption is the process of encoding information or data in order to prevent unauthorized access. These days we need to secure the information that is stored in our computer or is transmitted via internet against attacks. There are different types of cryptographic methods that can be used. Basically, the selecting cryptographic method depends on the application demands such as the response time, bandwidth, confidentiality and integrity. However, each of cryptographic algorithms has its own weak and strong points. In this paper, we will present the result of the implementation and analysis that applied on several cryptographic algorithms such as DES, AES, RSA and blowfish. Also, we will show the comparisons between the previous cryptographic techniques in terms of performances, weaknesses and strengths .Advanced Encryption Standard (AES) algorithm is one on the most common and widely symmetric block cipher algorithm used in worldwide. This algorithm has an own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world. It is extremely difficult to hackers to get the real data when encrypting by AES algorithm**.** AES has the ability to deal with three different key sizes such as AES 128, 192 and 256 bit and each of this ciphers has 128 bit block size. This paper will provide an overview of AES algorithm and explain several crucial features of this algorithm in details and demonstration some previous researches that have done on it with comparing to other algorithms such as DES,3DES, Blowfish etc.Security is playing a very important and crucial role in the field of network communication system and Internet. Data encryption standard (DES) is a private key cryptography system that provides the security in communication system but now a days the advancement in the computational power the DES seems to be weak against the brute force attacks. To improve the security of DES algorithm the transposition technique is added before the DES algorithm to perform its process. By using an Enhanced DES algorithm the security has been improved which is very crucial in the communication and field of Internet. If the transposition technique is used before the original DES algorithm then the intruder required first to break the original DES algorithm and then transposition technique. So the security is approximately double as compared to a simple DES algorithm.

Keywords: Network security, Data encryption, secure communication, Attacks, Cipher text**:**

2 . INTRODUCTION

Cryptography is an effective way for protecting sensitive information .It is a method for storing and transmitting data in form that only those it is intended for read and process. The evolution of encryption is moving towards a future of endless possibilities. Stenography is the art of passing information through original files. It is arrived from Greek word meaning “covered writing”. Stenography refers to information or file that has been concluded inside a picture, video or audio file.

Internet communication is playing the important role to transfer large amount of data in various fields. Some of data might be transmitted through insecure channel from sender to receiver. Different techniques and methods have been using by private and public sectors to protect sensitive data from intruders because of the security of electronic data is crucial issue. Cryptography is one of the most significant and popular techniques to secure the data from attackers by using two vital processes that is Encryption and Decryption. Encryption is the process of encoding data to prevent it from intruders to read the original data easily. . This stage has the ability to convert the original data (Plaintext) into unreadable format known as Cipher text.

Modern cryptography provide the confidentiality, integrity, nonrepudiation and authentication . These days, there are a number of algorithms have been available to encrypt and decrypt sensitive data which are typically divided into three types. Frist one is symmetric cryptography that is the same key is used for encryption and decryption data. Second one is Asymmetric cryptographic. This types of cryptography relies on two different keys for encryption and decryption. Finally, cryptographic hash function using no key instead key it is mixed the data .

The symmetric key is much more effective and faster than Asymmetric. Some of the common symmetric algorithms is Advance Encryption Standard (AES), Blowfish, Simplified Data Encryption Standard (S-DES) and 3DES. The main purpose of this paper will provide a detail information about Advanced Encryption Standard (AES) algorithm for encryption and decryption data then make a comparison between AES and DES algorithm to show some idea why replacing DES to AES algorithm.

The process of encoding the plaintext into cipher text is called Encryption and reverse the process of decoding ciphers text to plaintext is called Decryption. This can be done by two techniques symmetric-key cryptography and asymmetric key cryptography. Symmetric key cryptography involves the usage of the same key for encryption and decryption. But the Asymmetric key cryptography involves the usage of one key for encryption and another, different key for decryption. Secret key cryptography includes DES, AES, 3DES, IDEA, Blowfish algorithms etc. and public key cryptography includes RSA, Digital Signature and Message Digest algorithms.

For each algorithm there are two key aspects used: Algorithm type (define size of plain text should be encrypted per step) and algorithm mode (define cryptographic Algorithm mode). Algorithm mode is a combination of a series of the basic algorithm and some block cipher and some feedback from previous steps. We compare and analyzed algorithms DES and RSA.

A. Concepts used in Cryptograph

a.) Plain Text:

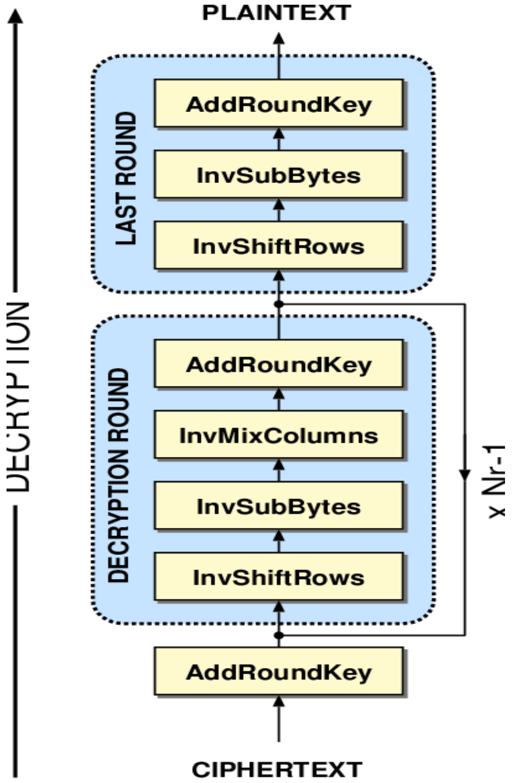
The original message that the person want to communicate is defined as plain text. For an example, Utkrishta is a person wishes to send "Hai, How are you" message to person Shivam, "Hi friend How are u "is referred as plain text.

b.)**Cipher Text**: The message which cannot be understood by anyone is defined as cipher text for an example"pe%hyrfzpv@ "is a cipher text produced for plain text "Hi, How are you ".

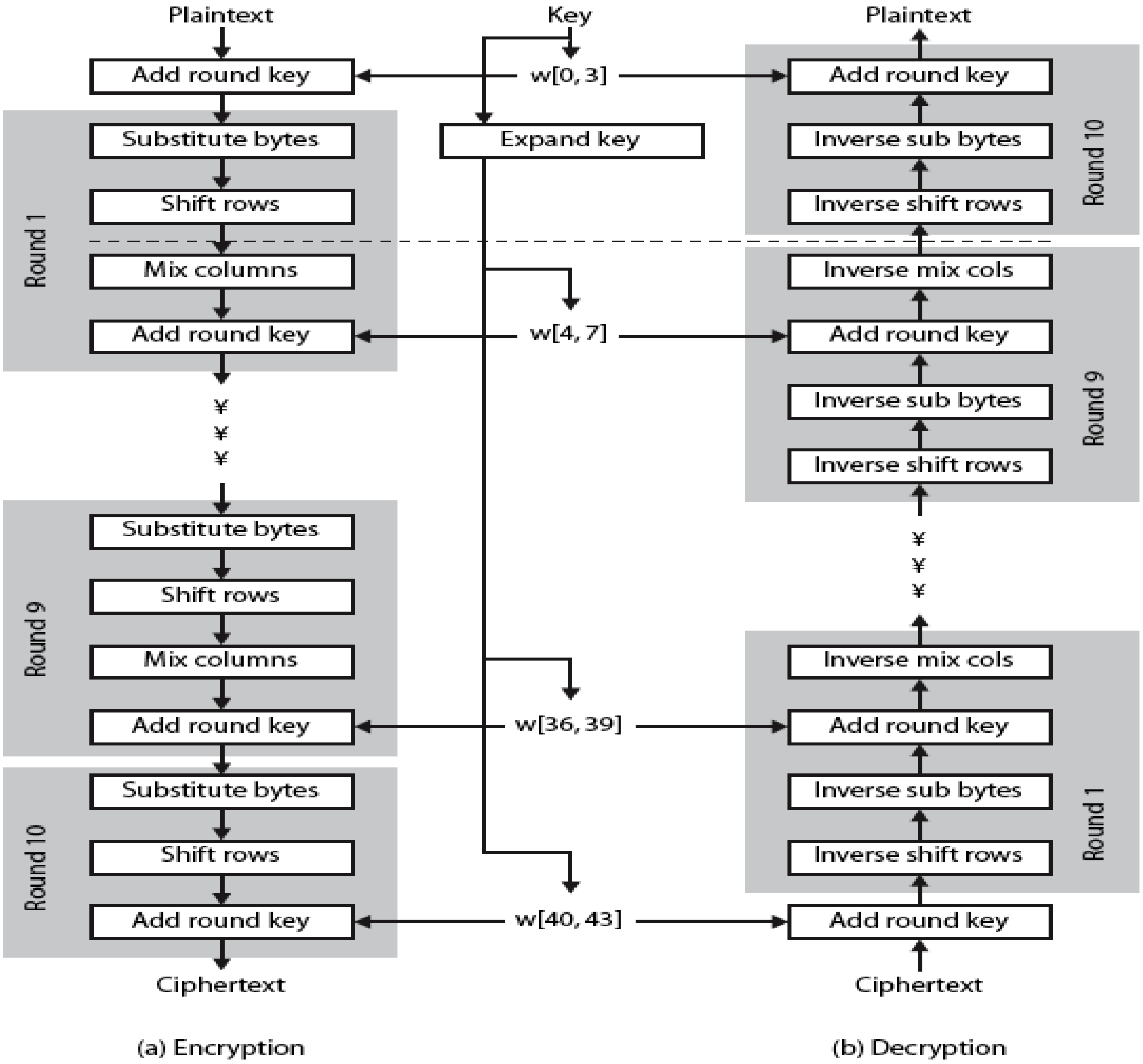
C.) Encryption: Converting plain text to cipher text is referred as encryption . It requires two processes . Encryption algorithm and a key.

d**.) Decryption** :Converting cipher text to plain text is referredas decryption . This may also need two requirements Decryption algorithm and key. The simple flow of commonly used encryption algorithms.

e.) **Key** : Combination of numeric or alpha numeric text or special symbol is referred as key .It may use at time of encryption or decryption key plays a important role in cryptography because encryption algorithm directly to acess.



The transposition technique does not replace the one alphabet with another like the substitution technique but perform the permutation on the plain text to convert it into cipher text. The various transposition techniques are used to perform the operation given below: A. Rail Fence Technique B. Simple Columnar Transposition Technique C. Vern am Cipher (One-Time Pad) D. Book Cipher/Running Key Cipher A. RAIL FENCE TECHNIQUE The Rail Fence Technique is simplest transposition technique. This technique involves writing plain text as a sequence of diagnosis and reading it row-by-row to produce the cipher text. An example is shown above diagram. In this figure the plain text is HELLO and the cipher text is HLOEL.



AES is an iterative instead of feistily cipher. It is based on two common techniques to encrypt and decrypt data knows as substitution and permutation network (SPN). SPN is a number of mathematical operations that are carried out in block cipher algorithms. AES has the ability to deal with 128 bits (16 bytes) as a fixed plaintext block size. The number of rounds is relied on the length of key. There are three different key sizes are used by AES algorithm to encrypt and decrypt data such as (128, 192 or 256 bits). The key sizes decide to the number of rounds such as AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

3.EXISTING SYSTEM

In this existing system we study about the various performance factor and technique or encrypting the data used by various papers are listed. In the research paper [1] proposed that the different performance factors are discussed such as key value ,computational speed and turnability They concluded that AES algorithm is better among Symmetric algorithm and RSA algorithm is found as better solution in asymmetric encryption technique. In the research paper [2] various experimental factors are analyzed Based on the text files used and the experimental result was concluded that DES2. Consume least encryption time and AES algorithm use least memory usage Encryption time differs in case of AES algorithm and DES algorithm .RSA consume more encryption time and memory usage is also very high but output byte is least in case of RSA algorithm. In the research paper [3] concluded that all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security. In the research paper [4] shown a new comparative study between encrypting techniques were presented in to nine factors, Which are key length, cipher type, block size,developed, cryptanalysis resistance, security, possibility key,possible ACSII printable character keys, time required to check all possible key at 50 billion second, these eligible’s proved the AES is better.In the research paper [5] discussed that DES is secret key based algorithm suffers from key distribution and key agreement problem .But RSA consumes large amount of time to perform encryption and decryption operation. It had been also observed that decryption of DES algorithm is better than other algorithms in throughput and less power.

There are various osi layer can be used:
There are 7 osi model can be used to describe the process of the encryption.
1) physical layer
2) Data link layer
3) Network layer
4) Transport layer
5) Session layer
6) Presentation layer
7) application layer
But in the given layer we are basically used to session layer because of in the session layer we are Doing both the encryption and decryption.
Also for security purpose we are used presentation layer.

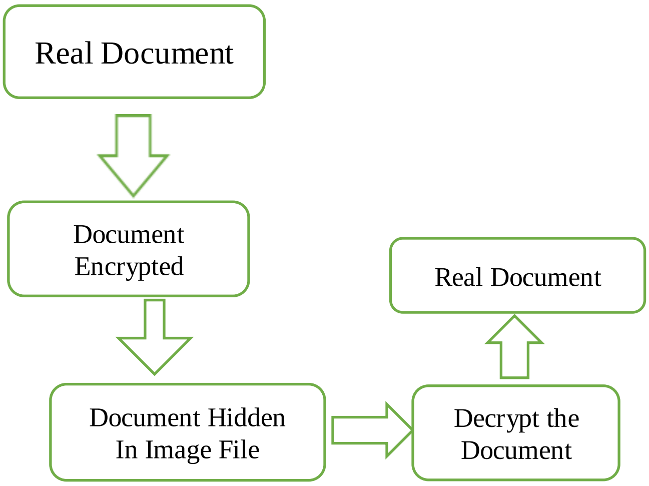


Figure 1 Working Structure

4.) PRAPOSED SYSTEM

Traditionally while transferring secured data over network lot of time is wasted in encrypting and decrypting audio data, video data and image at sender's and receiver's end The ciphered images have created the problem of patterns appearance in the AES algorithm because in these images Similar is present in the original image. Here we used the AES algorithm that was proposed in the figure 1. This paper has focused on reducing the time of encryption and decryption using parallel processing. Consider following scenario to understand the proposed work Using a 128 bit AES algorithm the number of steps required will be 5242880/128=40960. This means 40960 data blocks will be created on which AES will be applied individually. The modification is mainly focused on Shift Row transformations, if the value of 1'st element in state is even, the second and third rows are shifted right one and two times respectively, else the first and third rows are unchanged and each byte of the second and fourth rows of the state are cyclically shifted left over different number of bytes.

Hardware and software implementation of the AES algorithm is one of the most important area to attractive researches to do a research on it. Firstly to encrypt the data we compare and analyzed three different cryptographic algorithm Secondly encrypted secret message is then embeded in cover media by using LSB substitution technique in stegan

Total Time required for Uniprocessor
= (x/128)*AES calculating time.
Total Time required for Parallel approach
=(AES Calculating time/n)

Where,
x = File Size in bits
n = no. of processor

ographic algorithm.

5. IMPLEMENTATION OR ARCHITECTURE DIAGRAM

In this review we work , the secret data or document is encrypted before embedding in a cover file. We have compared DES, AES and RSA encryption technique to encrypt a data or document. Let us describe the algorithms one by one to explain proper formate.

1) DES: Data Encryption standard (DES) mainly adopted by industry for security products. Algorithm design for encryption and decryption process has been done with same key. This algorithm processes the following steps.

[1] DES accepts an input of 64-bit long plaintext and 56-bit key (8 bits of parity) and produce output of 64-bit block.
[2] The plaintext block has to shift the bits around.
[3] The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
[4] The plaintext and key will processed by following.
a. The key is split into two 28 halves.
b. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
c. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed keys used to encrypt this round’s plaintext.
d. The rotated key halves from step 2 are used in next round.
e. The data block is split into two 32-bit halves.
f. One half is subject to an expansion permutation to increase its size to 48 bits.
g. Output of step 6 is exclusive-OR’ with the 48-it compressed key from step 3.
h. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
i. Output of step 8 is subject to a P-box to permute the bits.
j. The output from the P-box is exclusive-OR’ with other half of the data block.
k. The two data halves are swapped and become the next round’s input.

2) AES : .Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10,12 and 14 round depending on key size as shown in Figure-3. .It can be implemented on various platform especially in small devices. It is carefully tested for many security applications. The following steps.
processed in AES algorithm.

Following steps used to encrypt a 128-bit block:

[1].Derive the set of round keys from the cipher key.
[2].Initialize the state array with the block data (plaintext).
[3].Add the initial round key to the starting state array.
[4] Perform nine rounds of state manipulation.
[5].Perform the tenth and final round of state manipulation.
[6].Copy the final state array out as the encrypted data (cipher text).

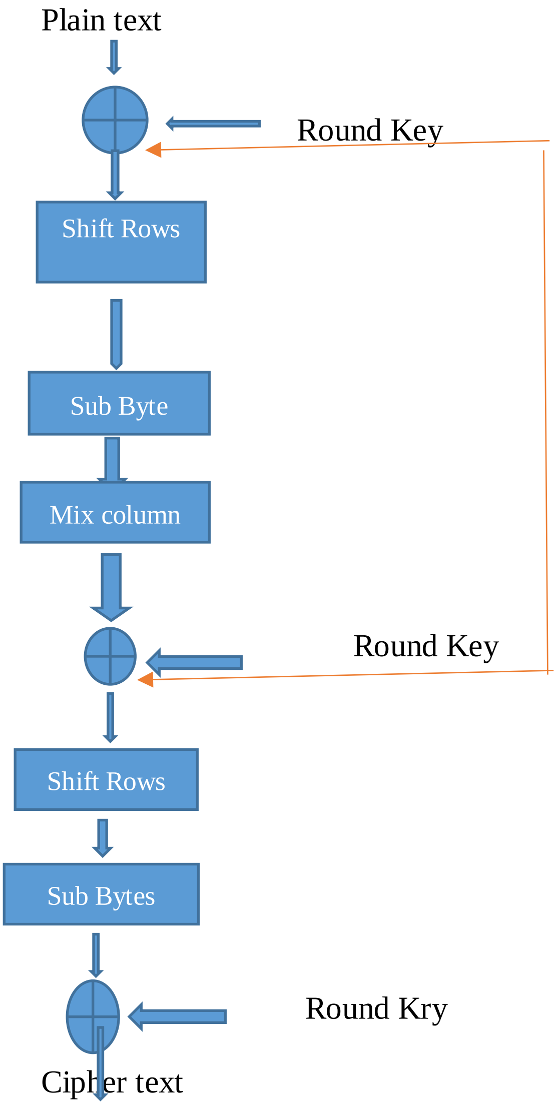
Each round of the encryption process requires a series of steps to alter the state of array. These steps involve four types of operations.

a. Sub Bytes: This operation is a simple substitution that converts every bite into a different value.

b. Shift Rows : Each row is rotated to the right by a certain number of bytes.

c. **Mix Columns** : Each column of the state array is processed separately to produce a new column. The new column replaces the old one.

d. **XorRoundKey** :This operation simply takes the existing state array.



Decryption: Decryption involves reversing all the steps taken in encryption using inverse functions like Inverse Sub Bytes ,Inverse Shift Rows , Inverse Mix Columns.

3) RSA:

Rivets Shamir Alderman is the most commonly used public key encryption algorithm. RSA computation occurs with integers modulo n = p*q. It requires keys of at least 1024 bits for good security. Keys of size 2048 bit provide best security. Widely used for secure communication channel and for authentication to identity service provider. RSA is too slow for encrypting large volumes of data . but it is widely used for key distribution Following steps are followed in RSA to generate the public and private keys

1. considers two large prime number s p and q such that p~=q.
2. Compute n=p*q
3. Compute $ (pp) = (p-1)*(q-1)
4. Consider the public key k1 such that gcd
($ (n), k1) =1; 1<k1<$ (n)
5. Select the private key k2 such that k2*k mod $ (n) =1
Encryption and Decryption are done as follow Encryption:Calculate cipher text C from plaintext P such that
C=P ^k1 mod n Decryption:
P=C^K2 mod n=P^k1k2 mod n

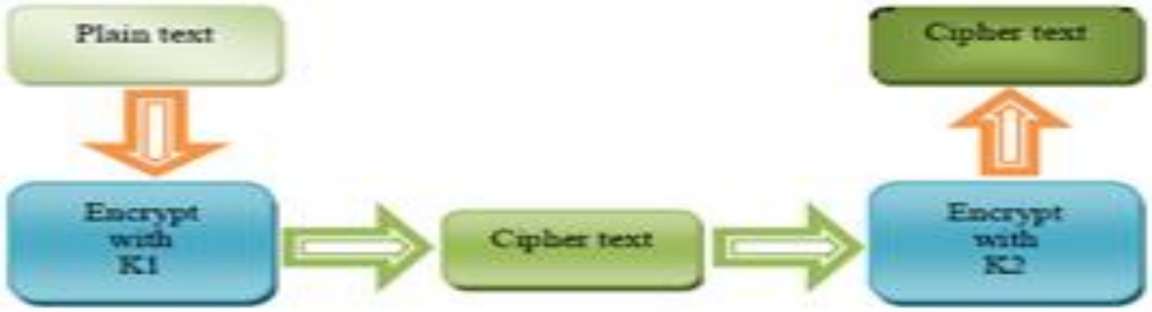


Fig. 2. Encraption process using two keys K1 and K2

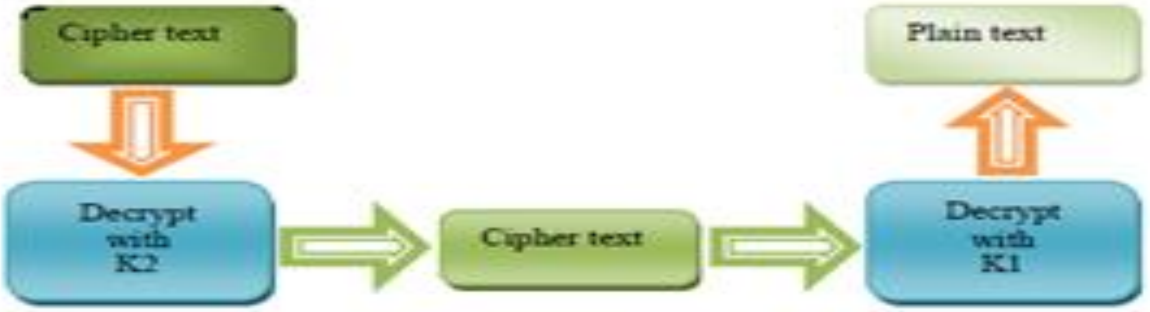
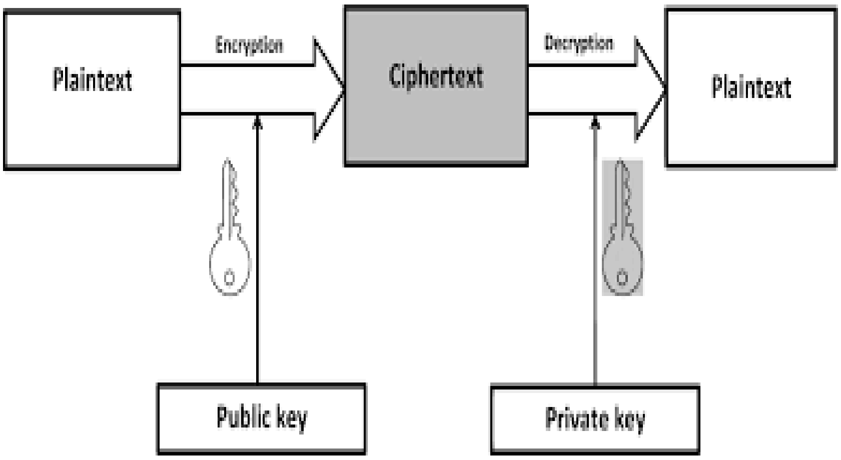


Fig. 3. Decraption process using two keys K1 and K2

LSB Technique:

Least Significant Bit (LSB) is a substitution method popularly used for embedding secret message. It involves the following steps.

1. Convert text into binary equivalent.
2. Get pixel value of each pixel one by one.
3. Replace each bit of cipher text with last bit of each pixe in image.As human eye is not very sensitive , after embedding data in a cover file, our eye cannot find difference between original image and data after inserting in the image.



6. OUTPUT/RESULT/SCREENSHOT

The experimental results are implemented using the Visual studio Net packages. The above said encryption algorithm. In the table below a comparative study between DES and AES is presented in to seven factors, Which are key length, cipher type, block size, developed, cryptanalysis, security, possibility key, possible ACSII printable character keys, time required to check all possible key are compared for different file size and shown in table-2. Performance of those algorithm is evaluated by considering the following parameters. Stimulation Time taken during the process is to be noticed. Encryption time is the time taken to produces a cipher text from plain text Decryption time is the time taken to produce a plain text from cipher text.
In the table we insert the data as the proper formate.

Method/ File(size(Mb))	150	192	306	852	1120
DES	1.0	1.1	1.2	1.3	1.4
AES	1	1.2	1.4	1.6	2.0
RSA	3.0	3.4	3.7	4.7	5.0

Buffer Size Variation in memory usage is referred as buffer size. By analyzing Fig 2, Time taken by RSA algorithm for both encryption and decryption process is much higher compare tothe time taken by AES and DES algorithm. Variation in buffer size is noticed. It does not increase according to size of file in all algorithm. and DES And RSA By analyzing Fig-3 which shows time taken forencryption and decryption on various size of file by three algorithms. RSA algorithm takes much longer time compare to time taken by AES and DES algorithm.

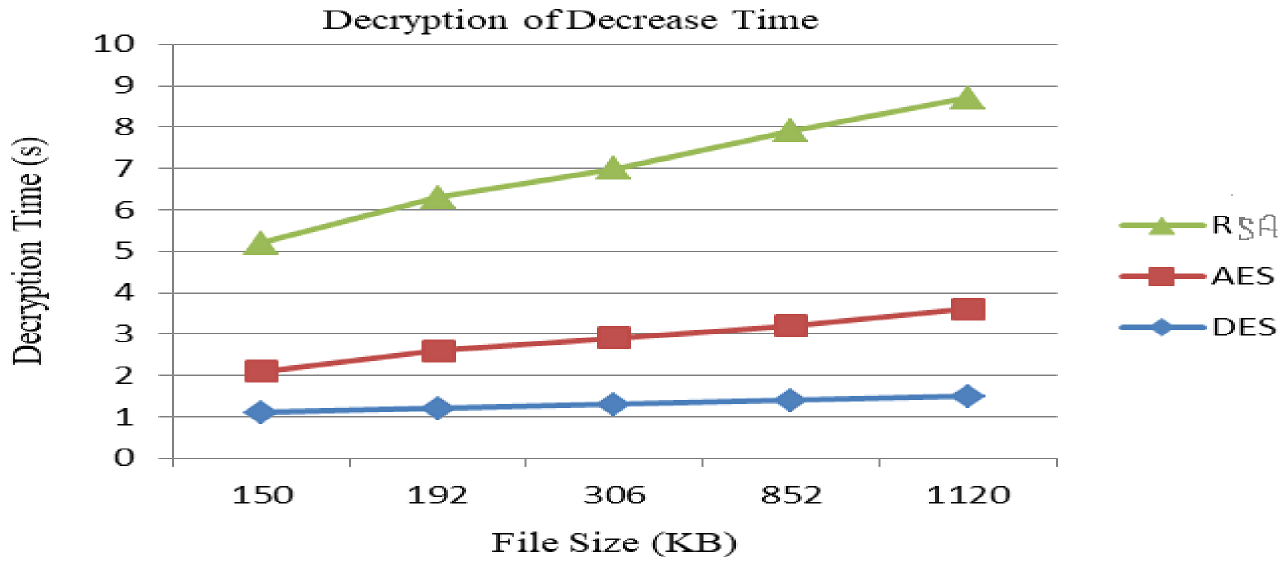


Fig2 Comparison Status of encryption AES,DES

In this result we are , the following factors are used such as the Key length value; Simulation speed, the key length management, the encryption ratio, power consumption, scalability, key used and the security of data against attacks are discussed in Fig 2.

1.**Developed:** It states about the time line of algorithm

2. **Key length Value** : It plays a important lrole that shows How data is encrypted.

3. **Type of Algorithm** : Two type of algorithm exist. Based on process and key it is segregated as symmetric and asymmetric

4. Encryption ratio : Measures amount of data that is to be encrypted. It should be minimized to reduce complexity. In our analysis we stated three levels like low , medium ,high.

5. Security issues: Encryption technique must satisfy cryptographic security like plaintext – cipher text attack.

6. Simulation speed : Encryption and Decryption algorithms are fast enough to meet real time requirements.

7**. Scalability :** Key size and block size variation is referred as scalability.

8. Key Used: To specify whether same key is used for encryption and decryption process or different key.

9. Power Consumption: Measure the power in units when the process takes place. It stated in two levels such as high and low.

10. Implementation: Hardware and Software are effective in AES compared to DES and RSA.

FACTOR	AES	DES	RSA
DEVELO-PED	2000	1977	1978
KEY SIZE	128,192,256bits	56 bits	>1024bits
BLOCK SIZE	128 bits	64bits	Min 512 bits
CIPHERING $$ DECIPHERINF KEY	Same	Same	Same
ENCRYPTION	Faster	Moderate	Slow
DECRYPTION	Faster	Moderate	Slow
SECUIRITY	Excellent secured	Less Secured	Very Less Secured

Comparison of AES,DES And

Fig 3 Decryption RSA

7. CONCLUSION / FUTURE IMPROVMENT

In Data communication, encryption algorithm plays an important role. Our research work surveyed the existing encryption techniques like AES, DES and RSA algorithms along with LSB substitution technique. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security. Based on the experimental result it was concluded that AES algorithm consumes least encryption and decryption time and buffer usage compared to DES algorithm. but RSA consume more encryption time and buffer usage is also very high .we also observed that decryption of AES algorithm is better than other algorithms. From the simulation result, we evaluated that AES algorithm is much better than DES and RSA algorithm.

We have compared and analyzed existing cryptographic algorithm like DES, AES and RSA along with the same LSB technique for hiding the document in an image file. Our future work will focus on SLSB which replace LSB.

8. REFERENCES

[1] M. E. Hellman,"DES will be totally insecure within ten years" lEEE Spectrum, Vo1.16, N0.7, pp32-39, July 1979.

[2] Alani, M.M.," A DES96 - improved DES security ", 7th International Multi-Conference on Systems, Signals and Devices, Amman , 27-30 June 2010.

[3] Seung-Jo Han , Heang-Soo Oh , Jongan Park," IEEE 4th International Symposium on Spread Spectrum Techniques and Application Proceedings ", 22-25 Sep 1996.

[4] Manikandan. G, Rajendiran.P, Chakarapani.K, Krishnan.G, Sundarganesh.G,"A Modified Crypto Scheme for Enhancing Data Security", Journal of Theoretical and Advanced Information Technology, Jan 2012.

[5] Shah Kruti R., Bhavika Gambhava,"New Approach of Data Encryption Standard Algorithm", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[6] Govind Prasad Arya, Aayushi Nautiyal, Ashish Pant, Shiv Singh, Tishi Handa,"A Cipher Design with Automatic Key Generation using the Combination of Substitution and Transposition Techniques and Basic Arithmetic and Logic Operations",The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), Vol. 1, No. 1, March-April 2013.

[7] Diaasalama, Abdul Kadar, MohiyHadhoud, “Studying the Effect of Most Common Encryption Algorithms”, International Arab Journal of e-technology, vol 2, no.1, January 2011.

[8] Diana Salaam Abdi Elminaam1, Hatem Mohamed Abdul Kader2, and Mohan Mohamed Hadhoud2,” Evaluating the

Performance of Symmetric Encryption Algorithm “,International Journal of Network Security, Vol.10, No.3,PP.213 {219, May 2010.

[9] Humane Agawam & Manish Sharma” Implementation and analysis of various Cryptography” Dec-2010

[10] Gurjeevan Singh, Aswan Kumar Single, K. S. Sandhu, “Through Put Analysis of Various Encryption Algorithms”, IJCST Vol.2, Issue3, September 2011

[11] RSA Cryptography Specifications http://www.ietf.org.

[12] Performance Evaluation Of Symmetric Algorithms Published In Volume 3, No. 8, August 2012 Journal Of Global Research In Computer Science

[13] Performance Evaluation of Symmetric Encryption Algorithms D. S. Abdul. Elmina am, M. Abdul Kader, M. M. Handhold published in Communications of the IBIMA Volume 8, 2009 ISSN: 1943-7765

[14] www.di-mgt.com.au/rsa_ alg.html developed by David Ireland

[15] Alexander Berzati ,Jean-Guillaume Dumas , Louis Goubin discussed “Fault attacks in RSA public key “Published in: · Proceeding CT-RSA '09 Proceedings of the Cryptographers' Track at the RSA Conference 2009 on Topics in Cryptology ages 414 - 428

[16] “Secure Data Hiding Algorithm Using Encrypted Secret message “ by Harshitha K M, Dr. P. A. Vijay published in International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012 1 ISSN 2250.