International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 06 | June -2020 ISSN: 2582-3930

Comparative Study of Security algorithm for Data Transfer

Shubham Maurya, Mr.Ashutosh Upadhyay

AS Boy's Hostel Greater Noida Uttar Pradesh (221310)

Abstract — It is basically a process in which we are basically encoding the information into such that no one access the data at any way. There are different method we used to encoding and decoding the information so that the way to get the data is very effective and efficient way. There are various technique we used to encode and decode the data, AES, DES and RSA. These technique today is very import at to protect the data so that attacker is not able access my data. These day security is very important to store the data in our computer and transmit our data over by the internet. There are different types of cryptographic methods that can be used. These cryptography is depends upon application such as response time, Bandwidth confidentiality and integrity. All these cryptography algorithm have week as well as strong point to so that we secure the data to transmit the data over the channel. We will show the comparisons between the previous cryptographic techniques in terms of performances, weaknesses and strengths.

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

1 .INTRODUCTION

It is basically process in which we are secure the information or protect the data so that when we transmitted data over by the internet so my data is secure as well as is not recognized by the any attacker The evolution of encryption is moving towards a future of endless possibilities. It is taken the word from Greek to "covered writing". Cryptography refers to information or file that has been concluded inside a picture, video or audio file.

A. Concepts used in Cryptograph

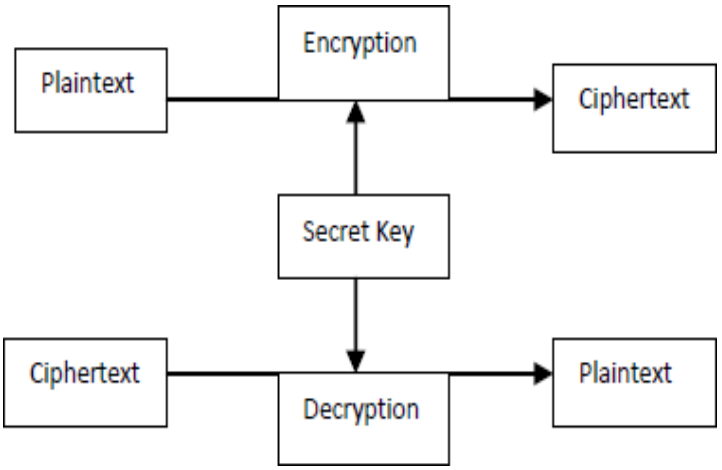
a) Plain Text: The Real Massage that the person want to communicate is defind as plain text.lets an example Utkrishta is a person who send "Hai,How are you" Message to person shivam,"Hi friend how are you" is referred as plain text.

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,My Dear Friend".

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.



PROBLEM STATEMENT

Now days, internet has become one of the important part in our lives and it is considered as one of the communication way. There are lots of communications by sending or receiving the data or files between the sender and receiver.

some of the people are want to secure our data about the accuracy of this encryption process where some errors may occur when encrypting the data and doing translation to the receiver, in order to prevent the wrong interpretation of the receiver.
Some question are asked in research paper.
i.) How to know about the AES,so that it will be more understand by the readers?
ii.) How to improve the AES encryption with correct process of encryption and decryption the data and file?

2.) LITRATURE SURVEY:

In this Survey we study about the various performance factor and technique of encrypting the data by various papers that we read the reference of other author. In the research paper [1] proposed that the different performance factors are discussed such as key value ,computational speed and turn ability They tells that the 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 is basically 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 very important to secure the data by the internet in which we are suitable for different applications. Everyday new encryption technique is evolving hence fast and secure our data over by the internet as well as the accessing the data from different medium so, encryption techniques will always work out with high rate of security. In the research paper [4] shown a new comparative technique it tells that the between encrypting techniques were presented in to nine factors, Which are key length, cipher type, block size, developed, cryptanalysis resistance, security, possibility key, possible alphabet or number character keys, time required to check all possible key at very large second, these are proved the AES is better. In the research paper [5] discussed that DES is secret key based algorithm so that key distribution and key agreement play a important role .But RSA consumes large amount of time to perform encryption and decryption operation. But it is basically more secure as compare to all other algorithm. 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.

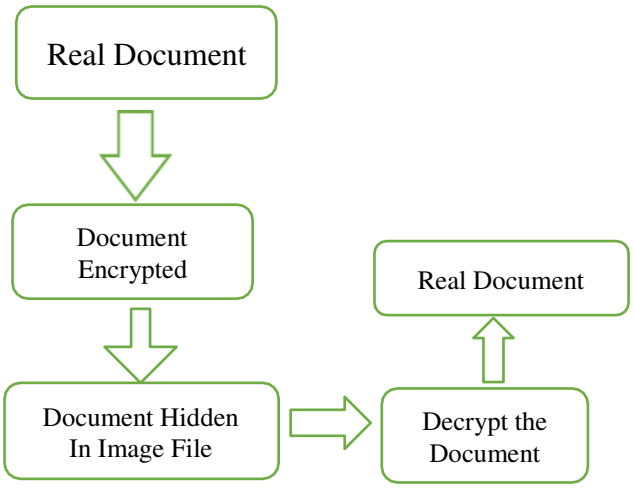


Figure 1 Working Structure

3.) PRAPOSED MODEL:

In this model we are basically know about how the model is calculate the total time require to find the processing time. There are two way to calculate the processing time, the first was Uniapproch and second was parallel Approach. In this model security data over network take a lot of time is wasted in encrypting and decrypting audio data, video data and image at sender's and receiver's end . The ciphered diagram have create he problem of patterns appearance in the AES algorithm because in these diagram are Similar is present in the original Diagram. 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 Shifting 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 is implemented by the AES algorithm is one of the most important area to attractive researches to do a research on it. First encryption over the data we compare and analyzed three different cryptographic algorithm Second encryption secure message is then embeded in cover media by using LSB substitution technique in steganographic algorithm.

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

3.1) Cryptographic Algorithm

In this research paper we work to secure our data or document is encrypted before embedding in a cover file. We have to comapre all these algorithm such as DES, AES and RSA encryption technique to encrypt a data or document. Let us we tell about the algorithms one by one to explain proper formate.

1) DES: Data Encryption standard (DES) is mainly adopted by channel for security purpose. 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 as well as 56-bit key (8 bits of parity) and produce output of 64-bit block.
[2] The plaintext block has to shift around the bit.
[3] The 8 bit of parity are removed from the key by subsisting the key to its Key Permutation.
[4] The plaintext and key will processed by following.

1. The data key is split into two 28 parts.
2. Each part of the key is shifting around the one by one or two bits, depending on the round.
3. The parts 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.
4. The rotated key parts from step 2 are used in next round.
5. The data block is divided into two 32-bit halves.
6. One parts is subject to an expression to increase its size to 48 bits.
7. The Output of step 6 is exclusive-OR' with the 48-it compressed key from step 3.
8. The Output of step 7 is into an S- box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
9. The Output of step 8 is subject to a P-box to permute the bits.
10. The output from the P-box is exclusive-OR' with other half of the data block.
11. The two data parts are swapped and become the next round's input.

2) AES: .Advanced Encryption Standard (AES) algorithm is used for security and well as to improve the speed of the system. Both hardware and software implementation are faster still. New encryption standard recommended by different organization to replace DES. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size .It can be implemented on various platform especially in small devices. It is basically used to testing for many security applications. The following steps processed in AES algorithm.

Following steps used to encrypt a 128-bit block:
[1] Determine the set of round keys from the cipher key.
[2] Initialize the state array with the block data (original data).
[3] To perform the Add operation initial round key to the beginning state Array.
[4] Perform nine rounds of state manipulation.
[5] Perform the tenth and final round of state manipulation.
[6] Copy the final state of array out as the encrypted data (Encrypted data).

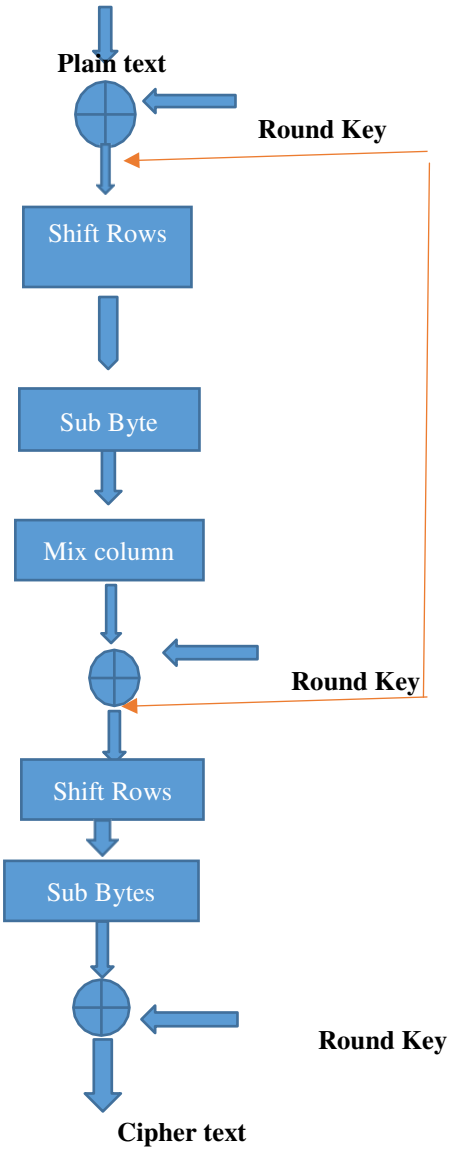
Each round of the encryption process requires to perform the various steps to alter the state of array. These steps involve four types of operations.

a. Sub Bytes: It is very simple substitution that converts every bits into a different other value.

b. Shift Rows: Each row is moved 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. And any mistake is happened in between then they are perform again and again so that we get the accurate values.

d. Xor-Round-Key: This operation is simply takes the existing state array.

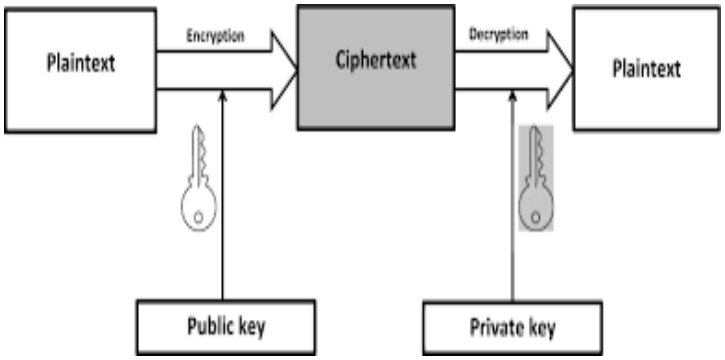


Decryption: Decryption is basically involves reversing all the steps taken in encryption using inverse functions like Inverse Sub Bytes, Inverse Shift Rows , Inverse Mix Columns.

3) RSA: Rivets Shamir Alderman is the most commonly used public key encryption algorithm. RSA computation occurs with integers modulo n = r*s. 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. Assume two large prime number such that r and s such that r=s.
2. Then Compute the value of n=r*s
3. Compute $ (n) = (r-1)*(s-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

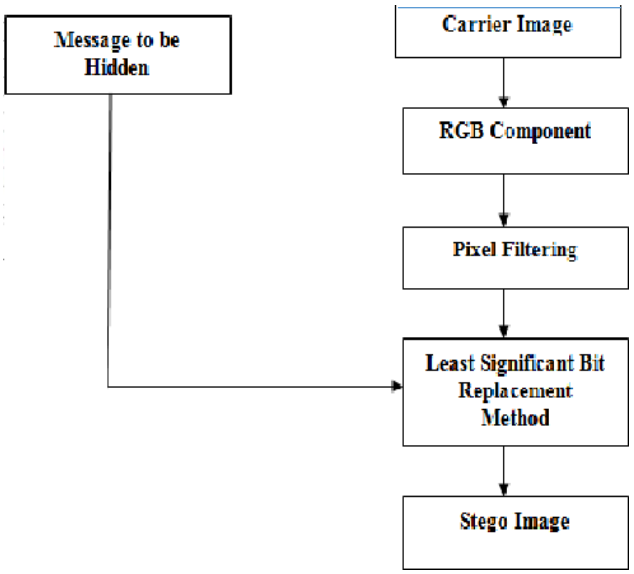
Encryption and Decryption are done as follow Encryption: Calculate cipher text (C) from plaintext (P) such that
C=P ^k1 mod n Decryption:
P=C^K2 mod n=P^k1k2 mod n



LSB Technique:

Least Significant Bit (LSB) is very important to compute the number of bits that are shifted around the given data so that, substitution method popularly used for fitting secret message. LSB is basically is also used in the digital design so that.it improve the performance of given environment. 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 pixel in a Diagram. 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.



FACTORS ANALYZED

In this paper we are analysed , 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..

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

2. Key length Value : It plays a important role that shows the how data is encrypted.

3. Type of Algorithm: Two type of algorithm exist. Based on process and key it is separated by symmetric and asymmetric

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

5. Security issues: Encryption technique is satisfy cryptographic securitylike plaintext – cipher text attack.

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

7. Scalability: The Key size of 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.

4. EXPERIMENTAL RESULT

The experimental results are implemented using the various studio package like the Net. The encryption algorithm we do various technique to perform the task so that to generate the output we used to make the model is very efficient way.
The data shown in the below table according to the given graph.

Method/ File size (MB)	150	192	306	852	1120
DES	2.3	2.9	3.0	3.7	5.2
AES	1.4	1.5	1.6	2.0	2.1
RSA	2.8	3.8	4.9	5.6	8.2

Table 1. Comparison of Encryption Time(sec)

In the given we improved the performance of Encryption time so that when any user can be transferring the data by the any server so that we convert the plain text to cipher text at very fast so that user can be used at very effective way.

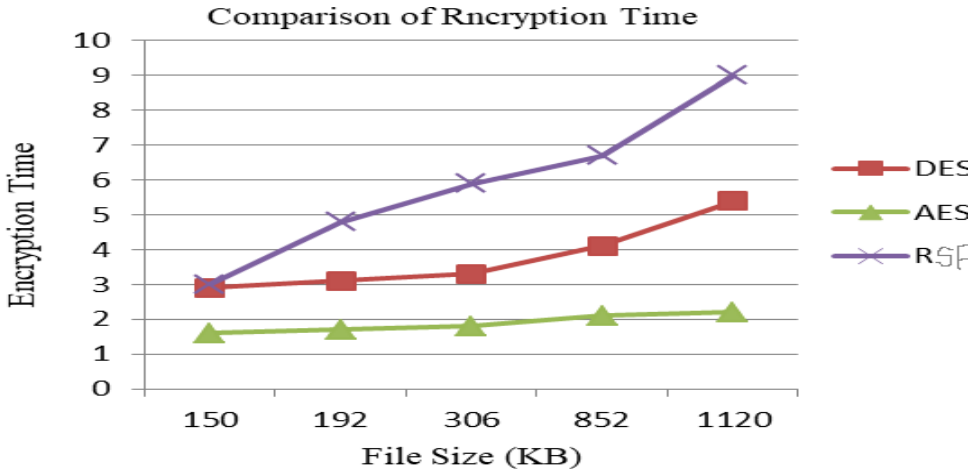


Fig2 Comparison Status of encryption AES,DES,RSA

Comparision of all three cryptography Algorithm:

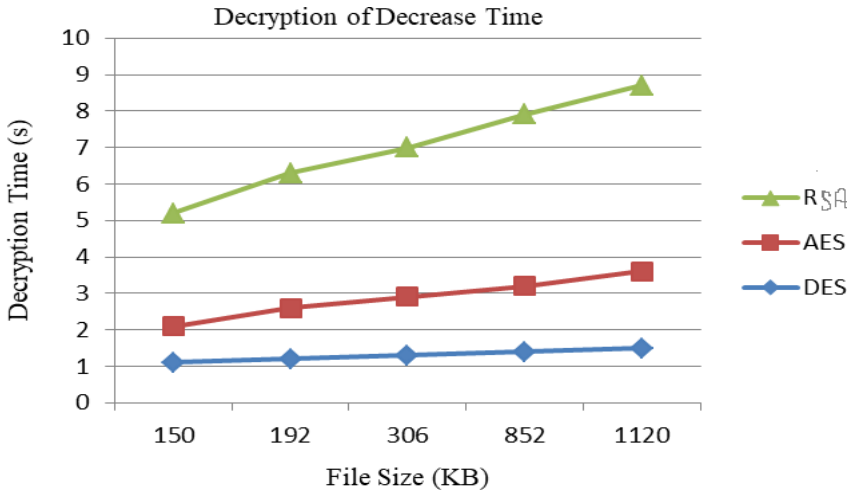
In the table below a comparative study between DES and AES is presented in to seven factors, Which are key length, cipher type, block size, developed, cryptanalysis, security, possibility key, possible Organization printable character keys, time required to check all possible key are compared for different 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. 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

In Table we insert all the data as the following mention graph below.

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

Table 2. comparison of Decryption time(ms)

Similar to encryption in this method we are basically convert the cioher text into plain text so that reciver can be accessed the any file at very fast way. 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.



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

5.ACKNOWLEDGMENT

Thanks to all the authors that is listed below in list of Reference. And sincere thanks to my guide under whose guidance this project can be fulfilled.

6. CONCLUSION

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.

7. FUTURE IMPROVMENT

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] Sung-Jo Han, Hang-Soo Oh, Jong and Park," IEEE 4th International Symposium on Spread Spectrum Techniques and Application Proceedings ", 22-25 Sep 1996.
[4] Manikandan. G, Rajendiran.P, Chakarapani.K, Krishnan, Sundarganesh.G,"A Modified Crypto Scheme for Enhancing Data Security", Journal of Theoretical and Advanced Information Technology, Jan 2012.
[5] Shah Kruti R., Bhavika Gam bhava, "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] Govan Prasad Arya, Aarush Nautical, Ashish Pant, Shiv Singh, Trish 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
[17] Ramesh G, Umarani. R," Data Security In Local A Area Network Based On Fast Encryption Algorithm", International Journal of Computing Communication.
.