Performance Analysis of DES, AES and RSA Algorithm along with LSB SubstitutionTechnique

Mrs. G Uma Maheshwari[1], Mrs. Joshi Padma[2]

[1]*M tech, Sreyas institute of Engineering and technology, Nagole, Hyderabad , India.*

[2]*Associate Professor, Sreyas institute of Engineering and technology, Nagole, Hyderabad , India.*

Abstract: ***Now a days sharing the information over internet is becoming a critical issue due to security problems. Hence more techniques are needed to protect the shared data in an unsecured channel. The present work focus on combination of cryptography and steganography to secure the data while transmitting in the network. Firstly the data which is to be transmitted from sender to receiver in the network must be encrypted using the encrypted algorithm in cryptography .Secondly the encrypted data must be hidden in an image or video or an audio file with help of steganographic algorithm. Thirdly by using decryption technique the receiver can view the original data from the hidden image or video or audio file. Transmitting data or document can be done through these ways will be secured. In this paper we implemented three encrypt techniques like DES, AES and RSA algorithm along with steganographic algorithm like LSB substitution technique and compared their performance of encrypt techniques based on the analysis of its stimulated time at the time of encryption and decryption process and also its buffer size experimentally. The entire process has done in C#.***

Keywords: Cryptography, Steganography, DES, RSA, AES, LSB.

1. 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 concealed inside a picture, video or audio file.

A. Concepts used in Cryptography

a. Plain Text: The original message that the person want to communicate is defined as plain text. For an example,Alice is a person wishes to send “Hai, How are you” message to person Bob, “Hi friend how are u “is referredas plain text.
b. Cipher Text: The message which cannot be understood by anyone is defined as cipher text for an example “ ib%ipvbufzpv@ “ is a cipher text produced for plain text “Hi , How are you “.
c. Encryption : Converting plain text to cipher text is referredas encryption . It requires two processes . Encryption algorithm and a key.
d. Decryption :Converting cipher text to plain text is referred as decryption . This may also need two requirements Decryption algorithm and key. Figure 1 shows 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 vital role in cryptography because encryption algorithm directly depends on it.

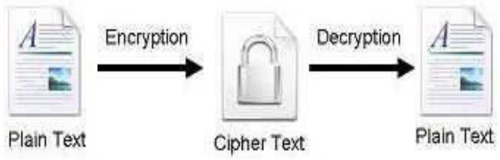


Figure-1: Encryption-Decryption Flow

2. Literature Review

In this section the various performance factor and technique for 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 tunability 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 DES algorithm consumes least encryption time and AES algorithmuse 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 evolvinghence 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 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 problems .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 consumption.

3. Proposed Work

Now a day's securing data is a very big challenge to computers users such as Business , Professionals and Home users from the intruders . In this proposed system we implemented and compared three different encryption algorithm for data encryption and then the encrypted file is hidden within a image by using LSB substitution technique .as shown in Figure-2 Both cryptography and steganography are used to enhance the security of data.

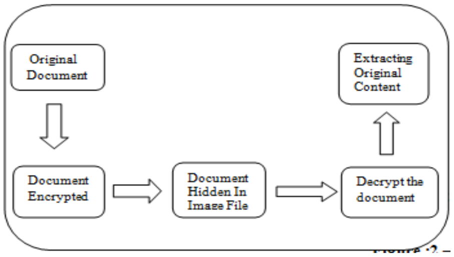


Figure 2. Proposed work

In the proposed system two technique used as shown in Fig-2. Firstly to encrypt the data we compare and analyzed three different cryptographic algorithms . Secondly encrypted secret message is then embed in cover media by using **LSB** substitution technique in steganographic algorithm

B. Cryptographic Algorithm

In this research 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.

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 block.
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 increaseits size to 48 bits.
g. Output of step 6 is exclusive-OR'ed with the 48-it compressed key from step 3.
h. Output of step 7 is fed into an S-box, which substitutes keybits 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'ed with otherhalf 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 platforms 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 . They are

a. Sub Bytes : This operation is a simple substitution that converts every bite into a different value.
b. ShiftRows : Each row is rotated to the right by a certain number of bytes.
c. MixColumns : 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 InvSubBytes , InvShiftRows , InvMixColumns

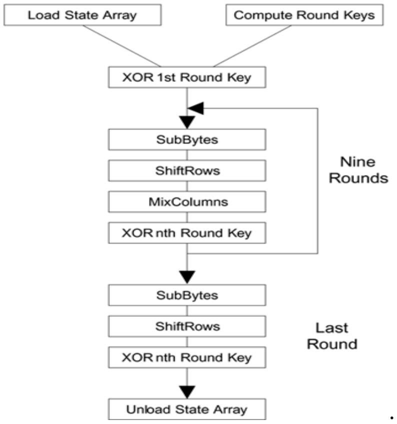


Figure 3. Flow of AES Algorithm

3) RSA : Rivest Shamir Aldeman 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 bitprovide best security. Widely used for secure communicationchannel and for authentication to identity service provider.RSA is too slow for encrypting large volumes of data . but itis widely used for key distribution Following steps arefollowed in RSA to generate the public and private keys 1.Conisder two large prime numbers p and q such that p~=q. 2.Compute n=p*q

3. Compute φ (pq) = (p-1)*(q-1)
4. Consider the public key k1 such that gcd (φ (n), k1) =1; 1<k1< φ (n)
5. Select the private key k2 such that k2*k mod φ (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

C. LSB Technique

Least Significant Bit (LSB) is a substitution method popularly used for embedding secret message. It involves thefollowing 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 image.

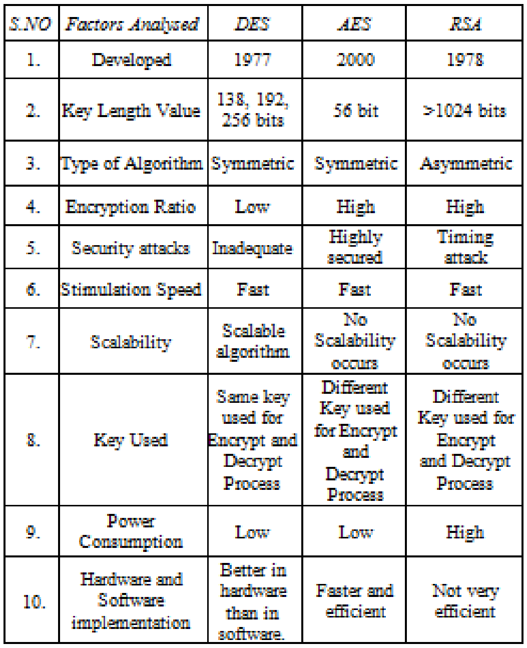
As human eye is not very sensitive , after embedding data in a cover file, our eye cannot find difference between original image and data after inserting in the image.

3.1 FACTORS ANALYZED

In this paper, 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 table - 1.

1. Developed: It states about the timeline of algorithm
2. Key length Value : It plays a vital role 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. Inour 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.

Table 1: Analysis of various factors



S.NO	Factors Analysed	DES	AES	RSA
1.	Developed	1977	2000	1978
2.	Key Length Value	138, 192, 256 bits	56 bit	>1024 bits
3.	Type of Algorithm	Symmetric	Symmetric	Asymmetric
4.	Encryption Ratio	Low	High	High
5.	Security attacks	Inadequate	Highly secured	Timing attack
6.	Stimulation Speed	Fast	Fast	Fast
7.	Scalability	Scalable algorithm	No Scalability occurs	No Scalability occurs
8.	Key Used	Same key used for Encrypt and Decrypt Process	Different Key used for Encrypt and Decrypt Process	Different Key used for Encrypt and Decrypt Process
9.	Power Consumption	Low	Low	High
10.	Hardware and Software implementation	Better in hardware than in software.	Faster and efficient	Not very efficient

4. Experimental Result And Discussion

The experimental results are implemented using the Visual studio Net packages. The above said encryption algorithm are compared for different file size and shown in table-2.Performance of those algorithm is evaluated by considering the following parameters.

A. Stimulation Time

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.

B. Buffer Size

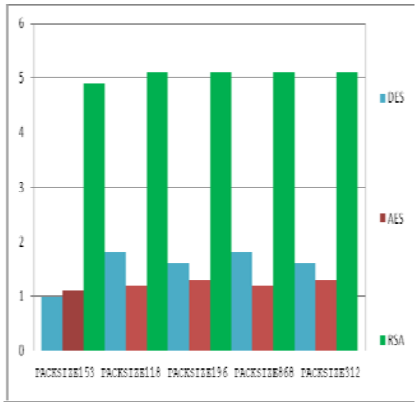
Variation in memory usage is referred as buffer size.

Table 2. Comparison of various packet sizes for DES,AES & RSA algorithm

algorithm show very minor difference in time taken forencryption and decryption process.

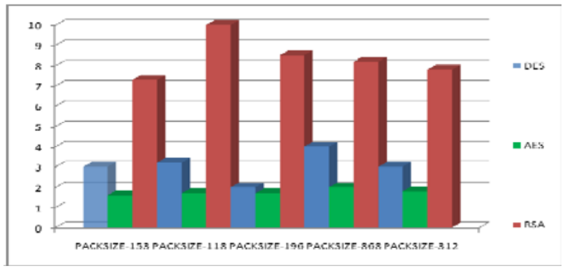
S.NO	*Algor*	*Pack Size (KB)*	*Encrypt Time (Sec)*	*Decrypt Time (Sec)*	*Buff Size*
1	DES	153	3.0	1	157
	AES		1.6	1.1	152
	RSA		7.3	4.9	222
2	DES	118	3.2	1.2	121
	AES		1.7	1.2	110
	RSA		10.0	5.0	188
3	DES	196	2.0	1.4	201
	AES		1.7	1.24	200
	RSA		8.5	5.9	257
4	DES	868	4.0	1.8	888
	AES		2.0	1.2	889
	RSA		8.2	5.1	934
5	**DES**	312	3.0	1.6	319
	AES		1.8	1.3	300
	RSA		7.8	5.1	416

Figure.2 Comparative analysis of Buffer Size among AES and RSA algorithm



By analyzing table-2, Time taken by RSA algorithm for both encryption and decryption process is much higher compare to the time taken by AES and DES algorithm. Variation inbuffer size is noticed. It does not increase according to sizeof file in all algorithms.

Figure 3. Comparative status of Encryption Time among DES, AES and RSA



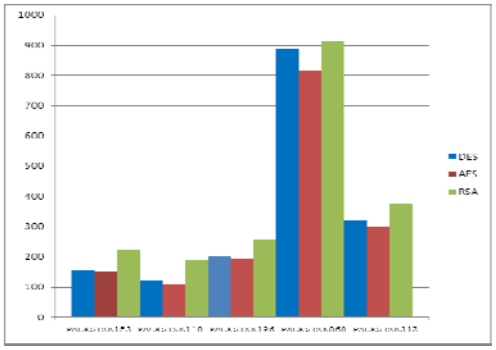


Figure 4. Comparative status of Decryption Time among DES, AES and RSA

By analyzing Fig-3 , Fig-4 which shows time taken for encryption 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. AES and DES

By analyzing Figure 5 , it shows buffer size usages by AES, DES and RSA algorithm and noticed that RSA algorithm buffer size usages are highest for all sizes of document file.

5. Acknowledgements

Thanks to all the authors that is listed below in list of reference.

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 Enhancement

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

References

[1] AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram “Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037

[2] Shashi Mehrotra Seth, Rajan Mishra “Comparative Analysis Of Encryption Algorithms For Data Communication” IJCST Vol. 2, Issue 2, June 2011 ISN :29-43(Print)|ISSN:0976-8491(Online)www.ijcst.com

[3] E.Thamiraja ,G.Ramesh,R.Uma rani “A Survey on Various Most Common Encryption Techniques” International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X

[4] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani “New Comparative Study Between DES, 3DES and AES within Nine Factors” Journal Of Computing, Volume 2, Issue 3, March2010,Issn2151-9617

[5] Aman Kumar , Dr. Sudesh Jakhar , Mr. Sunil Makkar “comparative analysis between DES and RSA algorithm” International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X

[6] Diaasalama, Abdul kader, MohiyHadhoud, “Studying theEffect of Most Common Encryption Algorithms”, International Arab Journal of e-technology, vol 2, no.1, January 2011.

[7] Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader2, and Mohiy Mohamed Hadhoud2,” Evaluating the Performance of Symmetric Encryption Algorithm “, International Journal of Network Security, Vol.10, No.3, PP.213 {219, May 2010.

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

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

[10] Paar, Cristof et al. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Springer.p. 30ISBN 9783642041006 http://books.google.com/books?id=f24wFELSzkoC&pg =PA30

[11] RSA Cryptography Specifications http://www.rsa.com 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. Elminaam, M. Abdul Kader, M. M. Hadhoud published in Communications of the IBIMA Volume 8, 2009 ISSN: 1943-7765

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

[15] Alexandre 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 Cryptologyages 414 - 428

[16] “Secure Data Hiding Algorithm Using Encrypted Secret message “ by Harshitha K M, Dr. P. A. Vijaya published in International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012 1 ISSN 2250-3153

[17] Ramesh G, Umarani. R,” Data Security In Local A Area Network Based On Fast Encryption Algorithm”, International Journal of Computing Communication and Information System (JCCIS) Journal Page 85-90. 2010.

[18]. Prasanta Kumar Sahoo, Cheguri Rajitha, “Detecting Forged E-Mail using Data Mining Techniques”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1, October 2019

[19]. GHULAM MUJTABA, LIYANA SHUIB , RAM GOPAL RAJ , NAHDIA MAJEED , AND MOHAMMED ALI

AL-GARADI ,”Email Classification Research Trends: Review and Open Issues”, Received April 17, 2017, accepted May 4, 2017, date of publication May 8, 2017, date of current version June 28, 2017. Digital Object Identifier 10.1109/ACCESS.2017.2702187

[20]. Artūrs Lavrenovs, F. Jesús Rubio Melón ,“HTTP Security Headers Analysis of Top One Million Websites”, 2018 10th International Conference on Cyber Conflict

[21]. Rafał Kozik, Michał Choraś, Witold Hołubowicz, “Packets tokenization methods for web layer cyber security”, Logic Journal of the IGPL, Volume 25, Issue 1, February 2017, Pages 103-113, https://doi.org/10.1093/jigpal/jzw044

[22]. Kailas Patil , “AN INSECURE WILD WEB: A LARGE-SCALE STUDY OF EFFECTIVENESS OF WEB SECURITY MECHANISMS”, DOI:10.21917/IJCT.2017.0217 , Corpus ID: 54838104

[23]. Sarika Choudhary, Rajesh Ghusinga, “E-mail Security: Issues and Solutions”, International Journal of Computer Information Systems, Vol. 7, No.4, 2013