Performance Evaluation Of Various Cryptography Algorithms Along With LSB Substitution Technique

Amita Pandey ,Padma Bonde
Department Of Computer Science
Shri ShankaraCharya Institute Of Technology & Management
Bhilai, India

Abstract: ***Now- a-days revealing the knowledge above world-wide-web is starting to become an important difficulty due to protection difficulties. For this reason much more approaches are needed to shield your discussed facts within the credit card funnel. The existing work concentrates on combined cryptography in addition to steganography for you to secure the data although transmitting inside the system. To begin with the data which is usually to be carried through sender for you to phone inside the system has to be encrypted while using encrypted protocol within cryptography. Second your encrypted facts have to be concealed within the graphic or perhaps video clip or perhaps a good music record having support of steganographic protocol. Third by making use of decryption method your phone can easily check out an original facts in the concealed graphic or perhaps video clip or perhaps music record. Transmitting facts or perhaps file may be accomplished through these types of methods are going to be anchored. In this papers most of us implemented about three encrypt approaches such as DES, AES in addition to RSA protocol in conjunction with steganographic protocol such as LSB replacement method in addition to in contrast their functionality of encrypt approaches in line with the examination of it is triggered occasion in the time encryption in addition to decryption practice and in addition it is load measurement experimentally. The complete practice did within C#.***

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

1. Introduction

Cryptography is an effective way for protecting hypersensitive details. It is just a means for stocking and also sending info with kind in which just those people it really is created for go through and also procedure. The evolution associated with encryption is going in the direction of an upcoming associated with limitless possibilities. Stenography is the fine art associated with transferring details as a result of original records. It really is come coming from Greek concept significance "covered writing". Stenography identifies details or perhaps document that is hid in a very photograph, online video or perhaps music document.

A. Cryptography Concepts

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 referred as 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 referred as 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.

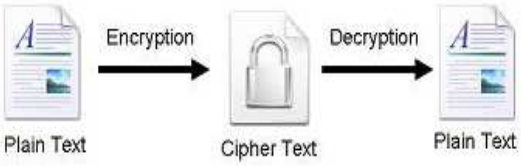


Figure-1: Flow of Encryption-Decryption

2. Literature Review

In this particular segment different overall performance aspect in addition to way of encrypting the information as used by several paperwork are generally listed. Inside the exploration papers [1] suggested that the distinct overall performance aspects are generally outlined such as essential value, computational rate in addition to tunability That they figured AES algorithm is way better amid Symmetric algorithm in addition to RSA algorithm can be found because far better option in asymmetric encryption process. Inside the exploration papers [2] several trial and error aspects are generally analyzed. Good word records utilized plus the trial and error consequence seemed to be figured DES algorithm eats very least encryption time period in addition to AES algorithm work with very least recollection consumption, Encryption time period differs in case there is AES algorithm in addition to DES algorithm. RSA ingest much more

encryption time period in addition to recollection consumption is additionally extremely high however production byte is actually very least in case there is RSA algorithm.

Inside the exploration papers [3] figured each of the techniques are useful intended for real-time encryption. Every process is exclusive in a technique, which might be well suited for distinct apps. Day-to-day completely new encryption process is actually changing therefore quickly in addition to secure typical encryption techniques will certainly always determine having high fee involving protection.

Inside the exploration papers [4] proven a new relative review between encrypting techniques ended up displayed into eight aspects, That happen to be essential length, cipher form, stop dimensions, developed, cryptanalysis level of resistance, protection, probability essential, feasible ACSII printable persona recommendations, time period necessary to look at just about all feasible essential with 50 billion subsequent, these kinds of eligible's proved this AES is way better.

Inside the exploration papers [5] outlined of which DES is actually magic formula essential primarily based algorithm is afflicted with essential submitting in addition to essential deal difficulties. However RSA eats lots of time to perform encryption in addition to decryption functioning. It was in addition observed of which decryption involving DES algorithm surpasses different algorithms in throughput in addition to a lesser amount of energy consumption.

3. Proposed Work

Now the day's acquiring data is a very major challenge to computer systems end users including Small business, Pros as well as Home end users in the intruders. In this particular suggested method we all put in place as well as compared a few diverse encryption protocol intended for data encryption and then the encrypted document is actually concealed inside a photograph through the use of LSB replacement technique. Because shown in Figure-2 both equally cryptography as well as steganography is utilized to enhance the protection connected with data.

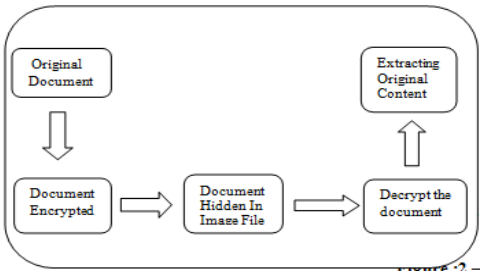


Figure 2. Proposed work

B. From the suggested method a couple of technique utilized because shown in Fig-2. For starters to encrypt the results we all review as well as analyzed a few diverse cryptographic protocols. Subsequently encrypted secret meaning is actually after that introduce in protect marketing through the use of LSB replacement technique in steganographic protocol.

C. 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 key is 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 increase its 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 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'ed 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 Normal (AES) protocol not just regarding security but in addition excellent rate. Equally computer hardware as well as software setup usually are faster even now. New encryption common advised by simply NIST to exchange DES. Encrypts information obstructs associated with 128 pieces with 10, 12 as well as age 14 circular depending on critical size seeing that proven with Figure-3.. It might be implemented with several programs specifically with smaller devices. It can be meticulously screened for many people security applications. These methods prepared with AES protocol.

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 byte 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 InvSubBytes , InvShiftRows , and InvMixColumns

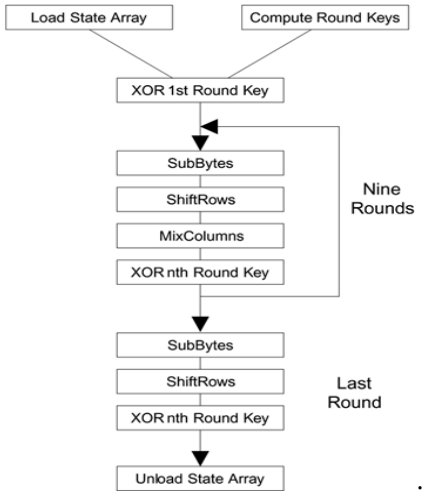


Figure 3. Flow of AES Algorithm

3) RSA : Rivest Shamir Aldeman could be the mostly employed general public key encryption algorithm. RSA working out arises having integers modulo d = p*q. The item demand important factors of at the least 1024 parts for good security. Keys of dimensions 2048 little bit offers greatest security. Trusted intended for risk-free verbal exchanges route along with intended for authentication to identification service provider. RSA is also slow intended for encrypting huge amounts of facts. However it is traditionally used intended for key supply Next steps tend to be put into practice inside RSA to get the public along with exclusive important factors..

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

D. 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 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. 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.

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

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

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. Deviation in buffer size is noticed. It does not increase according to size of file in all algorithms.

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

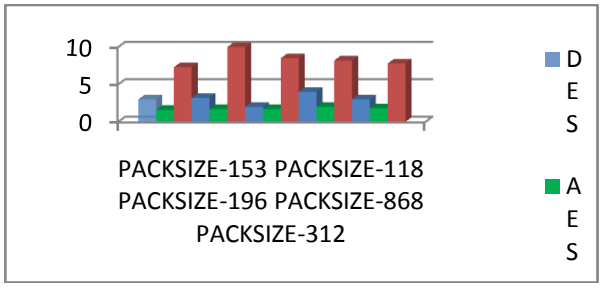
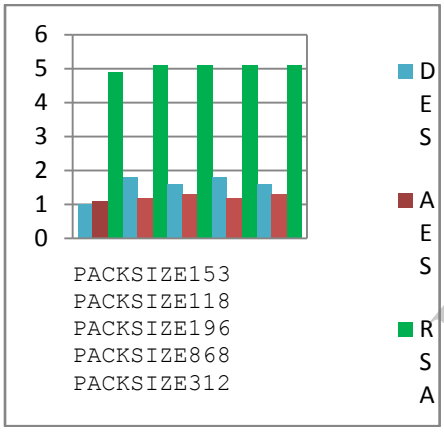
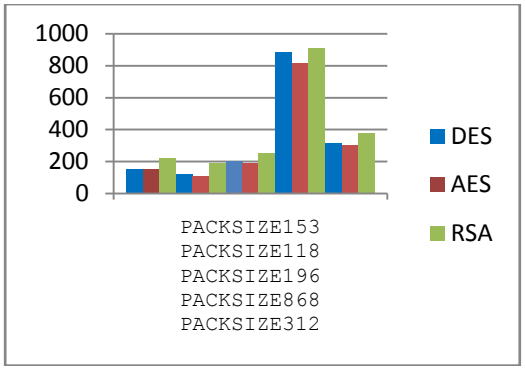


Figure 4. Comparative status of Decryption Time among DES, AES and RSA



By analyzing Fig-3 , Fig-4 which shows time taken for encryption and decryption on different size of file by three algorithms. RSA algorithm takes much longer time compare to time taken by AES and DES algorithm. AES and DES algorithm show very minor variation in time taken for encryption and decryption progression.

Figure 5. Comparative analysis of Buffer Size among DES, AES and RSA algorithm



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. Conclusion

In Data connection, encryption formula plays a new critical part. The analysis work surveyed the previous encryption methods including AES, DES along with RSA algorithms in addition to LSB alternative method. Individuals encryption methods tend to be learnt along with assessed very well to market the effectiveness with the encryption procedures in addition to guarantee the safety measures. Based on the experimental result it turned out figured AES formula consumes minimum encryption along with decryption occasion along with barrier use compared to DES formula. Although RSA eat far more encryption occasion along with barrier use can also be high. Most of us in addition discovered that will decryption connected with AES formula surpasses other algorithms. From your simulation result, most of us evaluated that will AES formula are more preferable as compared to DES along with RSA formula.

6. Future Scope

We have compared and analysed various cryptographic algorithms along with the same LSB technique for hiding the document in an image file. Our future 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 I S S N : 2 2 2 9 - 4 3 3 3 (P r i n t) | I S S N : 0 9 7 6 - 8 4 9 1 (On l i n e)www. i j c s t. c o m

[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 the Effect 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] Himani Agarwal &Manish Sharma" Implementation and analysis of various Cryptography" Dec-2010

[9] Gurjeevan Singh, Ashwani Kumar Singla, 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 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.