ISSN: 2321-7782 (Online)
Volume 1, Issue 7, December 2013
International Journal of Advance Research in Computer Science and Management Studies
Research Paper
Available online at: www.ijarcsms.com

Comparing Popular Symmetric Key Algorithms Using Various Performance Metrics

Gurvinder Singh Sandhu[1]
MTech Scholar
Department of Computer Science & Engineering
Punjab Technical University
Jalandhar, Punjab - India

Vinay Verma[2]
MTech Scholar
Department of Computer Science & Engineering
Punjab Technical University
Jalandhar, Punjab - India

Rajesh Kumar[3]
Assistant Professor
Department of Computer Science & Engineering
Punjab Technical University
Jalandhar, Punjab - India

Abstract: ***Plenty of cryptography and steganography based techniques have been developed in the past decades. Some of them are not able to completely ensure the safety of data from permutations, applied by eavesdroppers. Some others make use of large key size and complex procedures to encrypt data for better safety. This creates an extra computational overhead for CPU. Where as some techniques do not ensure even data integrity and hence use other integrity mechanisms, which in turn reduce execution speed. Some techniques have good security and performance, but they are not able to encrypt multimedia data or large volumes of data. In this paper, we compare and analyze popular symmetric key encryption algorithms using various performance metrics. Their features and issues have been highlighted in order to give the researchers a better problem formulation and come up with best solutions in the area of steganography and cryptography.***

Keyword: Stenography, Cryptography, Symmetric Key, Zero Loss, Comparison, Analysis.

I. INTRODUCTION

In the current scenario of internet, user data gets highest priority in the field of data communication. This data must be sent securely so as to keep the internet usage reliable. For this security of data, several ways have been discovered. Some popular ways are cryptography and steganography, water marking etc. Each of these techniques has some problems associated with them. In case of traditional cryptography the sender either uses the transposition cipher or substitution cipher.

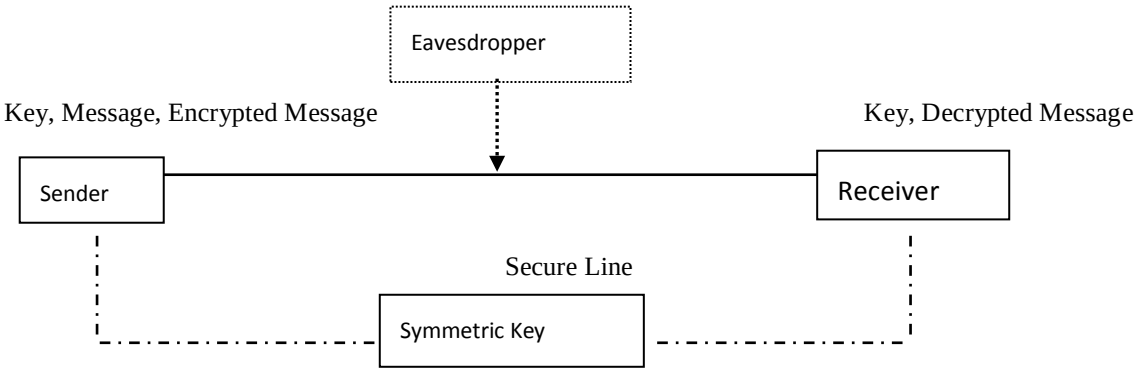

Fig. 1 Traditional Cryptography System

On the other hand, all the standardized symmetric key algorithms use large key and complex operations to achieve confidentiality, such as, Data Encryption Standard (DES), Advance Encryption Standard (AES), and Blowfish etc. Some

algorithms like Triple DES (3DES) follow complex procedure and multiple keys technique to make it difficult for an attacker to decipher it. There is no doubt that these mechanisms make it very hard for the attacker to crack, but they also pose large computational overhead on CPUs and network. As the security levels increases security increases, but the complexity also increases.

Using multiple keys in the ciphering process is a good alternative. But, multiple keys are hard to generate and exchange. It also results in increased network traffic. In order to overcome this problem, some algorithms try to change the data bits with some complex procedures and it results in odds of loss of data integrity and using data integrity algorithms pose extra burden on CPU. Some Steganography techniques or image cryptography techniques use Transform Domain Steganography or Spatial Domain Steganography, which possibly does not return actual data on the receiver end, as the picture restoration algorithms does not ensure 100% integrity.

This paper proposes a comparative analysis of popular crypto systems. It facilitates a global view of the problem and solution space. By setting apart and emphasizing crucial features of cryptography mechanisms, while abstracting detailed differences, these comparisons can be used by researchers to answer many important questions:

- Which data have been handled effectively by existing crypto systems?
- What problems still remain unaddressed and why?
- How would crypto mechanisms perform?
- What are cryptography mechanisms' vulnerabilities?
- Can cryptography mechanisms complement each other and how?

The proposed comparisons are complete because, the comparison provides representative examples of existing mechanisms. These comparisons may not be detailed as possible. Many published algorithm classes could have been left out. Also, new techniques are likely to appear, thus adding new comparisons to the ones we propose. Our goal was to select several important features of security mechanisms that might help researchers design innovative solutions, and to use these features as comparative criteria. It is our hope that our work will be further extended by other researchers.

This paper does not propose or advocate any specific cryptography mechanism. Even though some sections might point out vulnerabilities in certain classes of cryptography techniques, our purpose is not to criticize, but to draw attention to these problems so that they might be solved. Following this introduction, Section 2 addresses the computational overhead or security limitations in some popular existing symmetric key algorithms. Section 3 proposes metrics to measure efficiency of cryptography approaches. Section 4 will describe detailed comparison followed by conclusion in section 5.

II. LITERATURE REVIEW

In the past years various symmetric key encryption algorithms have been developed. Some of these algorithms work very efficiently. But they still have some overheads relating to them. No doubt that there has been a great revolution in the field of internet security, especially cryptography, since the internet concept has come into existence, but the old algorithms have still their importance in various applications, So before discussing the current research findings, it is important to have a glance on the old popular symmetric key algorithms.

In the early days of cryptography, Horst Feistel developed Data Encryption Standard, a symmetric key algorithm to encrypt block of data which is based upon Balanced Feistel network. The algorithm uses 16 different iterations on the data and was designed to operate on different modes. The key size of DES is 56 bits only, which can be broken by Eavesdroppers [1].

To enhance the performance of DES, Triple DES was introduced in 1998 which has a key size of 64 bits. Triple DES encrypts the data by using three different keys. Each triple encryption algorithm encrypts one block of 64 bits of data by

different three 56-bit keys, which enhance size of key to 168 bits. [2]. As there are three security levels, more computations are required at the sender as well as the receiver end. Also the large key size increases the complexity of algorithm. Moreover the keys are of fixed size and do not change with time. Thus the attacker has always a chance to find the key by applying several permutations.

The Advanced Encryption Standard (AES) was developed by Rijmen V, Daemen J in 1998. AES is a variant of Rijndael which has a fixed block size of 128 bits, and has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys [3].

To ensure data security, Debnath Bhattacharya et al. (2009) have proposed an approach to steganography [4]. In this algorithm they combined cryptography, steganography and an extra security layer to encrypt text messages. The algorithm used two public keys and one primary key to encrypt data. This layer concept increases computation time thrice to encrypt/decrypt the text message. Moreover the algorithm works only for text messages.

V.S. Shankar Sriram et al. (2010) introduced an interesting Block Cipher Multiple Key Symmetric Encryption (BCMKSE) algorithm to reduce computational time as well as message overhead. [5]. As this approach is symmetric key based, two private keys which are NOBS (no of bits) and the Key K are computed and shared by sender and receiver by some other modes. The key K is computed by various components like generating MINi (client node related), MINs (server related), SRMPNi (based on screen resolution and mouse position) and Ti (which is a time component). In the same manner NOB is calculated by applying various XOR, addition functions on these components. It is very difficult for eavesdropper to find out the private keys. This symmetric approach is very much secure, but this approach is there is a lot of overhead to compute the values of Key K and NOB which are fixed values and can be assumed as well to reduce computational overhead. Also the key comprises of a combination of server and client related information, which can be easily accessed and used by an attacker to generate the key and the number of permutations for NOB are very less. Any sophisticated attacker can find the key with little overhead of applying permutations. Moreover, this technique has an extra overhead of using MD5 to ensure message integrity.

Aditee Gautam et al. (2011) proposed a new technique using block based transformation which is used for image encryption. In this algorithm image is transformed into other image before encryption process is done. Blowfish algorithm is used for this transformation. [6] Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. It is based upon 16 rounds. There are number of key dependent permutations, variable keys used on data at each round with XOR, addition operations. Blowfish is fast block algorithm, when the same key is used. But computation time increases with changing keys. Each new key requires pre-processing equivalent to encrypting text, which is very slow compared to other algorithms. Secondly, if there is lack of synchronization between two parties then it will not be able to use the same key of encryption and decryption.

For all the above mentioned algorithms, two common problems are there, First, is the much computation is required for different iterations. Second is the unique key size. The key is fixed and it doesn't change with the respective session. So, using a single key for long time doesn't empower the message secrecy. Also all the above mentioned techniques are primarily based upon the encryption of text messages.

Other types of multimedia like audio, video, images etc are getting popularity these days. So the security of these types of media files is needed to be focused. Along with this, these ciphers are capable of encrypting text message to a satisfactory level. But cipher text can be easily decrypted by applying some bruit force techniques. As far as steganography view of 'data confidentiality' is concerned, In the early stages of steganography it was an efficient technique because it was less expected that a media file may contain a hidden message.

In the present state, the eavesdropper is available with lots of technology advancements that they can apply all possible permutations to crack the code. In order to hide data in more efficient manner transform domain steganography has been

developed, which shows less distortion in multimedia content while hiding the text. For providing more security, Multi Layer Data Security algorithms which combine Cryptography and steganography have been used, making the security multilayered increases the computational overhead, which is not acceptable for large volumes of data.

III. PERFORMANCE / EFFICIENCY METRICS

The organizations suffer big losses due to growing number of attacks. The wastage of time caused to users result in lost revenues as time is money in on-line business. Also the terrorist organizations can harm a country by stealing their valuable secret information from the network. As most of the cryptography techniques do not assure complete and efficient security, there is a need to analyze their features in detail, so as to come up with an innovative approach that resolves all issues. In current work, our focus is on measuring the performance metrics of various encryption algorithms. We have measured performance using following metrics:

A. Encryption and Decryption Time

To evaluate computational overhead of the cryptography and steganography algorithms encryption and decryption time parameters are used. These are the basic parameters for measuring the performance of any algorithm.[7]

B. Pearsonian Chi-Square Value

To check the non-homogeneity of the source file and the corresponding encrypted file and also being termed as "Goodness-of-fit chi-square test", with the formula $\lambda^2 = \Sigma\{(f_s - f_e)^2 / f_e\}$, where f_s and f_o respectively being frequency of a character in source file and that of the same in the corresponding encrypted file.[8]

C. Invisibility

The invisibility is the most important requirement of a steganography algorithm, because the strength of steganography lies in its ability to be unnoticed by the human eye. If an Eavesdropper comes to know that an image has been tampered, the algorithm is likely to be compromised.

D. Payload capacity

The main principle of steganography is to hide communication and therefore requires sufficient embedding capacity keeping in mind that it can lead to increasing the space complexity of the algorithm. [9]

E. Robustness against statistical attacks

Statistical analysis is the practice of detecting hidden information by applying statistical tests. Most of the algorithms leave a mark that can be easily detected through statistical analysis. To be able to pass by an eavesdropper without being detected, an algorithm must not leave such a mark in the encrypted file as be statistically significant.[9]

F. Robustness against manipulation

In the secure communication, the file may undergo changes by an eavesdropper in an attempt to remove hidden / encrypted information. File manipulation, can be performed before it reaches its destination. Depending on the manner in which the message is embedded, these manipulations may destroy the hidden message. It is preferable for the algorithms to be robust against either malicious or unintentional changes. [9]

G. Independent of file type

With many different file types used for communication on the Internet, it might seem suspicious that only one type of file is continuously communicated between two parties. The most powerful algorithms thus possess the ability to encrypt any type of information in any type of file. [9]

IV. Results and Discussion

We conducted our comparisons using parameters listed in previous sections. Various files have been analyzed to analyze the metrics for the algorithms and then using them for graphs. Some of the Metrics does not contain actual values because multiple runs constitute only performance levels rather than actual statistical data. The Following comparisons are made on small sized file. The performance of algorithms is analyzed below:

TABLE I
COMPARISON OF STEGANOGRAPHY AND SYMMETRIC KEY BASED ALGORITHMS

Algorithm / Metric	DES	3DES	AES	Blow fish	BCMKSE	LSB Insertion	Aditee Gautam's Approach	RCRDB	IDEA	3D cat map
Encryption Time (Kbps)	0.3	0.8	0.3	0.2	0.18	0.3	0.2	0.2	2.5	0.35
Decryption Time (Kbps)	0.2	0.7	0.3	0.001	0.0001	0.2	0.2	0.2	2.5	0.35
Character Frequency after Chi-Square test	Medium	High	High	High	High	Medium	High	High	Medium	Low
Invisibility	High	High	High	High	High	Medium	High	High	High	High
Payload capacity	Low	Low	Low	Low	Low	Low	High	High	High	Medium
Robustness against statistical attacks	Medium	High	High	High	High	Low	High	High	High	High
Robustness against manipulation	Low	Low	Low	Low	Low	Low	Low	Low	Low	Medium
Independent of file Type	No	No	No	No	No	Yes	No	No	No	Yes

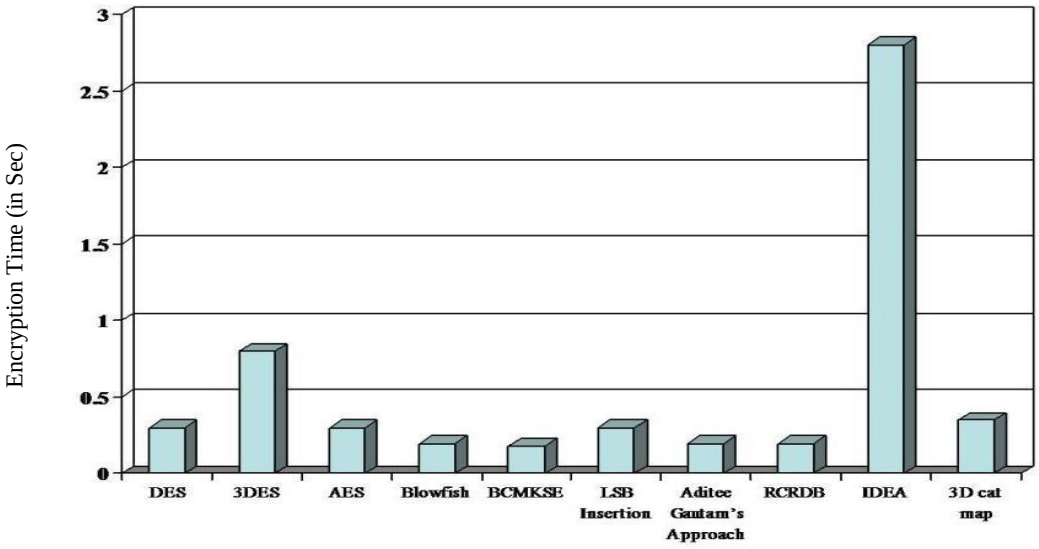

Fig 2: Comparison of Various Cryptography Algorithms Based On Encryption Time

V. Conclusion

There are various cryptography and steganography mechanisms available in related work for ensuring the safety of user data from being cracked by eavesdroppers; existing mechanisms are implemented on text or image files. Each technique has some limitations due to openness and vulnerabilities in the architecture of internet and they are unable to defend data from bruit force techniques. Few mechanisms have employed complex implementations, large key size and many security levels, which is not acceptable due to high QoS requirements.

Measurement of performance of various algorithms is quantified in terms of Encryption Time (Kbps), Decryption Time (Kbps), Chi-Square Value, Invisibility, Payload capacity, Robustness against statistical attacks, Robustness against

manipulation, Independent of file Type in this work. We evaluate our metrics in experiments on the text and image files. We used files of different sizes so that algorithms' efficiency can be compared at different scenarios of problem space. The future scope of this work is summarized as below:

- Computing the cumulative comparison of Algorithms by combining weight of all the metrics.
- Building a new Security Mechanism by introducing all the good features of existing techniques.

Acknowledgement

We would like to express our gratitude to all those who gave us the possibility to complete this experimental work. We are extremely thankful to all the colleagues and faculty members for their constructive criticism and guidelines.

References

1. Federal Information Processing Standards Publication 46-3, "Data Encryption Standard (DES)."U.S. DoC/NIST, October 25,1999..
2. American National Standard for Financial Services 1998, "Triple Data Encryption Algorithm Modes of Operation." American Bankers Association, Washington, D.C. X9.52- July 29, 1998.
3. Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography algorithms simulation based performance analysis" International Journal of Emerging technology and Advanced Engineering, Volume 1, Issue 2,December (2011).
4. Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay and Tai-hoon Kim, "Text Steganography: A Novel Approach", in "International Journal of Advanced Science and Technology", Vol 3, Feb 2009.
5. V.S.Shankar Sriram, Abhishek Kumar Maurya, G.Sahoo,"A Novel Multiple Key Block Ciphering Mechanism with Reduced Computational Overhead" in "International Journal of Computer Applications", Vol.1 (No.17):25–30, February 2010
6. Aditee Gautam, Meenakshi Panwar and Dr.P.R Gupta "A New Image Encryption Approach Using Block Based Transformation Algorithm", (IJAEST) international Journal of advanced engineering sciences and technologies Vol No. 8, Issue No. 1, 090 – 096, 2011.
7. Nidhi Singhal, J.P.S.Raina, "Comparative Analysis of AES and RC4Algorithms for Better Utilization", in "International Journal of Computer Trends and Technology", 2011
8. Pranam Paul, Saurabh Dutta, A K Bhattacharjee, "An Approach to ensure Security through Bit-level Encryption with Possible Lossless Compression" in "International Journal of Computer Science and Network Security", VOL.8 No.2, February 2008.
9. Gajendra Singh Chandel, Ravindra Gupta, Swati Jain, " Proposed Model of Dynamic encryption using Steganography" in "International Journal of Emerging Technology and Advanced Engineering", Volume 2, Issue 9, September 2012

AUTHOR(S) PROFILE

Gurvinder Singh Sandhu, received the B.Tech. in Computer Science & Engineering from Guru Teg Bahadur Khalsa Institute of Engineering & Technology, Malout. He is pursuing his M.Tech from LLRIET, Moga. His area of research is network security and data security.
Presently he is working as an Assistant Professor at Guru Teg Bahadur Khalsa Institute of Engineering and Technology, Chhapian wali, Malout (India)

Vinay Verma, received the B.Tech. in Computer Science & Engineering from Giani Zail Singh College of Engineering & Technology; Bhatinda He is pursuing his M.Tech from BGIET, Sangrur. His area of interest is network and data security.
Presently he is working as an Assistant Professor at Baba Hira Singh Bhattal Institute of Engineering and Technology, Lehragaga, (India)

Rajesh Kumar, is working as an Assistant Professor in the department of Computer Science & Engineering at BGIET, Sangrur. His Major areas of interest are Data Security and Digital Image Processing.

