COMPARITIVE ANALYSIS OF ENCRYPTION ALGORITHM FOR INFORMATION SECURITY

Shaista Siddiqui[1], Samta Gajbhiye[2]

[1] *Research scholar, Department of Computer Science and Engineering, Shri ShankaraCharya Technical Campus, Bhilai, CG, India.*
[2] *Sr. Associate Professor &Head, Department of Computer Science and Engineering, Shri Shanakracharya Technical Campus, Bhilai, CG, India*

ABSTRACT

With the advancement in various multimedia technologies, more and more multimedia data are generated and transmitted in the medical, commercial and military fields. These videos might include some sensitive information which should not be accessed by or can only be partially exposed to the general users. Therefore, security and privacy has become an important aspect. Over the last few years, various technologies and encryption algorithms have been emerged.. Cryptanalytic work has shown that there exist security problems and other weaknesses in most of the proposed multimedia encryption methods. In this paper, a description and a comparison between encryption methods is presented. Comparisons are made on the basis of parameters like encryption speed, security level and stream size.

Keyword : - *Public key, secret key, DES,RSA,AES,encryption*

1. INTRODUCTION

To achieve secure communication over internet, data can be protected by the method of encryption which means converting the data by any encryption algorithm using the 'key' in scrambled form. Only users having access to that key can decrypt the encrypted data. [1]

Encryption is a fundamental tool for the protection of sensitive information. Encryption is used to maintain privacy in the communications. It is like talking to someone while others are listening but such that other people cannot understand what is being said. [2].

Encryption algorithms can be categorized into symmetric (private) and asymmetric (public key). [1]

In symmetric key or secret key encryption, only one key is used for encryption and decryption of data. In asymmetric key or public key, two pairs of key 'public' and 'private' is used. Public key is used for encryption and private key is used for decryption [3]

1.1 BASIC ENCRYPTION ALGORITHMS

With the increase in use of internet many encryption algorithms have been proposed. Most popular among those are the AES DES and RSA. The basic concepts of these algorithms have been discussed below.

1.1.1 DES Algorithm

Introduction DES is a block cipher, with a 64 bit block size and a 56 bit key. DES consists of all 6 rounds series of substitution and permutation. In each round, data and key bits are shifted, permuted and XORed and sent through, 8 s-boxes, a set of lookup tables that are essential to the DES algorithm. Decryption is essentially the same process performed in reverse [4].

1.1.2 AES Algorithm

AES uses 10,12 or 14 rounds. Depending upon the number of rounds, key size can be of 128,192,256 bits. AEs uses several rounds and each rounds in AES consists of several stages. To provide security AES uses types of

transformation. Substitution, permutation, mixing and key adding each round of AES except the last uses the four transformation [5]

1.1.3 RSA Algorithm

RSA is the most commonly used public key cryptography algorithm. RSA is named for the three mathematicians who developed it, Rivest, Shamir and Adleman. RSA today is used in hundreds of software products and can also be used exchanging keys, in digital signatures and encrypting small blocks of data. RSA uses a variable size encryption block and variable size key. The pair of key is derived from very large number n that is the product of two prime numbers chosen according to special rule. [2]

2. LITERATURE REVIEW

It was concluded in [6] that AES is faster and more efficient algorithm. When the transmission of data is considered there are insignificant differences in performances of different symmetric key schemes. A study in [5] is conducted for different popular secret key algorithm as DES, AES, and Blowfish. They were implemented and their performances were compared by encryption input files of varying content and sizes .A study in [7] is conducted in which AES DES RSA were examined with different data sizes under different parameters like computation time, output byte, memory usage. The paper concluded that DES algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES algorithm and DES algorithm. RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm.

3.RESULT AND ANALYSIS

As per the experimental results of [7] the following table was formed with the observations made. By analyzing the table 1, it was observed that RSA has very smaller output byte compare to AES and DES algorithm. Time taken by RSA algorithm was much higher compare to the time taken by AES and DES algorithm. By analyzing chart1 which depicts the time taken for encryption on various size of file by three algorithms i.e. AES DES and RSA, it is noticed that RSA takes much longer time compared to AES and DES. AES and DES have very minute difference in time taken for encryption which DES having least time. Chart. 2 Shows the memory usage by AES, DES and RSA. It was observed that for RSA algorithm memory usages are highest for all sizes of text file while memory usage is least. Chart 3 shows the size of output byte for each algorithm used in experiment. The result of Fig shows same size of output byte for different size of text file in case of all three algorithms.

Table 1: Comparison of AES,DES,RSA in terms of time, memory and output

DATA	ALGO.	TIME (SEC)	MEMORY (KB)	OUTPUT BYTE
FILE 1 (68KB)	AES	2.2	81,912	131,072
	DES	1.8	85,261	131,072
	RSA	9.4	91,814	65,536
FILE 2 (105)	AES	2.1	62,544	131,072
	DES	1.8	67,531	131,072
	RSA	10.5	77,117	65,536
FILE 3 (124 KB)	AES	2.2	53,902	131,072
	DES	2	55,395	131,072
	RSA	11.4	57,178	65,536
FILE 4 (235KB)	AES	2.4	16,679	131,072
	DES	2.1	21,189	131,072
	RSA	16.2	26,891	65,536

FILE 5 (435KB)	AES	2.6	34,207	131,072
	DES	2.4	42,113	131,072
	RSA	24.4	44,321	65,536

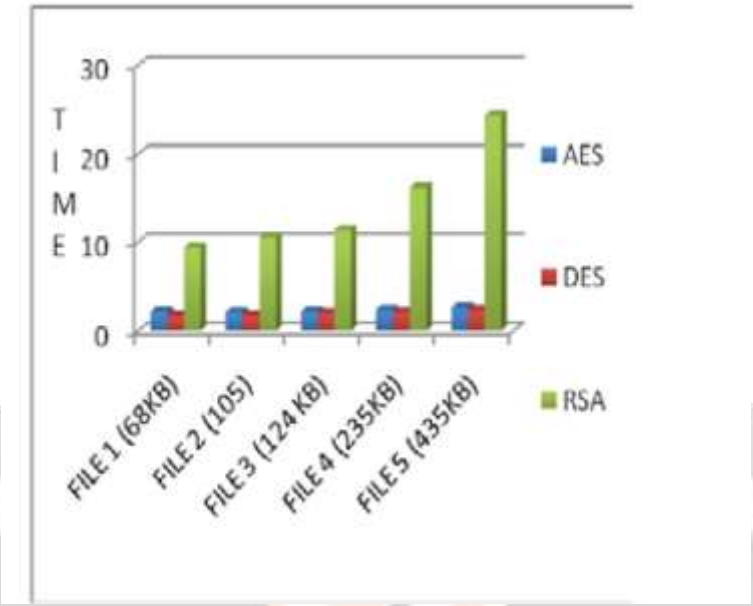

Chart -1: Computation time of AES, DES and RSA

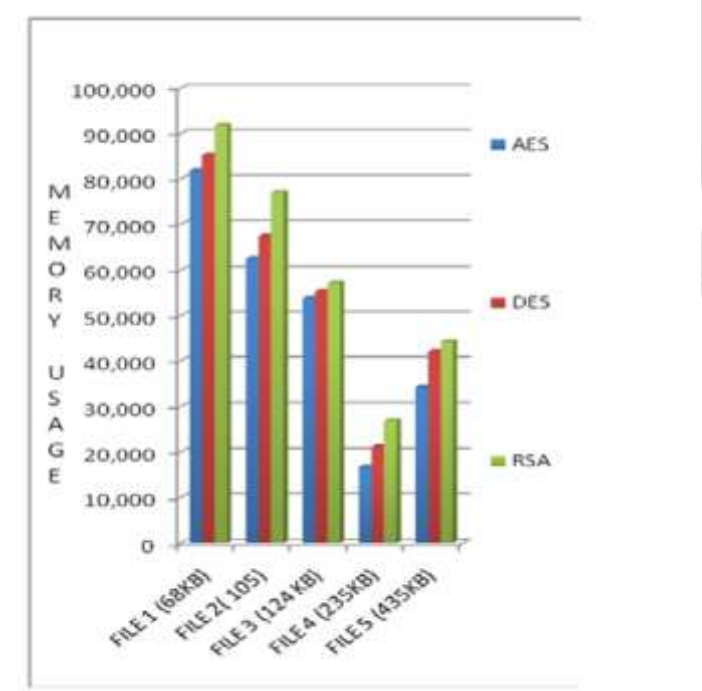

Chart2: Comparison of memory usage by AES, DES and RSA

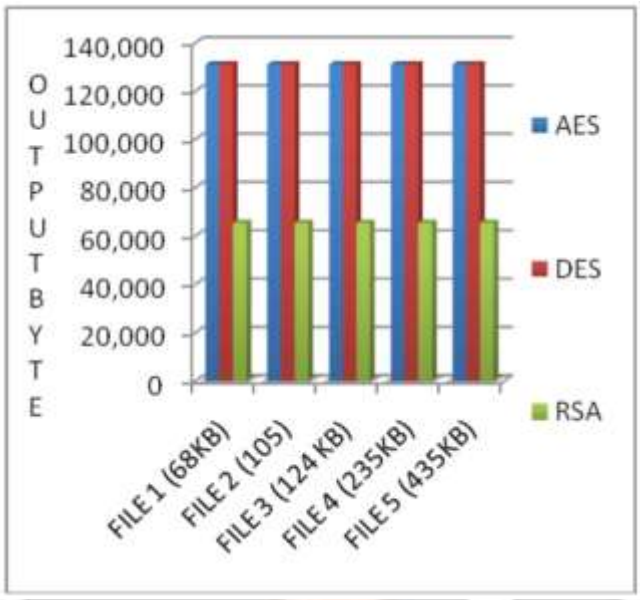

Chart3: Computation of output byte used by AES, DES and RSA

4. CONCLUSIONS

This paper presented a detailed study of the popular Encryption algorithm such as AES, DES and RSA With increase in usage of internet, the requirement to secure the data transmitted over different networks using different services is also increased. In this paper a survey on the existing work on the encryption algorithm is done. To summarize, all these techniques are good for real time encryption. Each technique is unique In its own way which might be suitable for different applications and has its own pro's and con's.

5. REFERENCES

[1] P.Ruangchaijatupon, P.Krishnamurthy, "Encryption andpower consumption in wireless LANs-n," The Third IEEE workshop on wireless LANS, pp. 148-152, Newton,Massachusetts, sep. 27-28, 2001.

[2] [Marshall D.Abrams, Harold J.podell on Cryptography

[3] Hardjono, security in wireless LANS and MANS, Artech house Publisher, 2005.

[4] Diaasalama, Abdul kader, MohiyHadhoud, "Studying the Effect of Most Common Encryption Algorithms", International Arab Journal of e-technology, vol 2,no.1,January 2011.

[5] A.Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.Bn

[6] Hirani, Energy Consumption of Encryption schemes in wireless device Thesis, university of Pittsburgh, Apr. 9, 2003,Retrieved Oct.1, 2008

[7] Shashi Mehrotra Seth, Rajan mishra"Comparitive Analysis of Encryption Algorithm for data communication" IJCST vol2,Issue 2,June 2011

[8] Gurpreet Singh,Supriya, "A study of Encryption algorithm(RSA,DES,3DES and AES) for Information Security.IJCA, vol67, no 19, April 2013

[9] NeetuSettia. "Cryptanalysis of modern Cryptography Algorithms". International Journal of Computer Science and Technology. December 2010

[10] Andrea Pellegrini, Valeria Bertacco, Todd Austin on topic Fault-Based attack of RSA Authentication