Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 15 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Study of Encryption Algorithms AES, DES and RSA for Security

By Dr. Prerna Mahajan & Abhishek Sachdeva
IITM, India

Abstract- In recent years network security has become an important issue. Encryption has come up as a solution, and plays an important role in information security system. Many techniques are needed to protect the shared data. The present work focus on cryptography 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 encryption algorithm in cryptography. Secondly, by using decryption technique the receiver can view the original data. In this paper we implemented three encrypt techniques like AES, DES and RSA algorithms and compared their performance of encrypt techniques based on the analysis of its stimulated time at the time of encryption and decryption. Experiments results are given to analyses the effectiveness of each algorithm.

Keywords: DES, RSA, AES, encryption, decryption, private key encryption, public key encryption, cryptography.

GJCST-E Classification : E.3

Strictly as per the compliance and regulations of:

A Study of Encryption Algorithms AES, DES and RSA for Security

Dr. Prerna Mahajan [α] & Abhishek Sachdeva [σ]

Abstract- In recent years network security has become an important issue. Encryption has come up as a solution, and plays an important role in information security system. Many techniques are needed to protect the shared data. The present work focus on cryptography 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 encryption algorithm in cryptography. Secondly, by using decryption technique the receiver can view the original data. In this paper we implemented three encrypt techniques like AES, DES and RSA algorithms and compared their performance of encrypt techniques based on the analysis of its stimulated time at the time of encryption and decryption. Experiments results are given to analyses the effectiveness of each algorithm.

Keywords: DES, RSA, AES, encryption, decryption, private key encryption, public key encryption, cryptography.

I. Introduction

Many encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys [1]. Public key is used for encryption and private key is used for decryption (e.g. RSA). Public key encryption is based on mathematical functions, computationally intensive. There are many examples of strong and weak keys of cryptography algorithms like DES, AES. DES uses one 64-bits key while AES uses various 128,192,256 bits keys [2].

Asymmetric key encryption or public key encryption is used to solve the problem of key distribution. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (E.g. RSA and Digital Signatures). Because users tend to use two keys: public key, which is known to the public and private key which is known only to the user[2]. There is no need for distributing them prior to transmission. However, public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices [3]. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [4].

This study evaluates three different encryption algorithms namely; AES, DES and RSA. The performance measure of encryption schemes will be conducted in terms of encryption and decryption time such as text or document[5].

II. Encryption Algorithms

Encryption is a well known technology for protecting sensitive data. Use of the combination of Public and Private Key encryption to hide the sensitive data of users, and cipher text retrieval [6].

a) Data Encryption Standard (DES)

DES (Data Encryption Standard) algorithm purpose is to provide a standard method for protecting sensitive commercial and unclassified data. In this same key used for encryption and decryption process [7].
DES algorithm consists of the following steps

i. *Encryption*

1. DES accepts an input of 64-bit long plaintext and 56-bitkey (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

i. The key is split into two 28 halves
ii. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
iii. 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.
iv. The rotated key halves from step 2 are used in next round.
v. The data block is split into two 32-bit halves.
vi. One half is subject to an expansion permutation to increase its size to 48 bits.
vii. Output of step 6 is exclusive-OR'ed with the 48-itcompressed key from step 3.
viii. 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.
ix. Output of step 8 is subject to a P-box to permute the bits.

Authors α σ : e-mail: aabhi616@yahoo.in

x. 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.

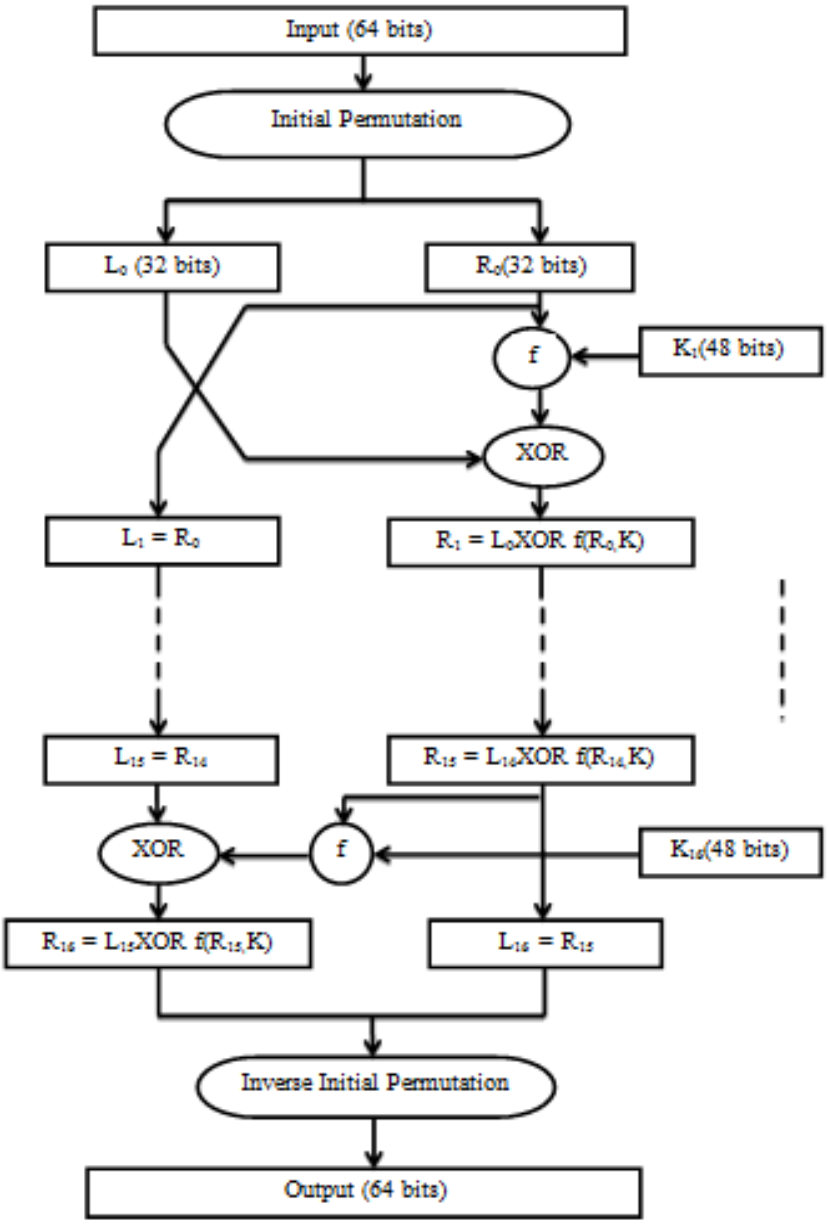

Figure 1 : Diagram of DES Algorithm

b) Advanced Encryption Standard (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 - 2. It can be implemented on various platforms specially in small devices. It is carefully tested for many security applications.

i. ***Algorithm Steps :*** These steps used to encrypt 128-bit block

1. The set of round keys from the cipher key.
2. Initialize state array and add the initial round key to the starting state array.
3. Perform round = 1 to 9 : Execute Usual Round.
4. Execute Final Round.
5. Corresponding cipher text chunk output of Final Round Step

ii. *Usual Round :* Execute the following operations which are described above.

1. Sub Bytes
2. Shift Rows
3. Mix Columns
4. Add Round Key , using K(round)

iii. *Final Round:* Execute the following operations which are described above.

1. Sub Bytes
2. Shift Rows
3. Add Round Key, using K(10)

iv. *Encryption :* Each round consists of the following four steps:

i Sub Bytes : The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.

ii Shift Rows : In the encryption, the transformation is called Shift Rows.

iii Mix Columns : The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.

iv Add Round Key : Add Round Key proceeds one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition.

The last step consists of XO Ring the output of the previous three steps with four words from the key schedule. And the last round for encryption does not involve the "Mix columns" step. [8]

v. *Decryption:* Decryption involves reversing all the steps taken in encryption using inverse functions like a) Inverse shift rows, b) Inverse substitute bytes, c) Add round key, and d) Inverse mix columns.

The third step consists of XO Ring the output of the previous two steps with four words from the key schedule. And the last round for decryption does not involve the "Inversemix columns" step.

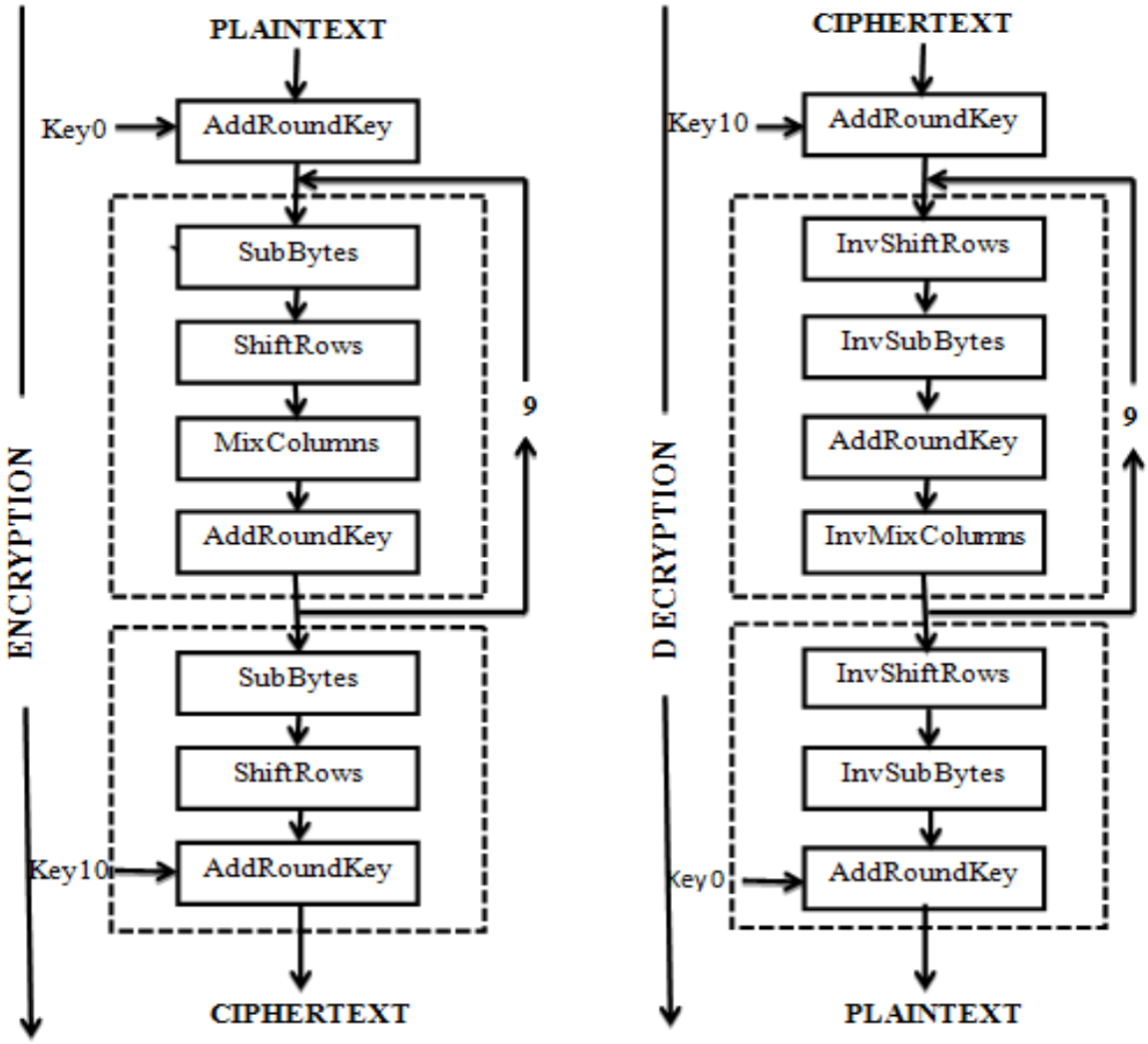

Figure 2 : AES Encryption and Decryption

c) Rivest-Shamir-Adleman (RSA)

RSA is widely used Public-Key algorithm. RSA firstly described in 1977. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it.

RSA algorithm involves these steps:

1. Key Generation
2. Encryption
3. Decryption

i *Key Generation*

Before the data is encrypted, Key generation should be done. [9]

Steps:

Generate a public/private key pair :

1. Generate two large distinct primes p and q
2. Compute $n = pq$ and $\varphi = (p-1)(q-1)$
3. Select an e, $1 < e < \varphi$, relatively prime to φ.
4. Compute the unique integer d, $1 < d < \varphi$ where $ed \equiv_{\varphi} 1$.
5. Return public key (n, e) and private key d

ii *Encryption*

Encryption is the process of converting original plain text (data) into cipher text (data).

Encryption with key (n , e)

1. Represent the message as an integer $m \in \{0, \ldots, n-1\}$
2. Compute $c = m^e \bmod n$

iii *Decryption*

Decryption is the process of converting the cipher text (data) to the original plain text(data). [10]

Decryption with key d: compute $m = c^d \bmod n$

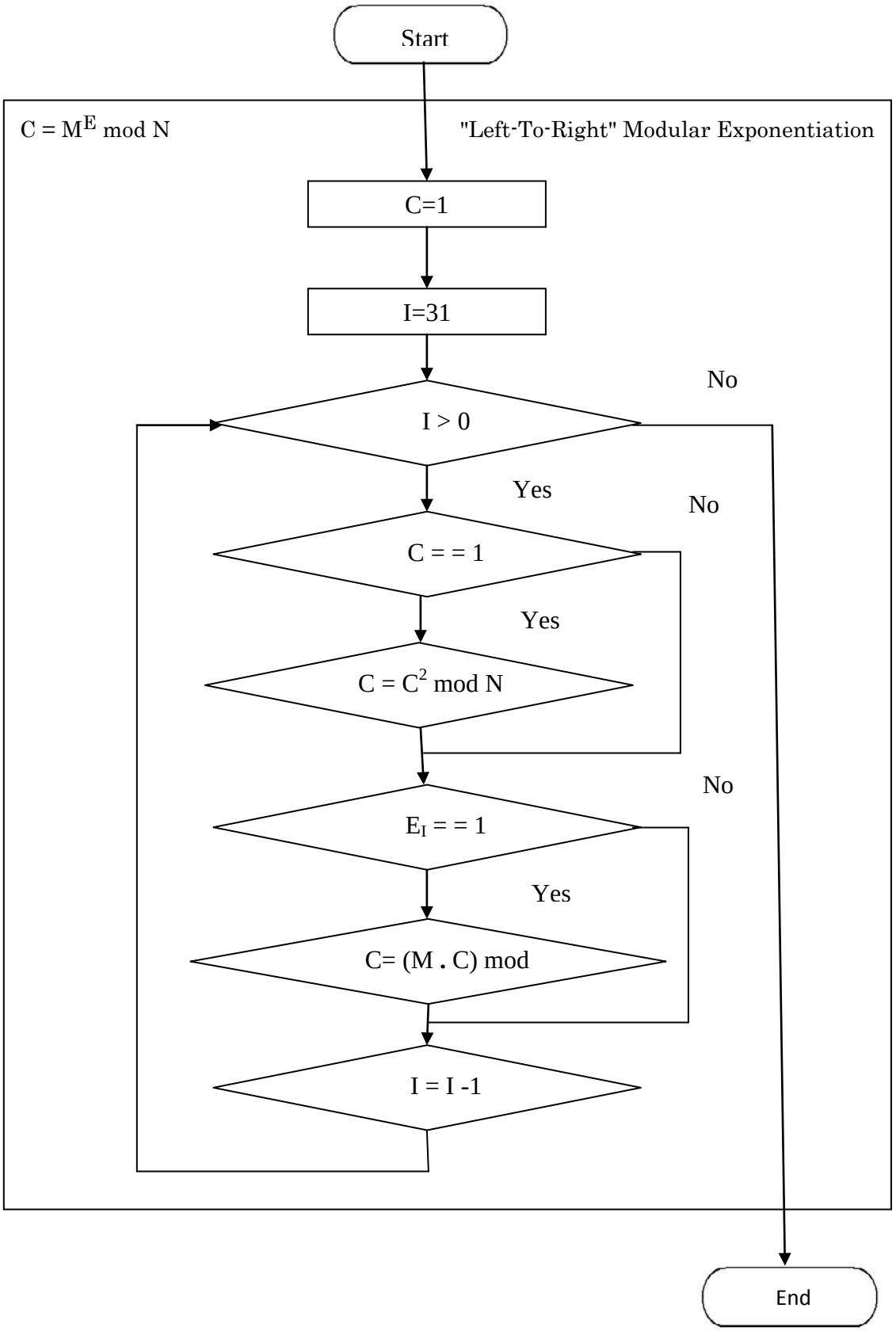

Figure 3 : RSA Encryption and Decryption Flowchart

III. Comparision

In the table below a comparative study between AES, DES and RSA is presented in to eighteen factors, which are Key Size, Block Size, Ciphering & Deciphering key, Scalability, Algorithm, Encryption, Decryption, Power Consumption, Security, Deposit of keys, Inherent Vulnerabilities, Key used, Rounds, Stimulation Speed, Trojan Horse, Hardware & Software Implementation and Ciphering & Deciphering Algorithm.

Table 1: Comparison between AES, DES and RSA

Factors	AES	DES	RSA
Developed	2000	1977	1978
Key Size	128, 192, 256 bits	56 bits	>1024 bits
Block Size	128 bits	64 bits	Minimum 512 bits
Ciphering & deciphering key	Same	Same	Different
Scalability	Not Scalable	It is scalable algorithm due to varying the key size and Block size.	Not Scalable
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm
Encryption	Faster	Moderate	Slower
Decryption	Faster	Moderate	Slower
Power Consumption	Low	Low	High
Security	Excellent Secured	Not Secure Enough	Least Secure
Deposit of keys	Needed	Needed	Needed
Inherent Vulnerabilities	Brute Forced Attack	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced and Oracle attack
Key Used	Same key used for Encrypt and Decrypt	Same key used for Encrypt and Decrypt	Different key used for Encrypt and Decrypt
Rounds	10/12/14	16	1
Stimulation Speed	Faster	Faster	Faster
Trojan Horse	Not proved	No	No
Hardware & Software Implementation	Faster	Better in hardware than in software	Not Efficient
Ciphering & Deciphering Algorithm	Different	Different	Same

IV. Experimental Design

The four text files of different sizes are used to conduct four experiments, where a comparison of three algorithms AES, DES and RSA is performed.

a) Evaluation Parameters

Performance of encryption algorithm is evaluated considering the following parameters.

A. Encryption Time
B. Decryption Time

The encryption time is considered the time that an encryption algorithm takes to produces a cipher text from a plain text. Encryption time is used to calculate the throughput of an encryption scheme, is calculated as the total plaintext in bytes encrypted divided by the encryption time. Comparisons analyses of the results of the selected different encryption scheme are performed. [11]

V. Experimental Results And Analysis

Experimental result for Encryption algorithm AES, DES and RSA are shown in table-2, which shows the comparison of three algorithm AES, DES and RSA using same text file for four experiment.

Table 2 : Comparisons of DES, AES and RSA of Encryption and Decryption Time

S.NO	*Algorithm*	*Packet Size (KB)*	*Encryption Time (Sec)*	*Decryption Time (Sec)*
1	AES	153	1.6	1
	DES		3.0	1.1
	RSA		7.3	4.9

2	AES	196	1.7	1.4
	DES		2.0	1.24
	RSA		8.5	5.9
3	AES	312	1.8	1.6
	DES		3.0	1.3
	RSA		7.8	5.1
4	AES	868	2.0	1.8
	DES		4.0	1.2
	RSA		8.2	5.1

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.

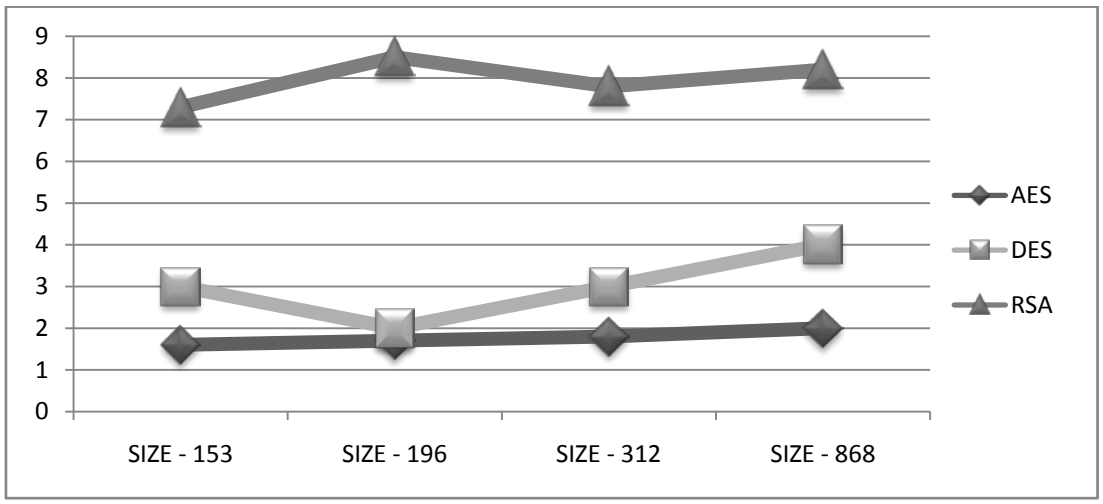

Figure 4 : Comparison of Encryption Time among AES, DES and RSA

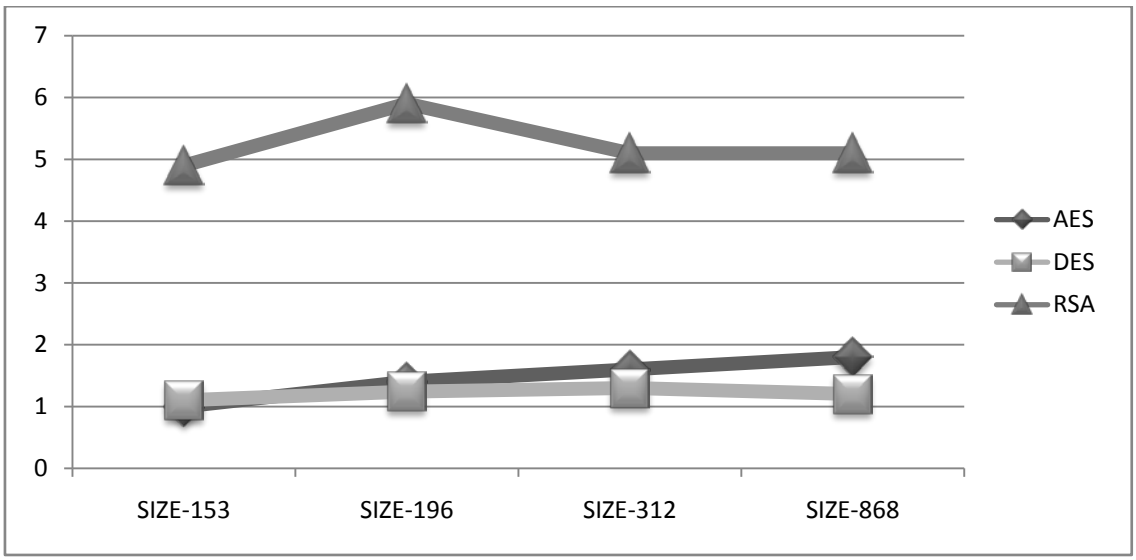

Figure 5 : Comparison of Decryption Time among AES, DES and RSA

By analyzing Fig-4 , Fig-5 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 algorithm show very minor difference in time taken for encryption and decryption process.

VI. Conclusion

Encryption algorithm plays very important role in communication security. Our research work surveyed the performance of existing encryption techniques like AES, DES and RSA algorithms.

Based on the text files used and the experimental result it was concluded that AES algorithm consumes least encryption and RSA consume longest encryption time.

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.

Our future work will focus on compared and analysed existing cryptographic algorithm like AES, DES and RSA. It will include experiments on image and audio data and focus will be to improve encryption time and decryption time.

References Références Referencias

1. Idrizi, Florim, Dalipi, Fisnik & Rustemi, Ejup. "Analyzing the speed of combined cryptographic algorithms with secret and public key". *International Journal of Engineering Research and Development*, *e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 8, Issue 2 (August 2013)*, pp. 45
2. Abdul.Mina, D.S, Kader, H.M. Abdual & Hadhoud, M.M. "Performance Analysis of Symmetric Cryptography". pp. 1.
3. Chehal Ritika, Singh Kuldeep. "Efficiency and Security of Data with Symmetric Encryption Algorithms". *International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X , Volume 2, Issue 8, August 2012,* pp. 1.
4. Hardjono, "Security In Wireless LANS And MANS," Artech House Publishers 2005.
5. Elminaam, Diaa Salama Abd, Abdual Kader, Hatem Mohamed & Hadhoud, Mohiy Mohamed. "Evaluating The Performance of Symmetric Encryption Algorithms". *International Journal of Network Security, Vol.10, No.3, May 2010*, pp. 216.
6. Padmapriya, Dr.A, Subhasri, P. "Cloud Computing: Security Challenges & Encryption Practices". *International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 3, March 2013,* pp. 257.
7. Prashanti.G, Deepthi.S & Sandhya Rani.K. "A Novel Approach for Data Encryption Standard Algorithm". *International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013,* pp. 264.
8. Das Debasis, Misra Rajiv. "Programmable Cellular Automata Based Efficient Parallel AES Encryption Algorithm". International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011, pp. 204.
9. Kalpana Parsi, Singaraju Sudha. "Data Security in Cloud Computing using RSA Algorithm". International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012. pp. 145.
10. Sunitha K, Prashanth K.S. "Enhancing Privacy in Cloud Service Provider Using Cryptographic Algorithm". IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 5 (Jul. - Aug. 2013). pp. 64.
11. Singh Narjeet, Raj Gaurav. "Security On Bccp Through Aes Encryption Technique". International Journal Of Engineering Science & Advanced Technology Volume-2, Issue-4, 813 – 819. pp. 817.

.