An Open Access Journal Available Online

Comparative Analysis of Encryption Algorithms

Nureni Ayofe Azeez[1] & Sayyidina'Aliyy Bolaji Abubakar[2]

[1,2]Department of Computer Sciences, Faculty of Science,
University of Lagos, Nigeria
nazeez@unilag.edu.ng
cloudcompt12@gmail.com

Abstract— the vulnerable nature of some sensitive and classified information such as health and bank related data has undoubtedly caused serious havoc to individuals who should enjoy the privacy and confidentiality of their information. In an attempt to guarantee absolute security of information from one source to another and also to prevent confidential information from being revealed to unauthorized people, encryption algorithms are being used to achieve this. Encryption algorithms are basically useful for securing and protecting data being transmitted from one end to another from any form of vulnerability. Over the years, researchers have adopted some of these algorithms to ensure privacy of information in banking, health and military. Some of these algorithms are varied in terms of efficiency, accuracy, reliability and response time whenever they are used for data protection. In an attempt to carry out a comparative assessment, we considered Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES) and Data Encryption Standard (DES) algorithms. Since there is skepticism on which of the algorithms is more reliable, dependable and functional when considering features that characterized their variation, this work therefore, attempts to do a comparative assessment of each of the encryption algorithms to ascertain the best using the stated metrics. The implementation was carried out with C#. The results obtained from the experimentation revealed that AES uses the lowest time for encryption while RSA consumes longest encryption time. Also, AES algorithm is considered the most efficient of all the three algorithms based on the metrics used for the evaluation. Few of the results obtained are presented in this paper.

Keywords/Index Terms— encryption, decryption, analysis, algorithm, audio and video.

1. Introduction

Various Internet applications have emerged in the recent years. Some of these transactions such as internet banking, e-commerce and stock trading are carried out over wireless or cable network that requires efficient and reliable end-to-end connection. What is more? The connection from one end to another end must strictly be protected and confidential to guarantee availability, integrity and confidentiality of information sharing across the network (Tingyuan, Chuanwang & Xulong, 2010.).

With the advent of advance technology in telecommunication and military, the need for more compact, highly secured data, files inclusive, military Intelligence for national security and global unity is important. Encryption comes to play with the sole aim of developing a technique for security mechanism to prevent, protect illegal access to data and files. The need for more complex ways to encrypt and decrypt with algorithms sprung up with various ways of encrypting files, data, password contents which spans across audio, video, pictures and messages (MAbdul, 2009).

Security in computing can simply be defined as a mechanism put in place to ensure that information and services within an organization, a domain, network is well protected, safeguarded from unauthorized individual, illegal access, manipulation, destruction or other vulnerabilities (Azeez and Venter, 2013). Cryptography is considered one of the main approaches being used in networking for achieving security.

Also, encryption is another major technique for ensuring security and privacy of sensitive and classified information. Over the years, encryption algorithms such as AES, RES and DES have been used successfully to protect sensitive and confidential information in military and health institutions. Encryption algorithms allow protection of information from one end to anther (AmanKumar & SudeshJakharet, 2012).

Since the implementation of cryptography has become difficult and complex with the emergence of human intelligence, encryption has become a better and reliable alternative being used by information security experts across the globe. Consequently, in this paper, a comparative assessment of encryption algorithms of DES, AES and RSA was carried out and tested with Audio and Video files. The results obtained are shown in this paper.

Decision was reached on the three algorithms used for evaluation because of their popularity along with observable contradictory results obtained on them from previous researches. What is more, they can provide relatively good performance on the comparative assessment task in this work.

2.Literature Review

Sharma and Sharma, 2016 presented a cryptographic algorithm that is FPGA based. It was used for hiding data. They implemented an algorithm that is multi-keyed in nature with key updated functionality that is real time. In the experiment, both sender and receiver update keys with adequate synchronization. The algorithm was designed using Verilog HDL while Spartan 3E Starter Kit was used for realization. The algorithm has a great benefit of changing keys per cycle. This

provides the benefit of making it extremely tough to break.

Singh and Supriya, 2013 did a comparative assessment of four encryption algorithms RSA, DES, 3DES and AES. They justified their work on the fact that some of the existing work on the encryption algorithms are real-time and that each of the techniques is special and unique in its own way which are definitely applicable to different applications. The research carried out revealed that AES algorithm is most efficient when considering speed, throughput, time as well as avalanche effect.

Seth et al. 2011 did a comparative assessment of RSA, DES and AES while considering metrics such as memory usage, output byte and computation time which are regarded as the major issues of worry in nearly all Encryption Algorithm. In this work, the experimental results reveal that that DES encryption algorithm consumes lowest time for encryption while AES encryption algorithm consumes the lowest memory usage. Finally, it was established that RSA takes longest encryption time as well as memory usage while RSA has the least output byte.

Elminaam et al., 2008 analyzed the performance of encryption algorithms with entirely different metrics. They evaluated most common algorithms: DES, 3DES, RC2, Blowfish, and RC6. Metrics considered for evaluation include encryption/decryption speed, different sizes of data blocks, different sizes of data blocks, different data types and different key size. The experimental results reveal that there is no much difference when the results are shown in base 64 encoding or hexadecimal base encoding. Also, RC6 requires less time when compared to all encryption algorithms except Blowfish. When changing data type was considered, it was discovered that Blowfish, RC6 and RC2 have merit over other algorithms with respect to time consumption.

Pavithra et al., 2012 did a performance evaluation of different encryption algorithms. They considered time as their main metric. Different video files were considered for the experimentation to affirm their processing speed by each of the algorithms. Also, different video file formats such as .DAT and .vob were considered with various sizes. The experimental results reveal that AES encryption algorithms is the best in terms of throughput level and processing time when compared to Blowfish and DES.

Mandal et al., 2012 compared advanced encryption standard (AES) and data encryption standard (DES) using avalanche effect, memory requirement as well as simulation time for both algorithms. The experimental results show that AES has a very high avalanche effect when compared to DES. However, the time required for simulation for DES is higher when compared to AES. This implies that AES is basically useful for message encryption.

The need for this similar research is as a result of different results obtained by researchers when evaluating the encryption algorithms. Also, some of the algorithms were empirically evaluated with different files. Some researchers used audio, images, videos and text files hence there is no uniformity in the results obtained. Aside from these issues, metrics used for evaluation are different. Some used timing required to encrypt, size of the

files, speed and memory requirements for encryption.

3. Evaluation Parameters

3.1. Encryption time

This can simply be defined as the time required to convert a given plaintext to ciphertext. This is dependent on plaintext block size, key size and mode. In this work, we succeeded in measuring the encryption time milliseconds.

3.2. The Decryption time

This is the time required to get back plaintext from ciphertext. In the implementation of this work, we have successfully measured the time for decryption in milliseconds.

3.3. Memory used

Each of the encryption techniques requires a unique and different memory size for its implementation. The number of required memory depends on the size of the file, type of operations, initialization vectors as well as key size adopted. For an algorithm to be termed as being effective, the memory requirement must be very small.

4. Implementation, Findings and Results

Implementation

AES, RSA and DES encryption algorithms have successfully been implemented. They were implemented with Java by using Eclipse IDE. We made use of both java crypto and java security packages which enable several security features such as authorization, authentication, decryption and encryption.

Also, audio and video files of difference sizes were considered (Ten (10) different types of multi-media file formats ranging from 500kb, 1024kb to 900mb) for the empirical evaluation of the algorithms as input files for encryption process. Each of the encrypted files is saved and later decrypted. To have a consistent and reliable comparison, the same input files were used for all the three algorithms.

A single system was used throughout for the implementation and analysis. This was done to ensure and ascertain that memory maintains the same for AES, RSA and DES encryption algorithms.

The two classes previously mentioned can be divided into two subsections. The first class carries out cryptography which implements operations to be transferred while the second class is the access control and authorization classes that perform digital signatures. With the libraries of the package, AES, RSA and DES encryption algorithms were conveniently and successfully implemented with little changes to the calling functions.

s/n	AUDIO	VIDEO
1	MP3	MP4
2	Flaac	FLV
3	.rm	3gp
4	Wma	mkv
5	M3u	webm
6	Amr	
7	M4a	

Table 1 shows the file format used for the implementation and testing of the three algorithms.

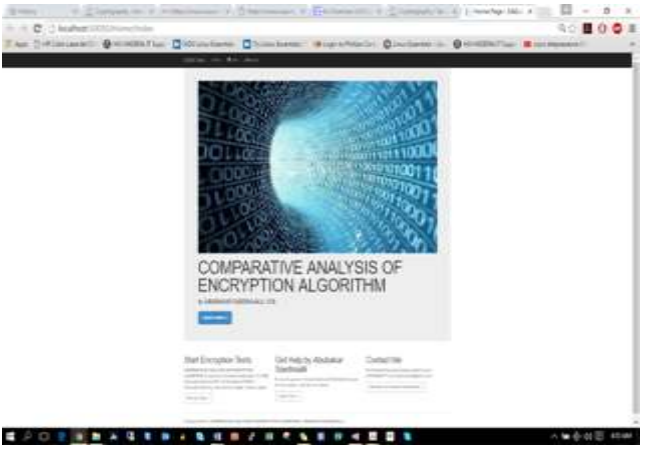

Figure 1. Design interface

5. Data Analysis

After the entire encryption process, the output is displayed in web format form which is then extracted into Excel sheet for further analysis to be discussed in the next chapter. A sample is given in Figure II:

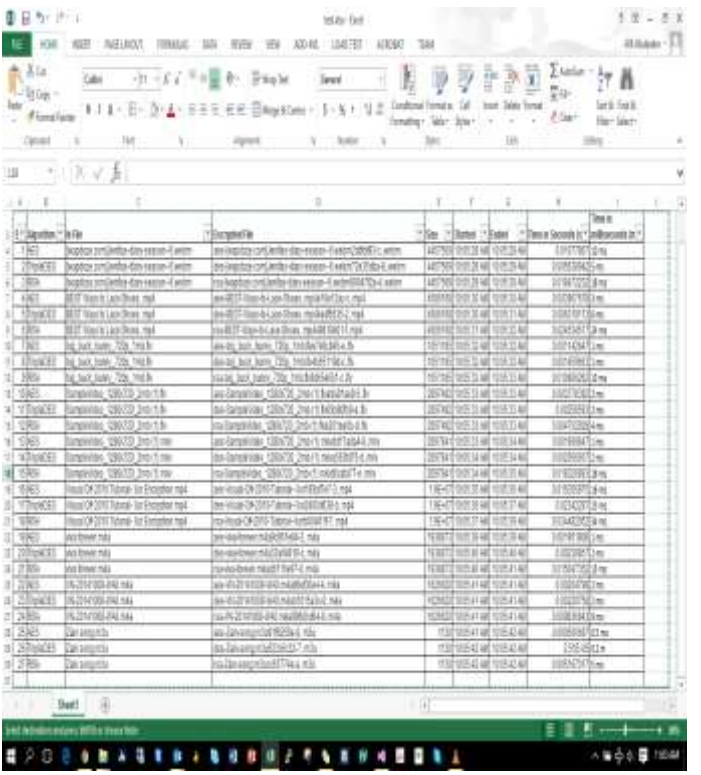

Figure 2: Result Exported to Excel for Analysis

Table 2: AES Audio and Video Results with size and Time

S/N	Algorithm	Size	Time in milliseconds (ms)
1	AES	4457569	10 ms
4	AES	4506168	3 ms
7	AES	1051185	1 ms
10	AES	2097492	2 ms
13	AES	2097841	1 ms
16	AES	19483441	16 ms
19	AES	1938873	1 ms
22	AES	1626620	2 ms
25	AES	1130	0.5 ms

From table Two (2), it was observed that the file format .mp4 and .webm took the longest time for encryption due to the file size of about 4.4mb and 19.4mb. With other format faster to encrypt with about the same file size with different format.

Table 3: DES Audio and Video Results with Size and Time

S/N0	Algorithm	Size	Time in milliseconds (ms)
2	DES	4457569	5 ms
5	DES	4506168	6 ms
8	DES	1051185	1 ms
11	DES	2097492	2 ms
14	DES	2097841	2 ms
17	DES	19483441	23 ms
20	DES	1938873	2 ms
23	DES	1626620	2 ms
26	DES	1130	0.2 m

From table three (3), it was observed that the file format .mp4 took the longest time for encryption, the rest file format moderately of the same time for encryption there about.

Table 4: RSA Audio and Video Results with size and Time

S/N	Algorithm	Size	Time in milliseconds (ms)
3	RSA	4457569	18 ms
6	RSA	4506168	24 ms
9	RSA	1051185	10 ms
12	RSA	2097492	4 ms
15	RSA	2097841	18 ms
18	RSA	19483441	34 ms
21	RSA	1938873	15 ms
24	RSA	1626620	9 ms
27	RSA	1130	5 ms

From Table Four (4), it took almost four times the time of encryption of AES, whilst the same for DES. This shows it's not a faster means and it is slow when used for encryption.

Table 5: Result Exported to Pivot Data for Analysis Combined

S/N	Algorithm	Size	Time in milliseconds (ms)
1	AES	4457569	10 ms
4	AES	4506168	3 ms
7	AES	1051185	1 ms
10	AES	2097492	2 ms
13	AES	2097841	1 ms
16	AES	19483441	16 ms
19	AES	1938873	1 ms
22	AES	1626620	2 ms
25	AES	1130	0.5 ms
2	DES	4457569	5 ms
5	DES	4506168	6 ms
8	DES	1051185	1 ms
11	DES	2097492	2 ms
14	DES	2097841	2 ms
17	DES	19483441	23 ms
20	DES	1938873	2 ms
23	DES	1626620	2 ms
26	DES	1130	0.2 m
3	RSA	4457569	18 ms

6	RSA	4506168	24 ms
9	RSA	1051185	10 ms
12	RSA	2097492	4 ms
15	RSA	2097841	18 ms
18	RSA	19483441	34 ms
21	RSA	1938873	15 ms
24	RSA	1626620	9 ms
27	RSA	1130	5 ms

Table five (5) shows the extraction of all the encryption methods used with the file size (Mb) and Time (mS) to be used for Analysis (Graph and Bar chats) while Table 5, Pivot table broken down and finalized from Table Six (6) with the help of excel.

Table 6: Audio Video Encryption Algorithm Finalized

Sum of Size	**Algorithms**			**Grand Total**
	AES	**RSA**	**DES**	
0.2 m			1130	1130
0.5 ms	1130			1130
1 ms	5087899		1051185	6139084
10 ms	4457569	1051185		5508754
15 ms		1938873		1938873
16 ms	19483441			19483441
18 ms		6555410		6555410
2 ms	3724112		7760826	11484938
23 ms			19483441	19483441
24 ms		4506168		4506168
3 ms	4506168			4506168
34 ms		19483441		19483441
4 ms		2097492		2097492
5 ms		1130	4457569	4458699
6 ms			4506168	4506168
9 ms		1626620		1626620
Grand Total	**37260319**	**37260319**	**37260319**	**111780957**

Figure Four (4) provides the combined Histogram output for all Algorithm used; File Size (Mb) plotted against Time (mS). The tallest Histogram Bar indicates the file format in each Figure from Figure 6, 8, and 10. With the longest time for encryption extracted from (Figure 3); (.webm for AES, .mp4

for DES, and .mp4 for RSA) likewise other histogram.

In Figures 6, 8 and 10, the yellow line indicates the encryption moving average time difference between different file format and sizes. While the red line gives the sudden fall and rise due to file format, sizes simultaneously, for each encryption algorithm technique used. The black line indicates the steady states of time between file format and size simultaneously due to the upload into the application/design used based on each algorithm implemented.

6. Conclusion

Each of the encryption algorithms has unique characteristics that is known for across the globe. Before using any of these algorithm therefore, it is very important the features of such algorithm are well known and familiar with since they are characterized with strengths and weaknesses. Having considered few metrics, as explained in the previous section, the results of the empirical evaluation has shown that Advanced Encryption Standard (AES) is the best when compared with the performances of RSA and DES under the same condition.

Acknowledgment

The authors wish to acknowledge the efforts of anonymous referees for their valuable comments and helpful suggestions in shaping this paper into a publishable condition.

.

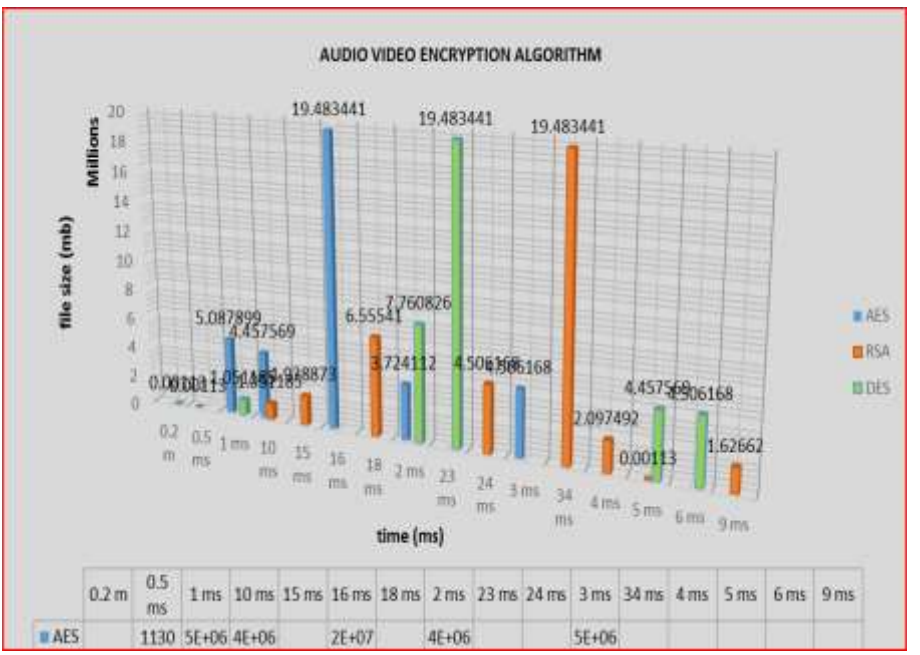

Figure 3: Combined Histogram Output for all Algorithms

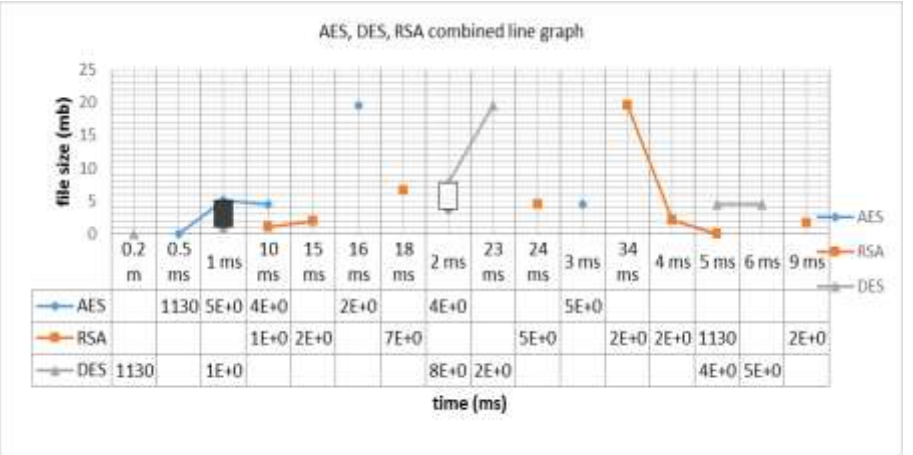

Figure 4: AES, DES, RSA combined line graph

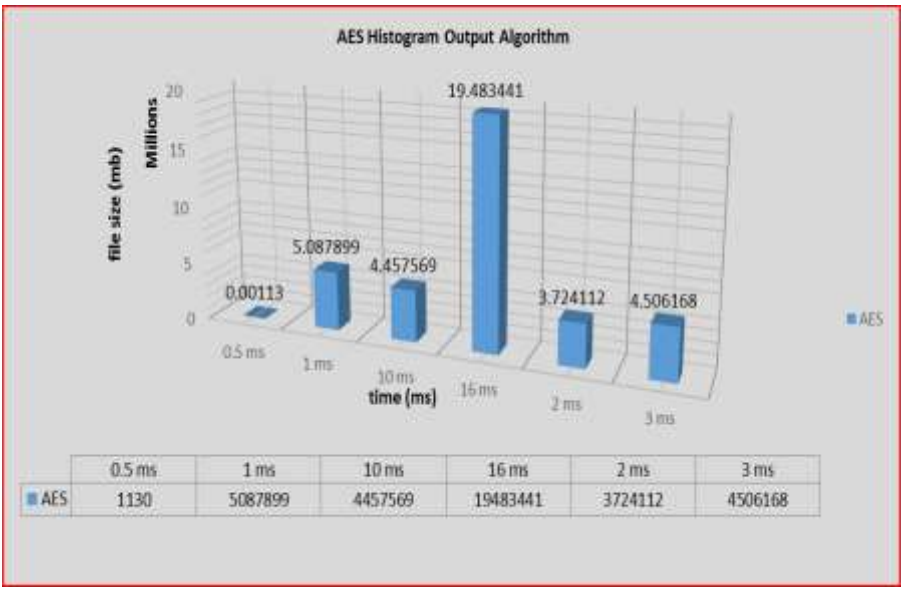

Figure 5: AES Histogram Output Algorithm

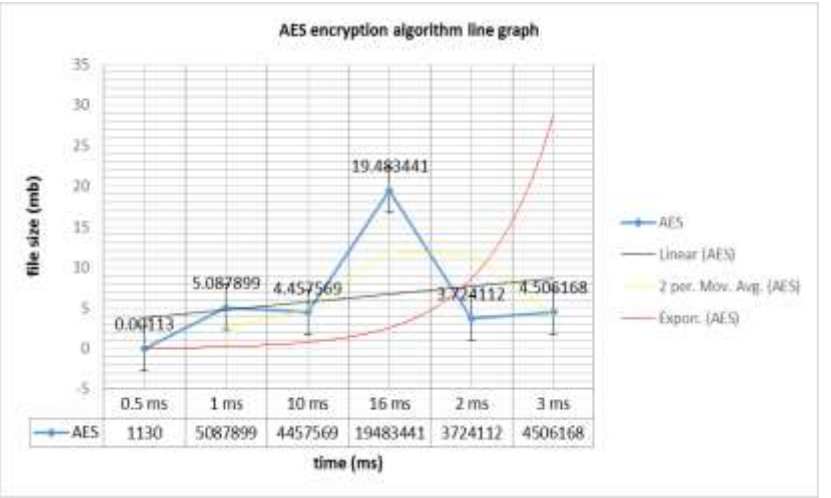

Figure 6: AES Encryption Algorithm Line Graph

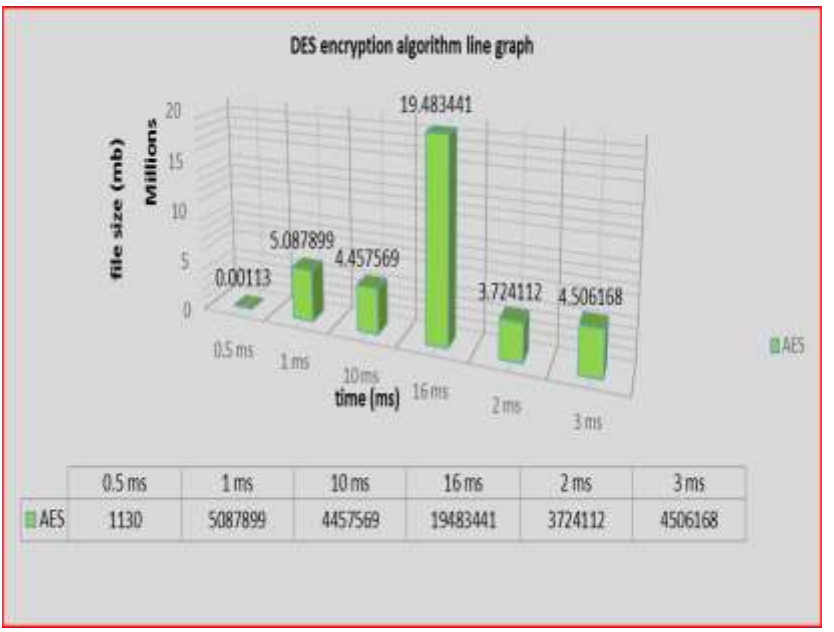

Figure 7: DES Encryption Algorithm Line Graph

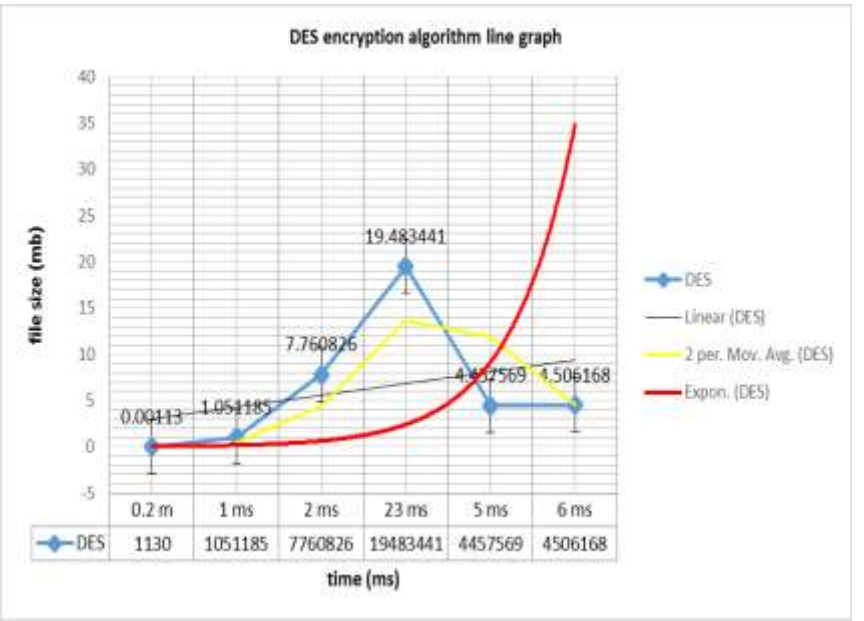

Figure 8: Des Encryption Algorithm Line Graph

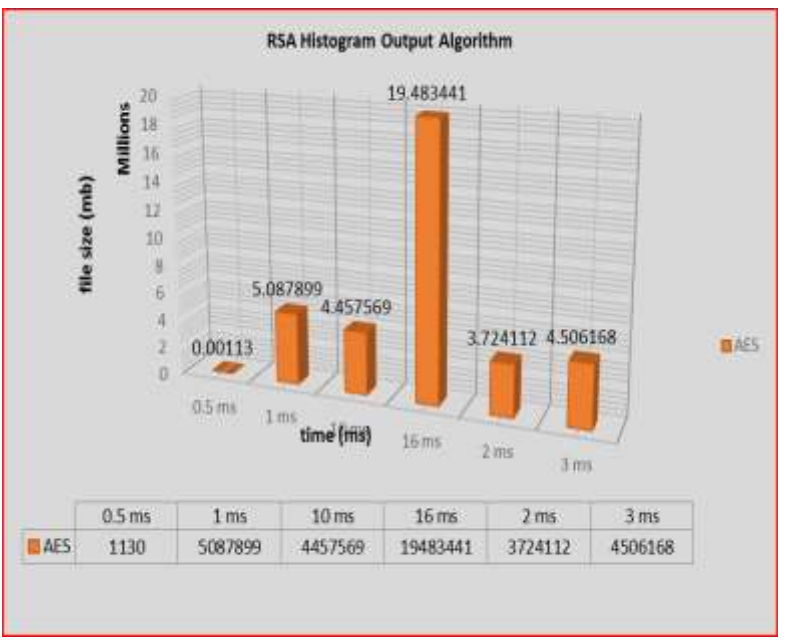

Figure 9: Rsa Histogram Output Algorithm

References

Oorschot, M.V and. Vanstone, J. (1996), Handbook of Applied Cryptography,CRC Press, 1996 (www.cacr.math.uwaterloo.ca/hac)

Stankovic, _P and. Wagner, K (2004), "Security in Wireless Sensor Networks,"ACM,Vol.47,No.653.2004

Hadhoud (2009) "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA,Volume 8, 2009, pp. 58-64

Agrawal, B and Pradeep, T (2012) "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering(IJCSE),Vol.4No.05 May2012, pp. 877-882.

Mandal, R and Tiwari, Y (2012), "Performance Evaluation of Cryptographic Algorithms: DES and AES",IEEE Students' Conference on Electrical, Electronics and Computer Science, pp.1-5,2012.

Kumar, P and Makkar, H (2012) "Comparative Analysis between DES and RSA Algorithm's", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue7,pp.386-391, July2012.

Yuke T and Wang, F(2002) "An efficient implementation of multi-prime RSA on DSP processor, University of Texas,Texas, USA,2002.

Yogesh, A.K (2013) "ComparativeStudyofDifferentSymmetricKeyCryptography",IJAIEM,vol.2,Issue7, July2013, pp. 204-206.

Sharma, L and Sharma, G (2016) "Design and Implementation of Encryption Algorithm for Real Time Speech Signals" 2016 Conference on Advances in Signal Processing (CASP). Cummins College of Engineering for Women, Pune. Jun 9-11, 2016, pp 237-241.

Seth, S.M, Rajan Ishra, R (2011)"Comparative Analysis of Encryption Algorithms for Data Communication", International Journal of Computer Science and Technology, Vol. 2, Issue 2, pp. 292-294, June 2011.

Elminaam, D.S, Kader, H.M and Hadhoud, M.M (2008) "Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, pp. 280-286, December 2008.

Pavithra, S and Ramadevi, E (2012) "Performance Evaluation of Symmetric Algorithms", Journal of Global Research in Computer Science, Volume 3, No. 8, pp. 43-45, August 2012.

Mandal, A.K, Parakash, C and Tiwari, A (2012) "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012.

Kakkar, A, Singh, M. L and Bansal,

P.K. (2012) "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", International Journal of Engineering and Technology, Volume 2 No. 1, pp. 87-92, January 2012.

Ayofe, A.N, Adebayo, S.B, Ajetola, A.R, Abdulwahab, A.F (2010) "A framework for computer aided investigation of ATM fraud in Nigeria" International Journal of Soft Computing, Vol. 5, Issue 3 pp. 78-82

Azeez, N.A, Olayinka, A.F, Fasina, E.P, Venter, I.M. (2015) "Evaluation of a flexible column-based access control security model for medical-based information" Journal of Computer Science and Its Application. Vol. 22, Issue 1, Pages 14-25

Azeez, N. A., and Ademolu, O. (2016). CyberProtector: Identifying Compromised URLs in Electronic Mails with Bayesian Classification. 2016 International Conference Computational Science and Computational Intelligence (CSCI) (pp. 959-965). Las Vegas, NV, USA: IEEE.

Azeez, N. A., and Babatope, A. B. (2016). AANtID: an alternative approach to network intrusion detection. The Journal of Computer Science and its Applications. An International Journal of the Nigeria Computer Society, 129-143.

Azeez, N. A., and Iliyas, H. D. (2016). Implementation of a 4-tier cloud-based architecture for collaborative health care delivery. Nigerian Journal of Technological Development, 13 (1), 17-25.

Azeez, N. A., and Venter, I. M. (2013). Towards ensuring scalability, interoperability and efficient access control in a multi-domain grid-based environment. SAIEE Africa Research Journal, 104 (2), 54-68.

Azeez, N. A., Iyamu, T., and Venter, I. M. (2011). Grid security loopholes with proposed countermeasures. In E. Gelenbe, R. Lent, and G. Sakellari (Ed.), 26th International Symposium on Computer and Information Sciences (pp. 411-418). London: Springer.

Azeez, N.A., and Lasisi, A. A. (2016). Empirical and Statistical Evaluation of the Effectiveness of Four Lossless Data Compression Algorithms. Nigerian Journal of Technological Development, Vol. 13, NO. 2, December 2016, 64-73.

Nureni, A. A., and Irwin, B. (2010). Cyber security: Challenges and the way forward. Computer Science & Telecommunications, 29, 56-69.

Azeez, N. A. (2012). Towards Ensuring Scalability, Interoperability and Efficient Access Control In a Triple-Domain Grid-Based Environment. Cape Town: University of the Western Cape.

Azeez, N. A. (2012). Towards Ensuring Scalability, Interoperability and Efficient Access Control In a Triple-Domain Grid-Based Environment. Cape Town: University of the Western Cape.

Azeez, N.A and Venter, I.M (2012).

Towards achieving scalability and interoperability in a triple-domain grid-based environment (3DGBE)- Information Security for South Africa (ISSA), 2012, pp 1-10.

N.A Azeez and A.E. Otudor (2016) "Modelling and Simulating Access Control in Wireless Ad-Hoc Networks" Fountain Journal of Natural and Applied Sciences. Vol 5(2), pp 18-30.

.