IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 6, Issue 10, October 2019

A new Cryptographic Algorithm AEDS (Advanced Encryption and Decryption Standard) for data security

Ali Mohammed Ali Argabi[1], **Md Imran Alam**[2]

Student, Department of Computer and Network Engineering, College of CS & IT, Jazan, Saudi Arabia[1]

Lecturer, Department of Computer and Network Engineering, College of CS & IT, Jazan, India[2]

Abstract: Nowadays security is very important to protect our sensitive information in computer or over the internet such as in online banking, online shopping, stock market and bill payments etc. Without security our information exchanged over internet are not safe. Encryption Algorithms provides the security to the information which is exchanged over the internet. In this project we are proposing a new cryptographic algorithm AEDS (Advanced Encryption and Decryption Standard) which is developed by combining properties of DES and AES algorithms. Then we compared all these three algorithms and we found that AEDS is more secure and robust for data security.

Keywords: Encryption, Algorithms, AEDS, DES, AES, Security, Internet

I. INTRODUCTION

Nowadays security is very important to protect our sensitive information in computer or over the internet such as in online banking, online shopping, stock market and bill payments etc. Without security our information exchanged over internet are not safe. Encryption Algorithms provides the security to the information which is exchanged over the internet. Encryption algorithms play a big role in providing data security against malicious attacks. There are two types of Encryption Algorithms:

First type is Symmetric key encryption also called private key or one key encryption algorithm. In this algorithm same key is used to encrypt and decrypt data, such as DES (Data Encryption Algorithm) and AES (Advanced Encryption Standard) algorithms.

Second type is Asymmetric key also called public key encryption algorithm, which uses one key for encryptions of data and other key for decryption of data such as RSA and ElGamal algorithms.

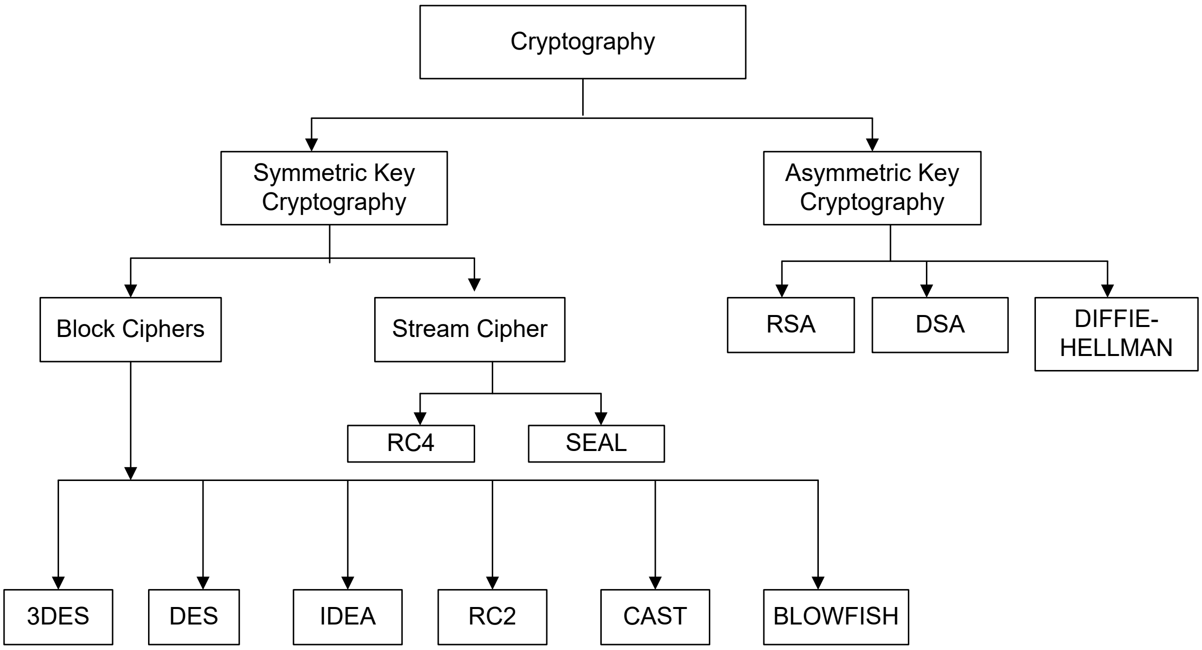


Fig. 1

DOI 10.17148/IARJSET.2019.61001

Above Fig. 1 shows classification and some invented algorithms of cryptography.

In this paper we are proposing a new cryptographic algorithm AEDS (Advanced Encryption and Decryption Standard) which is developed by combining DES and AES algorithms. We expect AEDS will be more secure and robust as compared to DES and AES.

II. LITERATURE REVIEW

In this section, the various performance factors and techniques used for encrypting and decrypting data used by various research papers are listed.

In the research paper [1] various experimental factors are analysed. Based on the text files used and the experimental results it was concluded that DES algorithm consumes least encryption time and AES algorithm use least memory usage. Encryption time differs in case of AES algorithm and DES algorithm.

Paper[2] presents a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are AES, DES, and 3DES, RC6, Blowfish and RC2. In the case of changing data type such as image instead of text, it was found that RC2, RC6 and Blowfish has disadvantage over other algorithms in terms of time consumption.

In the research paper [3] shown a new comparative study between encrypting techniques were presented in to nine factors, which are key length, cipher type, block size, developed, cryptanalysis resistance, security, possibility key, possible ACSII printable character keys, time required to 170 check all possible key at 50 billion second, these eligible proved the AES is better.

Paper [4] surveyed the existing encryption techniques like AES, DES and RSA algorithms along with LSB substitution technique. Those encryption techniques are studied and analysed well to promote the performance of the encryption methods also to ensure the security. Based on the experimental result it was concluded that AES algorithm consumes least encryption and decryption time and buffer usage compared to DES algorithm, but RSA consume more encryption time and buffer usage is also very high. 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

In Paper [5] it is discussed that in symmetric key encryption techniques the AES algorithm is specified as the better solution then follows the blowfish algorithm. In the Asymmetric encryption technique, the RSA algorithm is more secure key generation. since it uses the factoring of high prime number hence, the RSA algorithm is found as the better solution in this method.

III. OBJECTIVES AND IMPORTANCE OF RESEARCH TO SOCIETY

Our Objectives are as follows:

We implemented DES, AES and new Cryptographic algorithm AEDS in Java programming language. Then we compared these algorithms based on parameters like encryption time and decryption time. The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. The decryption time is considered the time that a decryption algorithm takes to reproduce a Plaintext from a Cipher text.

Based on decryption time, we analysed our algorithm is stronger than other two algorithms (AES and DES) or not. Our algorithm AEDS is taking more time in decryption as compared to previous algorithms AES and DES, it means our algorithm is more complex and not easy to break. So, we can say our proposed algorithm is stronger than others.

Importance of research to society

Nowadays Computers have a huge impact on society and the world will never be again the way it was before computers. Research in one of the field of computer science (Cryptography) has positive impact on humankind and society in more ways than we can think of.

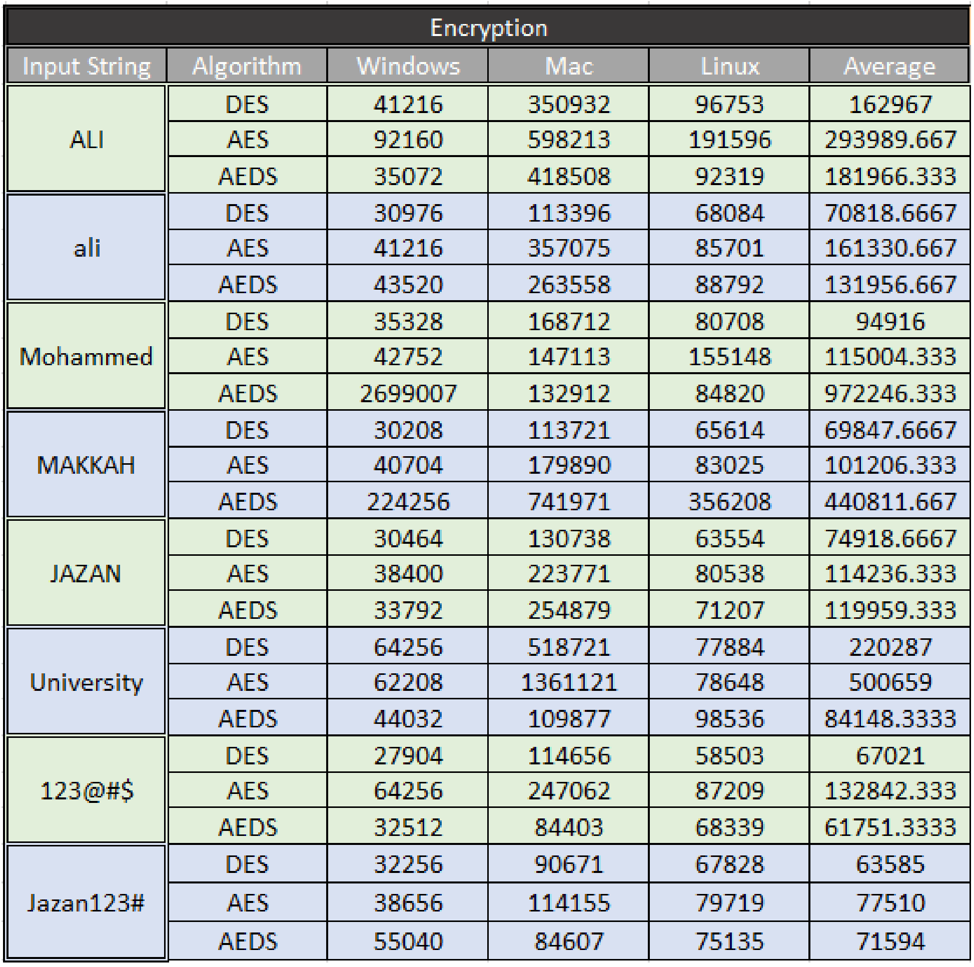
Below are few of the importance of research to society in Cryptography field of Information security. Security of data is very important for most online businesses and even home computer users. Client information, online payment transactions, personal files, bank account details - all of this information can be hard to replace and potentially dangerous if it falls into the wrong hands. Data lost due to disasters such as a flood or fire is crushing, but loosing data in to wrong hands of hackers or a malware infection can have much dangerous impact on humankind and society. To prevent data loss and protecting information of user's cryptographic techniques are used.

IV. RESEARCH METHODOLOGY

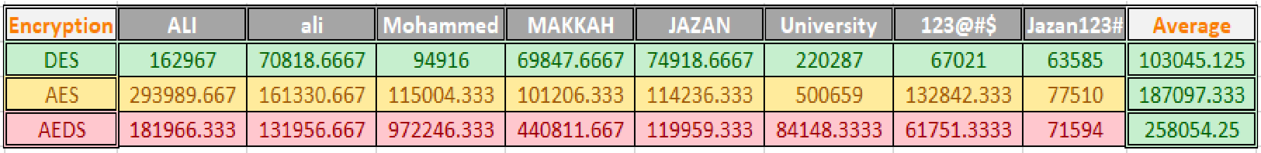
The experiment is performed on three different machines having three different operating systems (Linux, Mac OS X and Windows). We have taken different strings and files as plaintext. Then after executing our algorithms we got different cipher texts. Now we collected encryption time and decryption time of each plaintext from different operating systems. Based on decryption time we decided which algorithm is stronger.

Results:

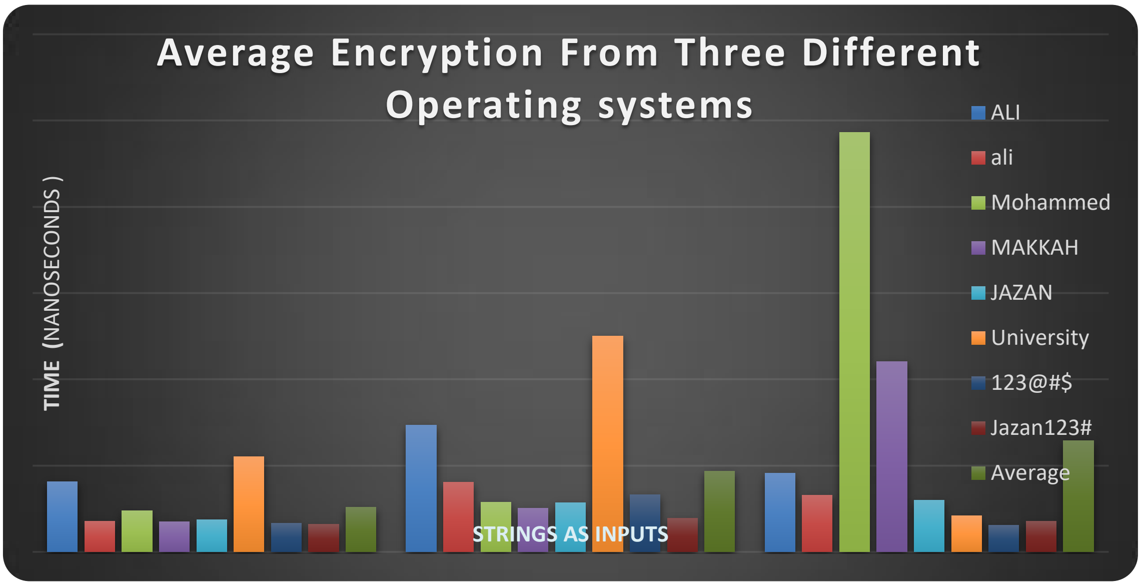
Encryption time are shown in the following Tables, When we are taking String(as Plaintext):



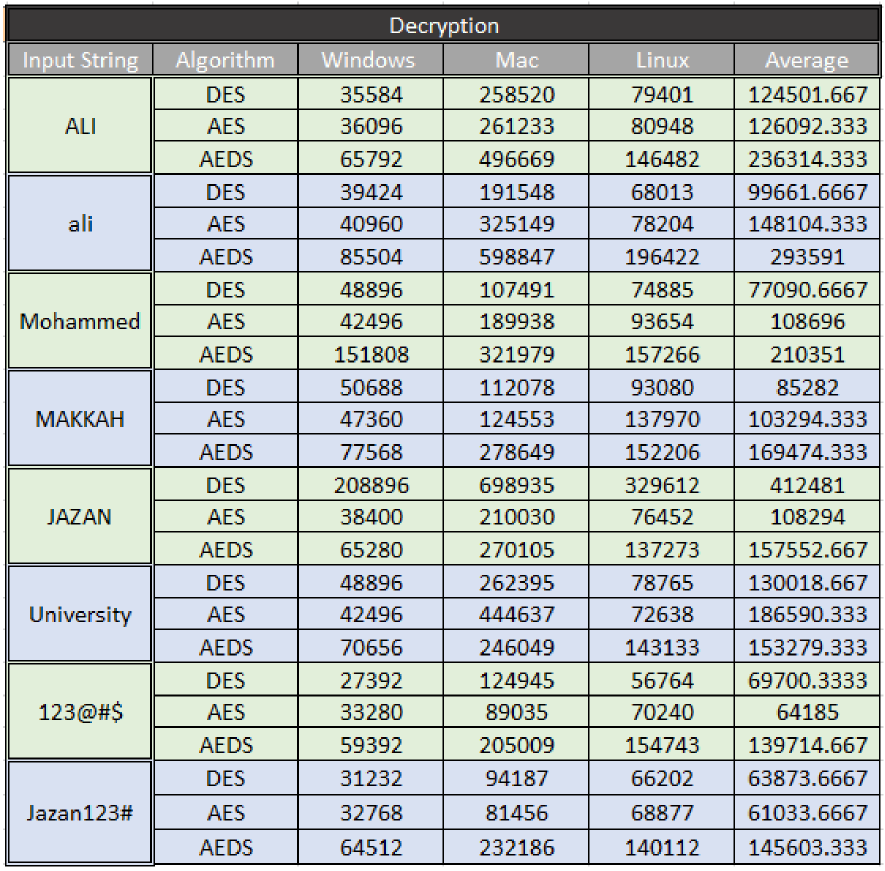
Encryption					
Input String	Algorithm	Windows	Mac	Linux	Average
ALI	DES	41216	350932	96753	162967
	AES	92160	598213	191596	293989.667
	AEDS	35072	418508	92319	181966.333
ali	DES	30976	113396	68084	70818.6667
	AES	41216	357075	85701	161330.667
	AEDS	43520	263558	88792	131956.667
Mohammed	DES	35328	168712	80708	94916
	AES	42752	147113	155148	115004.333
	AEDS	2699007	132912	84820	972246.333
MAKKAH	DES	30208	113721	65614	69847.6667
	AES	40704	179890	83025	101206.333
	AEDS	224256	741971	356208	440811.667
JAZAN	DES	30464	130738	63554	74918.6667
	AES	38400	223771	80538	114236.333
	AEDS	33792	254879	71207	119959.333
University	DES	64256	518721	77884	220287
	AES	62208	1361121	78648	500659
	AEDS	44032	109877	98536	84148.3333
123@#$	DES	27904	114656	58503	67021
	AES	64256	247062	87209	132842.333
	AEDS	32512	84403	68339	61751.3333
Jazan123#	DES	32256	90671	67828	63585
	AES	38656	114155	79719	77510
	AEDS	55040	84607	75135	71594



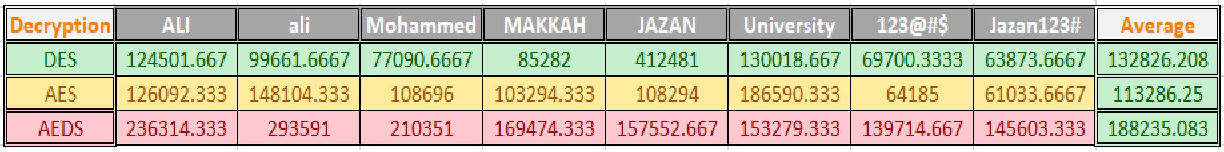
Encryption	ALI	ali	Mohammed	MAKKAH	JAZAN	University	123@#$	Jazan123#	Average
DES	162967	70818.6667	94916	69847.6667	74918.6667	220287	67021	63585	103045.125
AES	293989.667	161330.667	115004.333	101206.333	114236.333	500659	132842.333	77510	187097.333
AEDS	181966.333	131956.667	972246.333	440811.667	119959.333	84148.3333	61751.3333	71594	258054.25



Decryption time are shown in the following Tables, When we are taking String(as Plaintext):

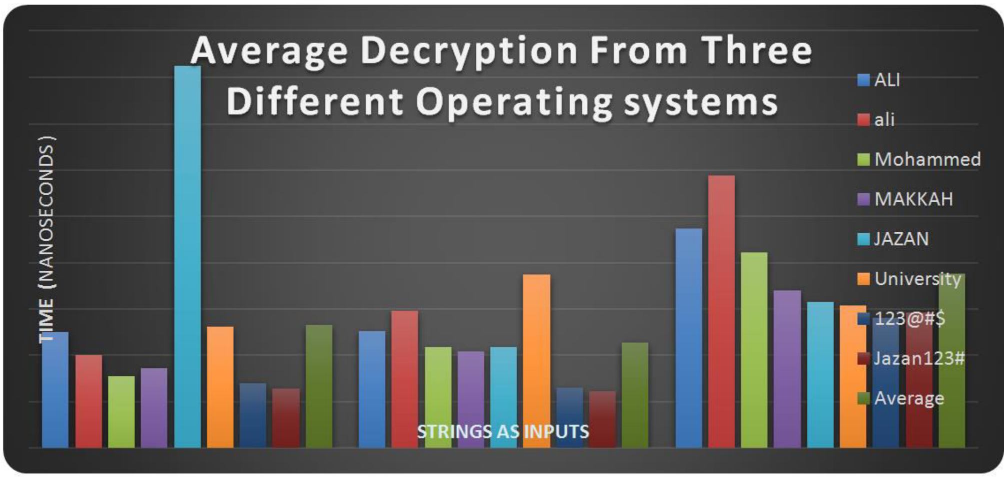


Decryption					
Input String	Algorithm	Windows	Mac	Linux	Average
ALI	DES	35584	258520	79401	124501.667
	AES	36096	261233	80948	126092.333
	AEDS	65792	496669	146482	236314.333
ali	DES	39424	191548	68013	99661.6667
	AES	40960	325149	78204	148104.333
	AEDS	85504	598847	196422	293591
Mohammed	DES	48896	107491	74885	77090.6667
	AES	42496	189938	93654	108696
	AEDS	151808	321979	157266	210351
MAKKAH	DES	50688	112078	93080	85282
	AES	47360	124553	137970	103294.333
	AEDS	77568	278649	152206	169474.333
JAZAN	DES	208896	698935	329612	412481
	AES	38400	210030	76452	108294
	AEDS	65280	270105	137273	157552.667
University	DES	48896	262395	78765	130018.667
	AES	42496	444637	72638	186590.333
	AEDS	70656	246049	143133	153279.333
123@#$	DES	27392	124945	56764	69700.3333
	AES	33280	89035	70240	64185
	AEDS	59392	205009	154743	139714.667
Jazan123#	DES	31232	94187	66202	63873.6667
	AES	32768	81456	68877	61033.6667
	AEDS	64512	232186	140112	145603.333



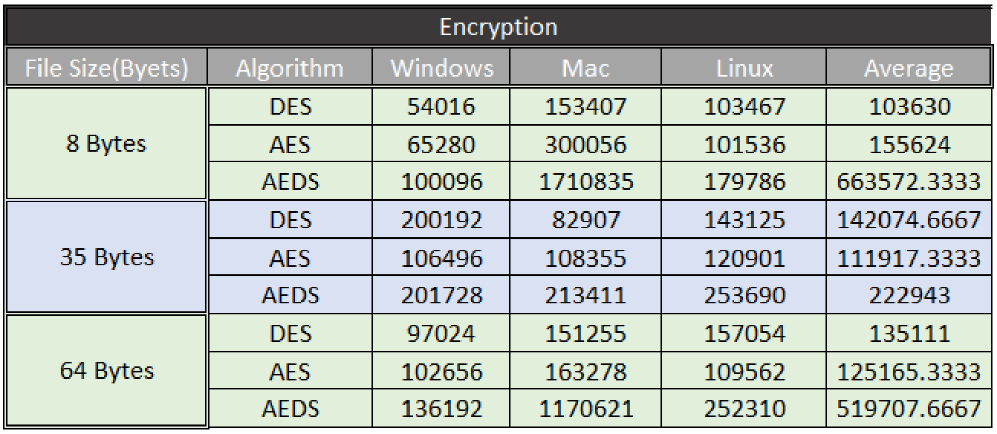
Decryption	ALI	ali	Mohammed	MAKKAH	JAZAN	University	123@#$	Jazan123#	Average
DES	124501.667	99661.6667	77090.6667	85282	412481	130018.667	69700.3333	63873.6667	132826.208
AES	126092.333	148104.333	108696	103294.333	108294	186590.333	64185	61033.6667	113286.25
AEDS	236314.333	293591	210351	169474.333	157552.667	153279.333	139714.667	145603.333	188235.083

DOI 10.17148/IARJSET.2019.61001

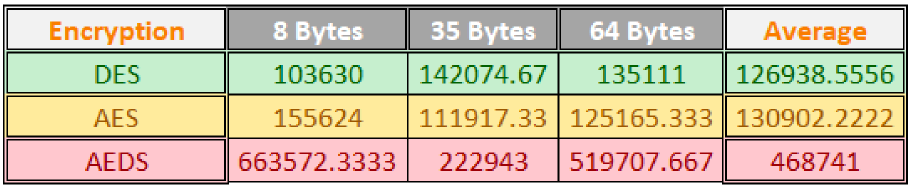


When we are taking Different size of Files (as Plaintext)

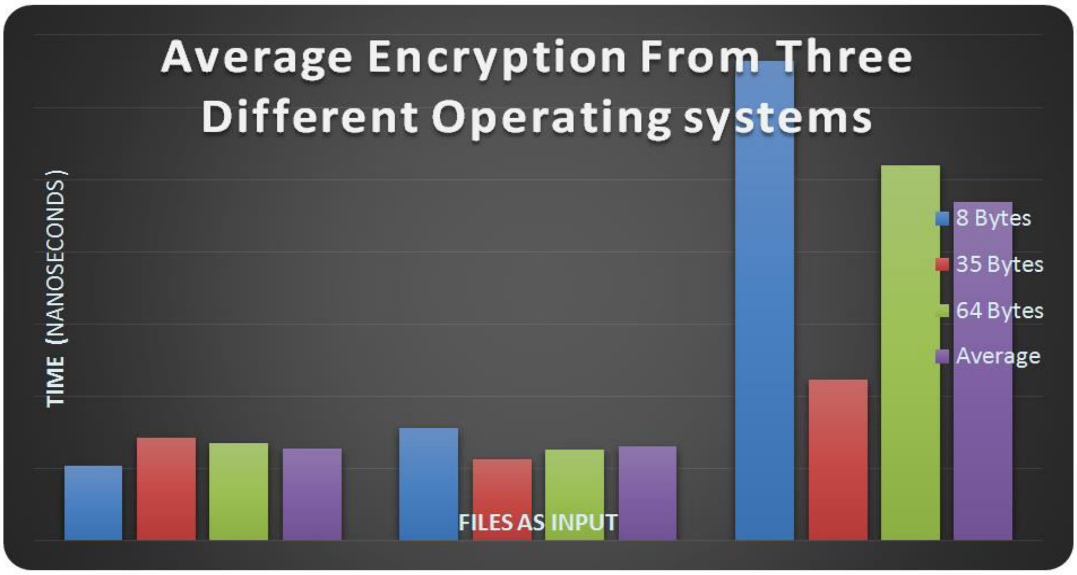
Encryption time are shown in the following Tables, When we are taking Different size of Files (as Plaintext):



Encryption					
File Size(Byets)	Algorithm	Windows	Mac	Linux	Average
8 Bytes	DES	54016	153407	103467	103630
	AES	65280	300056	101536	155624
	AEDS	100096	1710835	179786	663572.3333
35 Bytes	DES	200192	82907	143125	142074.6667
	AES	106496	108355	120901	111917.3333
	AEDS	201728	213411	253690	222943
64 Bytes	DES	97024	151255	157054	135111
	AES	102656	163278	109562	125165.3333
	AEDS	136192	1170621	252310	519707.6667

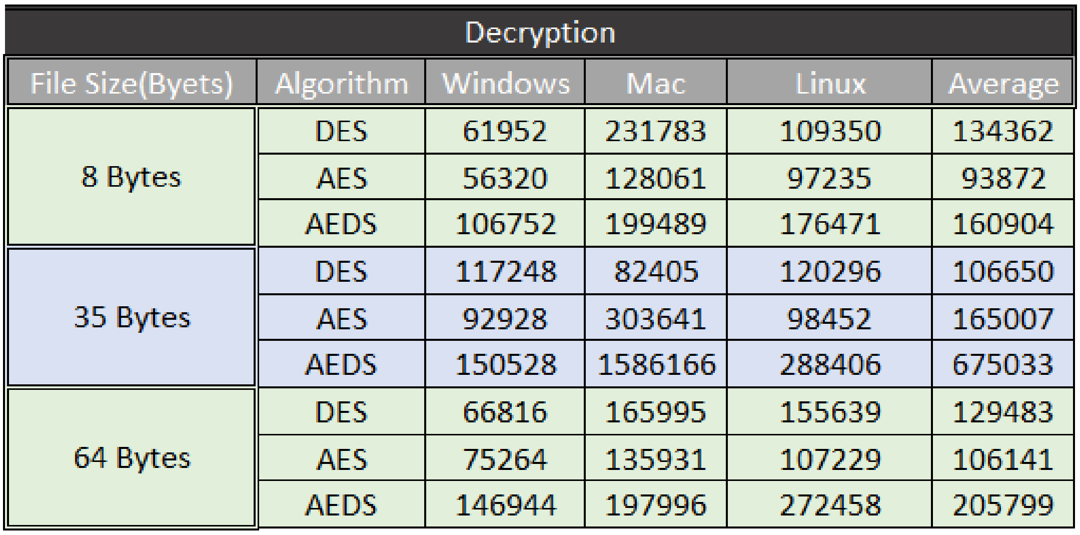


Encryption	8 Bytes	35 Bytes	64 Bytes	Average
DES	103630	142074.67	135111	126938.5556
AES	155624	111917.33	125165.333	130902.2222
AEDS	663572.3333	222943	519707.667	468741

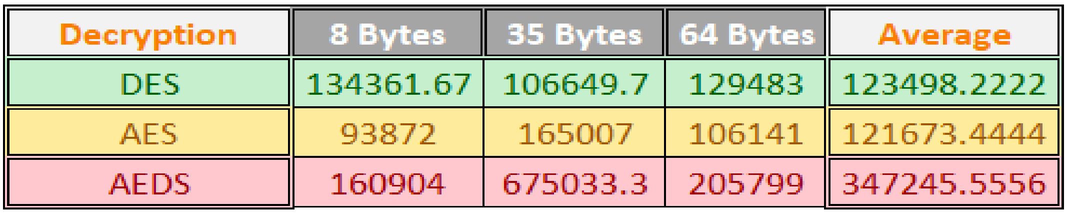


DOI 10.17148/IARJSET.2019.61001

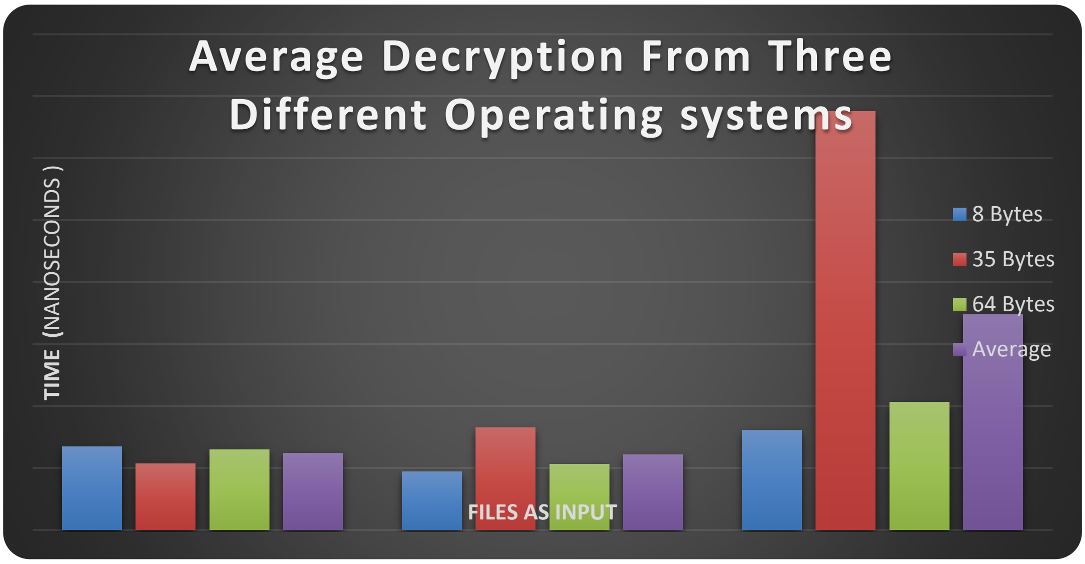
Decryption time are shown in the following Tables, When we are taking Different size of Files (as Plaintext):



Decryption					
File Size(Byets)	Algorithm	Windows	Mac	Linux	Average
8 Bytes	DES	61952	231783	109350	134362
	AES	56320	128061	97235	93872
	AEDS	106752	199489	176471	160904
35 Bytes	DES	117248	82405	120296	106650
	AES	92928	303641	98452	165007
	AEDS	150528	1586166	288406	675033
64 Bytes	DES	66816	165995	155639	129483
	AES	75264	135931	107229	106141
	AEDS	146944	197996	272458	205799



Decryption	8 Bytes	35 Bytes	64 Bytes	Average
DES	134361.67	106649.7	129483	123498.2222
AES	93872	165007	106141	121673.4444
AEDS	160904	675033.3	205799	347245.5556



V. CONCLUSION

Here we combined the concept of DES and AES Algorithms and developed a new algorithm AEDS. We tested different inputs like strings and files on theses algorithms (AES, DES and AEDS) on three different Machines. We have derived new Algorithm AEDS for data security and found it more robust and secure. Our AEDS Algorithm is best option over two individual Algorithms as it over comes the drawbacks of each. Brute force attack is nearly reduced by great extent as compare to rest two algorithms. Also, the time shown on the analysis (Fig.2 and Fig.3) are average time because the time may vary depend upon the processor availability and processor speed. Encryption and Decryption time for AEDS is more than that of individuals as it uses the feistel structure incorporated with DES and AES. The proposed AEDS Algorithm performs better.

DOI 10.17148/IARJSET.2019.61001

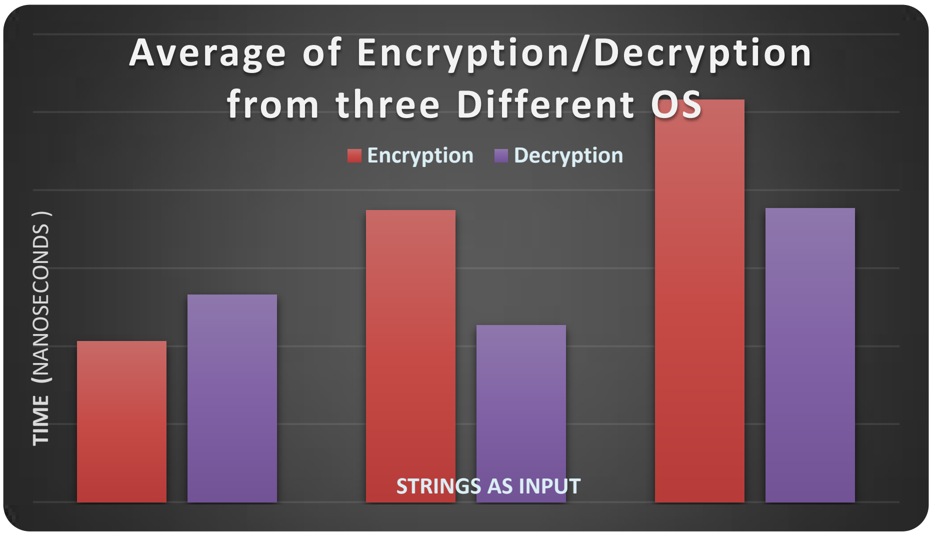


Fig.2

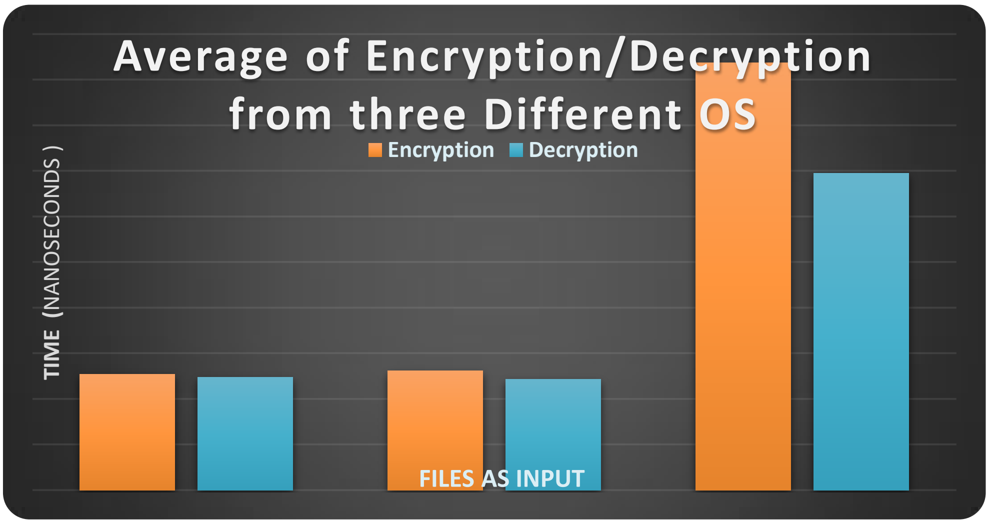


Fig.3

ACKNOWLEDGMENT

We would like to thank College of Computer Science & Information Technology and deanship of scientific Research, Jazan University, Jazan, KSA for their support and encouragement. The author would like to thank to all authors that are listed below in the reference lists as well as anonymous reviewers for their valuable comments and suggestions that improved the presentation of this paper.

REFERENCES

[1]. Shashi Mehrotra Seth, Rajan Mishra "Comparative Analysis of Encryption Algorithms For Data Communication" IJCST Vol. 2, Issue 2, June 2011 I S N: 2 9 - 4 3 (Print) | I S S N: 0 9 7 6 - 8 4 9 1 (Online) www. i j c s t. c o m

[2]. DiaasalamaAbdElminaam, HatemMohamadAbdualKader,Mohly Mohamed Hadhoud, ―Evolution The Performance of Symmetric Encryption Algorithms‖, international journal of network Security, vol.10,No.3,pp,216-222,May 2010

[3]. 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

[4]. B. Padmavathi1, S. Ranjitha Kumari2 ―A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique‖ International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064Volume 2 Issue 4, April 2013 www.ijsr.net

[5]. 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