Performance Evaluation of Different Cryptographic Algorithms: DES, 3DES, AES,IDEA & BLOWFISH

Md Imran Alam[1], Mohammad Rafeek Khan[2]

Department of Computer Engineering & Networks, Jazan University, Jazan
Saudi Arabia
imran.amu2008@gmail.com,rafeek04@gmail.com

***Abstract*— In recent years Data Security has emerged as a topic of significant interest in both academic and industry fields. For secure data transmission over unsecure network like Internet or any public networks there is no alternative to Cryptography. Cryptography means to transfer sensitive information across insecure networks like internet so that it cannot be read by anyone except the person whom we want to send it. Cryptographic Algorithms play very important role in security of data. In this paper we evaluate performance of different Cryptographic algorithms like DES, 3DES, AES, IDEA and BLOWFISH. Cryptographic algorithms have been compared based on the following factors: input size of data (in the form of text, audio, video and images), encryption time, and decryption time, throughput of encryption and decryption of each algorithm. From Experimental results, we evaluated performances of these Cryptographic algorithms (DES, 3DES, AES, IDEA and BLOWFISH).**

***Keywords*—Security, Cryptography, Algorithm, DES, 3DES, AES, IDEA, BLOWFISH, Throughput**

I. INTRODUCTION

The art and science of keeping messages secure is cryptography, and it is practiced by cryptographers [17]. It basically hides the information.

Some basic terms used in Cryptography:

a. Plain Text: The original message which a person want to transfer is called plain text. For an example, Alice is a person who wants to transmit the message "Hello, How do you do?" to his friend Bob. Here the message "Hello, How do you do ? "is called plain text.

b. Cipher Text: The message which cannot be understood by anyone except the person whom we want to send the message is called as cipher text. For an example "Khoor, Krz gr brx gr @" is a cipher text for the plain text message "Hello, How do you do? "

c. Encryption: It is a technique which transforms the original data or message to some non readable format. This non readable data or message is called Cipher text.

d. Decryption :Converting cipher text back to plain text is called as decryption .

e. Key: Combination of alphabets, digits or special symbol is known as key .It may be used at a time of encryption or decryption .Key plays a vital role in cryptography because encryption algorithms directly depend on it.

Keys play a very important role in cryptography. Strength of a Cryptographic algorithm depends on the choice of keys. If we use small keys then encryption algorithm will be weak. Anyone can break it easily. To make Algorithm strong we use large and complex keys.
Cryptography algorithms are divided into two parts:

Symmetric and **Asymmetric** key cryptography.

Symmetric key Cryptography uses only key to encrypt and decrypt data. Symmetric algorithms are of two types: Block ciphers and Stream ciphers.

Block Cipher: A block cipher is a deterministic algorithm operating on fixed-length groups of bits, Called blocks, with an unvarying transformation that is specified by a symmetric key. [15]
Examples of Block Ciphers are: DES, 3DES, CAST, BLOWFISH, IDEA and RC2.

Stream ciphers: A stream cipher is a method of encrypting text (to produce cipher text) in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time.[9] RC4 is an example of stream cipher algorithm.

In **Asymmetric key Cryptography,** two keys are used; private keys and public keys. Public key is used for encryption and private key is used for decryption. Public key is known to the public and private key is known only to the user. Examples of Asymmetric cryptographic algorithms are: RSA,Diffie-Hellman, and DSA.

Cryptography Classification is shown in Fig.1

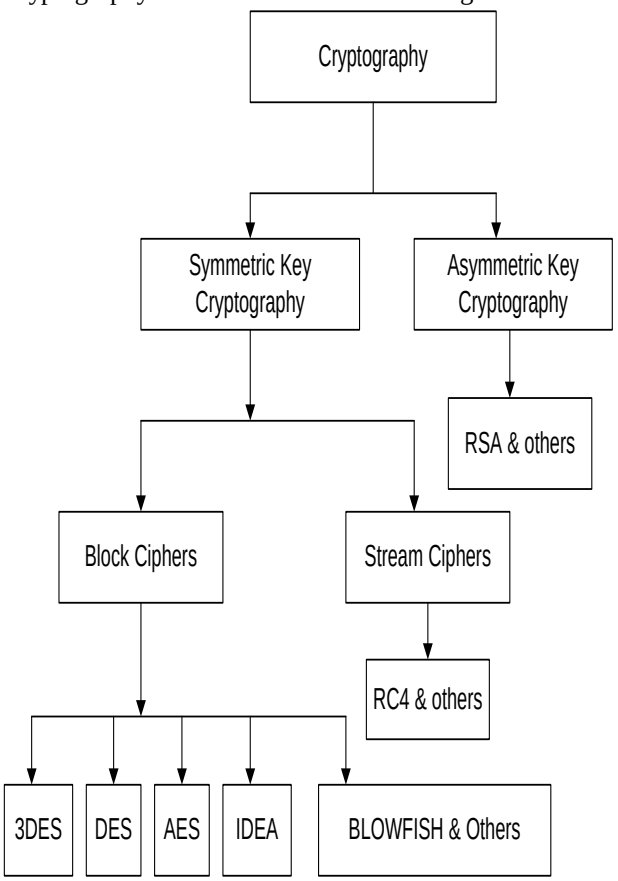

Fig.1 Classifications of Cryptography

This paper is organized as follows: In section I Introduction part of cryptography is discussed. Section II covers the literature reviews. In section III the different types of Encryption algorithms are discussed. In section IV the various performance factors for the algorithms are given. In section V the results and the discussions are presented. With the section VI the final conclusion of paper is provided.

II. LITERATURE REVIEW

In this section various performance factors and Encryption techniques used by different papers are discussed.

In paper[3] it is discussed that Encryption algorithm play an important role in communication security where encryption time, Memory usages output byte and battery power are the major issue of concern. The selected encryption AES, DES and RSA algorithms are used for performance evaluation. Based on the text files used and the experimental result it was 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.

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.

In paper[6] it was concluded that In Data communication, encryption algorithm plays an important role . Our research work 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.

Paper[7] presents a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are AES, DES, 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.

Paper[8] presents the superiority of Blowfish algorithm with others in terms of the throughput, processing time and power consumption. More the throughput, more the speed of the algorithm & less will be the power consumption. Secondly, AES has advantage over the other 3DES and DES in terms of throughput & decryption time. Third point is that 3DES has the least performance among all the algorithms mentioned here. Finally we can conclude that Blowfish is the best of all. In future we can perform same experiments on image, audio & video and developing a stronger encryption algorithm with high speed and minimum energy consumption 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.

Paper[11] presents comparative analysis of existing Encryption algorithms like DES, 3DES, AES, RSA and BLOWFISH. By analyzing experimental results it was concluded that BLOWFISH algorithm takes least encryption and decryption time as compared to DES, 3DES, AES and RSA algorithms. Throughput value of BLOWFISH is the highest as compared to DES, 3DES, AES and RSA algorithms. Power consumption value of AES is higher than BLOWFISH but lesser than DES, 3DES and RSA algorithms.

III.CLASSIFICATION OF CRYPTOGRAPHIC ALGORITHMS

A. **DES (Data Encryption Standard)** is the most popular computer encryption algorithm. DES is a U.S. and international standard. It is a symmetric algorithm; the same key is used for encryption and decryption. "Reference[5] shows" Digital Encryption Standard (DES) is a symmetric block cipher with 64-bit block size that uses using a 56-bit. DES encrypts and decrypts data in 64-bit blocks, using a 56-bit key. It takes a 64-bit block of plaintext as input and outputs a 64-bit block of cipher text. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm. DES has 16 rounds, meaning the main algorithm is repeated 16 times to produce the cipher text. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. So as the number of rounds increases, the security of the algorithm increases exponentially. DES was clearly no longer invulnerable to the attacks.

B. **3DES:** In cryptography, Triple DES is the common name for the Triple Data Encryption algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm. The encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. 3DES is slower than other block cipher methods. [8]

C. **AES:** The Advanced Encryption Standard (AES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in December 2001. The Advanced Encryption Standard (AES) was designed because DES's key was too small.[2] Although Triple DES ODES) increased the key size, the process was too slow. The National Institute of Standards and Technology (NIST) chose the Rijndael algorithm, named after its two Belgian inventors, Vincent Rijmen and Joan Daemen, as the basis of AES. AES is a very complex round cipher. AES is designed with three key sizes: 128, 192, or 256 bits. Below Table shows the relationship between the data block[2]

Size of Data Block	*Number of Rounds*	*Key Size*
128 bits	10	128 bits
	12	192 bits
	14	256 bits

D. **Blowfish:** Blowfish is a keyed, symmetric block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products.

- Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. [1]
- Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms.
- It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use.
- It is a 16 round fiestel cipher that uses the large key size. Since the key size is larger it is complex to break the code in the blowfish algorithm. Moreover it is vulnerable to all the attacks except the weak key class attack.[5]

E. . IDEA(International Data Encryption Algorithm): IDEA is a block cipher; it operates on 64-bit plaintext blocks. The key is 128 bits long. The same algorithm is used for both encryption and decryption. As with all the other block ciphers we've seen, IDEA uses both confusion and diffusion. The design philosophy behind the algorithm is one of "mixing operations from different algebraic groups." [1]
Three algebraic groups are being mixed, and they are all easily implemented in both hardware and software:
— XOR
— Addition modulo 216
— Multiplication modulo 216 + 1. (This operation can be viewed as IDEA's S-box.)
All these operations (and these are the only operations in the algorithm—there are no bit-level permutations) operate on 16-bit sub-blocks. This algorithm is even efficient on 16-bit processors.

IV. PERFORMANCE FACTORS

For our experiment, we used a laptop with i5, 2.53 GHz CPU and 4 GB RAM. We used the Microsoft Visual Studio .Net and Compact Framework as the software development environment. Code of block Ciphers algorithms was written using C# language. In the experiment, the laptop encrypts a different file size ranges from 55 KB to 11150 KB.

In this paper, the following factors are used as the performance criteria:

i. Input data (in the form of text, audio , video & images)
ii. Encryption Time of each algorithm
iii. Decryption Time of each algorithm
iv. Throughput of Encryption of different algorithms with text, audio video & images data
v. Throughput of Decryption of different algorithms with text, audio, video & images data

Encryption time: The time which an algorithm takes to convert plain text to a cipher text is called encryption time.

Decryption time: The time which an algorithm takes to get plain text from a cipher text is called decryption time.

Throughput of an encryption: It is defined as total plain text in Megabytes divided by total encryption time of each algorithm.

Throughput of a decryption: It is defined as total plain text in Megabytes divided by total decryption time of each algorithm.

If throughput value of an encryption is increased then power consumption of that encryption is decreased.

Similarly if throughput of an encryption is decreased then power consumption of that encryption is increased and hence the battery consumption is also increased.

V. **EXPERIMENTAL RESULTS & ANALYSIS**

Experimental results for Encryption algorithms DES, 3DES, AES, BLOWFISH and IDEA are shown in Table1 and Table 2.

Table 1: Comparisons of 3DES, DES, AES, BLOWFISH and IDEA based on Encryption Time

Input Size (KB)	3DES	DES	AES	BLOW -FISH	IDEA
55	121	41	49	15	51
251	171	55	56	30	72
560	232	78	72	65	98
920	381	125	105	72	141
5611	1240	385	372	290	650
11150	2699	950	921	590	1081
Throughput (MB/Sec)	3.82	11.35	11.77	19.74	8.86

Table 2: Comparisons of 3DES, DES, AES, BLOWFISH and IDEA based on Decryption Time

Input Size (KB)	3DES	DES	AES	BLOW -FISH	IDEA
55	105	34	51	14	52
251	162	53	48	35	68
560	211	81	65	71	85
920	361	116	98	81	119
5611	1195	345	361	298	631
11150	2701	960	905	621	1051
Throughput (MB/Sec)	3.91	11.67	12.13	16.55	9.24

Table 1 shows the encryption time of different algorithms based on input data of different sizes. In this table encryption throughput of different algorithms is also calculated.

Table 2 shows the decryption time of different algorithms based on input data of different sizes.
In this table decryption throughput of different algorithm is calculated.

After analyzing Table1 and Table 2, it is concluded that encryption and decryption time of 3DES algorithm is much higher than encryption and decryption time of AES, DES, IDEA and BLOWFISH algorithm. We also noticed here that encryption and decryption time of BLOWFISH algorithm is the lowest as compared to AES, DES, 3DES and IDEA.

Similarly by using the same sizes of Input data in the form of Audio, Video and images we have calculated the Encryption & Decryption Throughput of Audio , video and images data respectively. This throughput is shown in Table3.

Table3: It shows Encryption**(Enc)** and Decryption**(Dec)** Throughput of the data in the form of (Audio ,Video and Image).

Throughput (MB/Sec)	Audio		Video		Image	
	Enc	Dec	Enc	Dec	Enc	Dec
3DES	3.81	3.93	3.85	3.94	3.78	3.84
DES	11.32	11.65	11.37	11.68	11.28	11.62
AES	11.75	12.14	11.81	12.11	11.71	12.05
BLOWFISH	19.71	16.65	19.78	16.87	19.62	16.34
IDEA	8.84	9.21	8.87	9.26	8.76	9.15

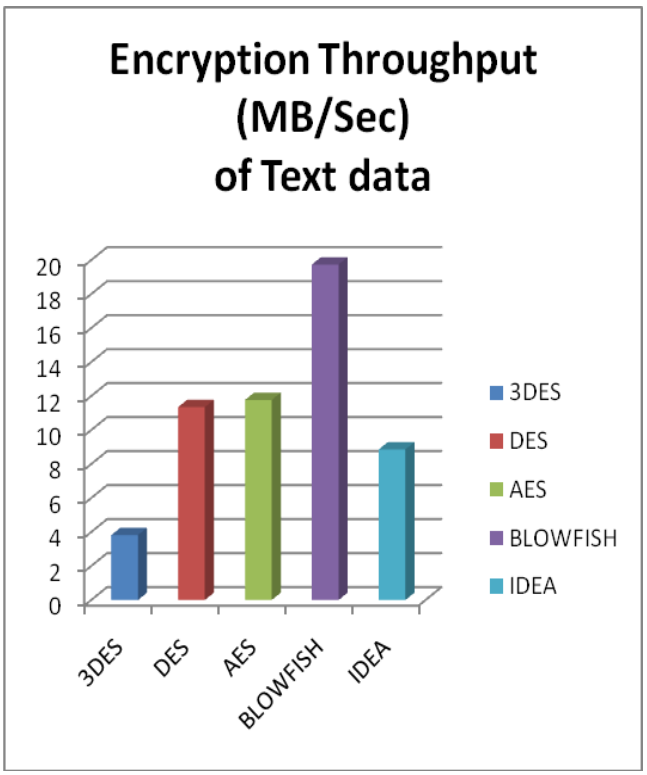

Fig. 2 Encryption Throughput of each Algorithm with Input as Text data

After analyzing Fig 2 we conclude that throughput of BLOWFISH algorithm is higher than throughput of all other algorithms like 3DES, DES, AES and IDEA. It is also noticed here that AES algorithm has advantage over DES, 3DES and IDEA algorithm in terms of the processing time.

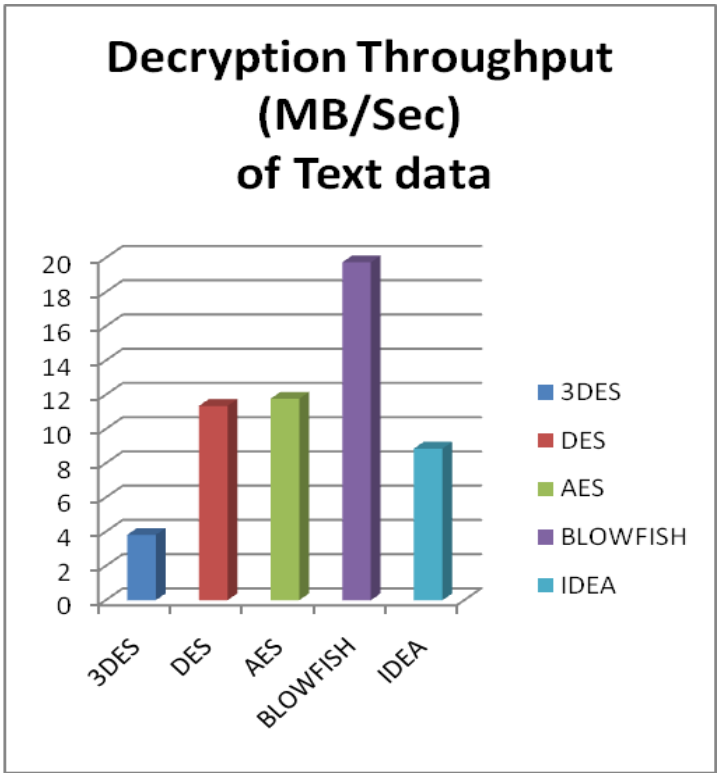

Fig. 3 Decryption Throughput of each Algorithm with Input as Text data

By analyzing fig. 3, it is noticed here that BLOWFISH algorithm is far better than other algorithms (3DES, DES, AES and IDEA) based on throughput value. It is also noticed that DES is better than 3DES. Throughput value of AES is higher than DES, 3DES and IDEA algorithm but lesser than BLOWFISH algorithm.

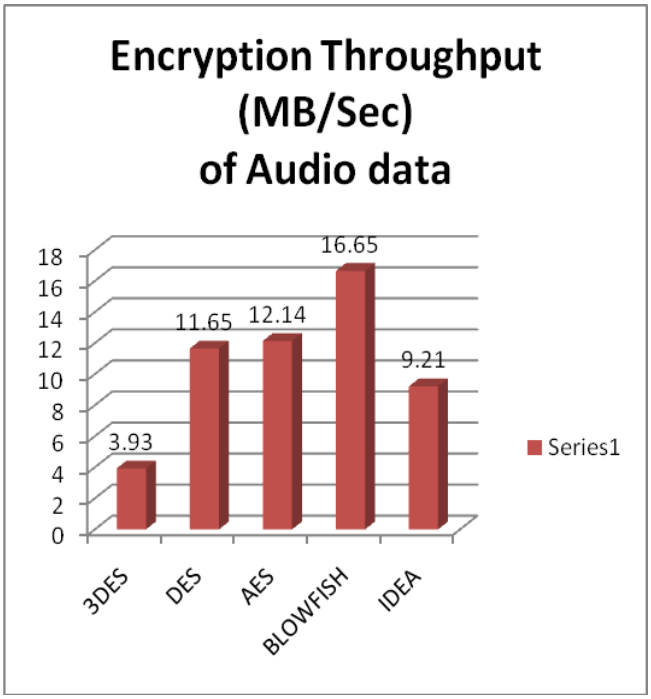

Fig. 4 Encryption Throughput of each Algorithm with Input as Audio data

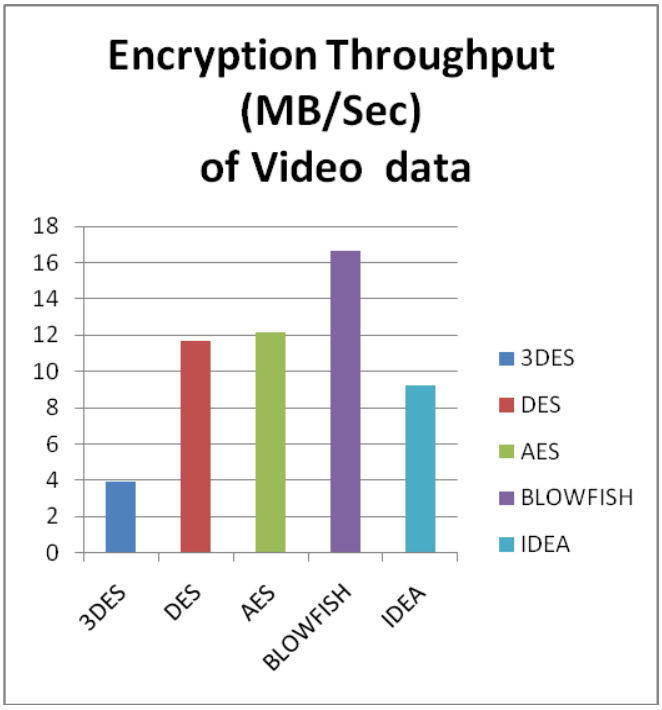

Fig. 6 Encryption Throughput of each Algorithm with Input as Video data

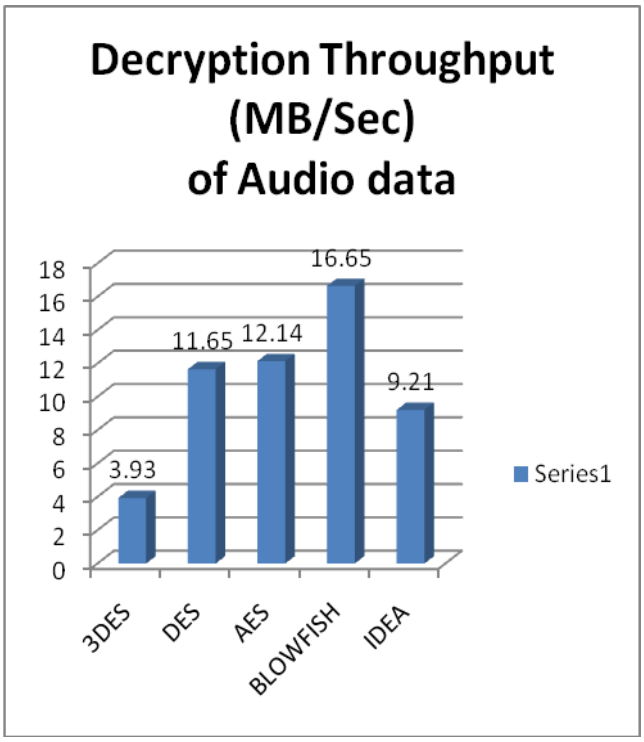

Fig. 5 Decryption Throughput of each Algorithm with Input as Audio data

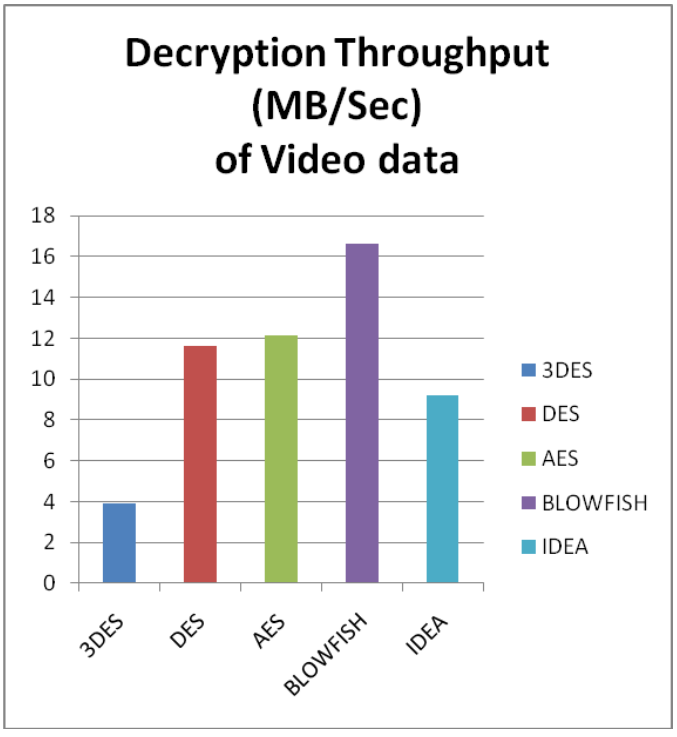

Fig.7 Decryption Throughput of each Algorithm with Input as Video data

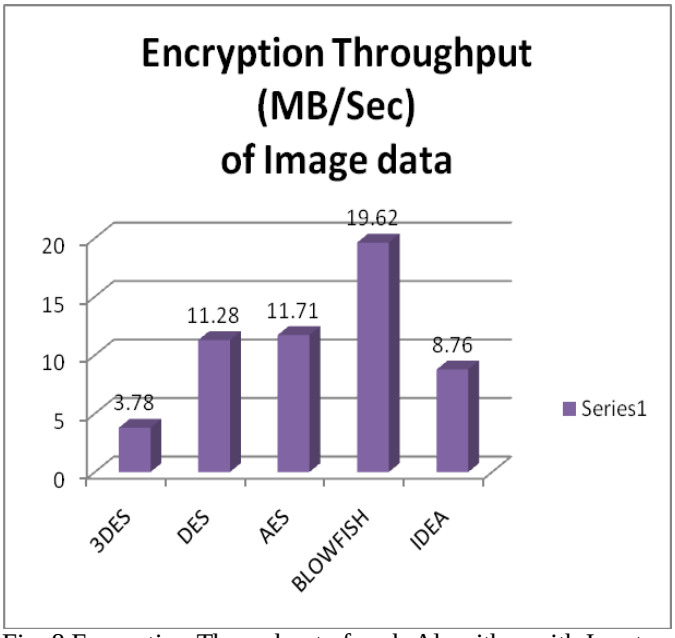

Fig. 8 Encryption Throughput of each Algorithm with Input as Image data

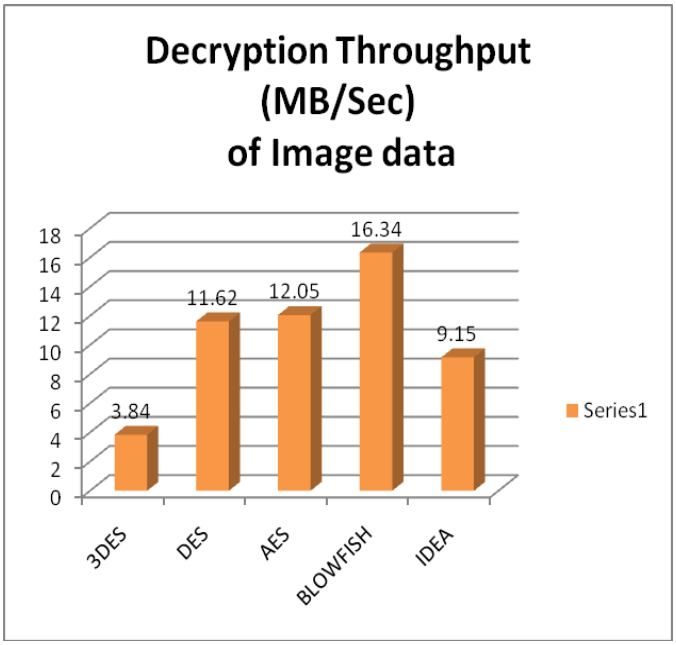

Fig.9 Decryption Throughput of each Algorithm with Input as Image data

By analyzing Fig. 4,5,6,7,8 and 9,Encryption Throughput and Decryption Throughput of each algorithm with Input data as audio, video and image is almost same.
Encryyption/decryption Throughput of each algorithm with input data as Image is slightly lesser than Throughput of each of these algorithms with input data as text, audio and video.

VI. Conclusions

This paper evaluates the performance of existing Cryptographic algorithms like DES, 3DES, AES, IDEA and BLOWFISH. By analyzing experimental results several points can be concluded. Throughput of AES is better than throughput of DES, 3DES and IDEA but lesser than BLOWFISH. Encryption and Decryption Throughput of DES is almost 3 times more than 3DES algorithms because of its triple phase characteristics. BLOWFISH algorithm takes least encryption and decryption time as compared to DES, 3DES, AES and IDEA. Throughput value of BLOWFISH is the highest as compared to DES, 3DES, AES and IDEA .Throughput of IDEA is better than 3DES but lesser than all other algorithms discussed in his paper. When we take input data of different sizes in the form of Text,Audio,Video and Image, we conclude that Throughput of each of these algorithms is almost same in all the above four forms of data.

From the experimental results, we finally conclude that 3DES has least performance efficiency as compared to DES,AES,IDEA & BLOWFISH algorithm. We also conclude that performance of BLOWFISH algorithm is best as compared to all other algorithms discussed in this paper.

Acknowledgment

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] Bruce Schneier ”Applied Cryptography, Protocols, Algorithms and Source Code in C”.

[2] Behrouz A. Forouzan “Data Communications and Networking ”

[3] Shasi Mehlrotra seth, Rajan Mishra “ Comparative Analysis of Encryption Algorithms For Data Communication”, IJCST Vol. 2, Issue 2, June 2011

[4] Ali Makhmali, Hajar Mat Jani” Comparative Study On Encryption Algorithms And Proposing A Data Management Structure”INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 6, JUNE 2013 ISSN 2277-8616

[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

[6] 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

[7] DiaasalamaAbdElminaam, HatemMohamadAbdual Kader,Mohly Mohamed Hadhoud, "Evalution the Performance of Symmetric Encryption Algorithms", international journal of network security vol.10,No.3,pp,216-222,May 2010.

[8] Pratap Chnadra Mandal' Superiority of Blowfish Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering 2(9), September - 2012, pp. 196-201

[9] . http://en.wikipedia.org/wiki/Stream_cipher

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

[11] Md Imran Alam" A Comparative Analysis of Different Encryption Techniques of Cryptography" International Journal of Advanced and Innovative Research (2278-7844) / # 160 / Volume 2 Issue 9

[12] B.Persis Urbana Ivy, Purshotam Mandiwa. Mukesh Kumar "A modified RSA cryptosystem based on 'n' prime numbers" International Journal of Engineering and Computer Science ISSN:2319-7242 Volume1 Issue 2 Nov 2012 Page No. 63-66

[13] Ruangchaijatupon, P. Krishnamurthy, "Encryption and Power Consumption in Wireless LANs-N,'' The Third IEEE Workshop on Wireless LANs – September 27-28, 2001- Newton, Massachusetts.

[14] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength against Attacks."I BM Journal of Research and Development, May 1994,pp. 243 -250.

[15] Gurjeevan Singh, Ashwani Kumar, K. S. Sandha" A Study of New Trends in Blowfish Algorithm" / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 1, Issue 2, pp.321-326

[16] http://en.wikipedia.org/wiki/Block_cipher

[17] W. Stallings. Cryptography and Network Security, Prentice Hall, 1999.

