Performance Analysis of Different Cryptographic Algorithms of Block and Stream Ciphers

Md Imran Alam

Lecturer, Department of Computer Engineering & Networks, Jazan University, Jazan Saudi Arabia

imran.amu2008@gmail.com

***Abstract*— Nowadays plenty of data are transferred through unsecured networks like interent.Today we can't expect life without internet. Whether it is business communications or banking transactions, every where we need internet. Transferring such important data over internet causes the issue of security. Cryptography plays very important role in security of data. In this paper we will analyse performance of different Cryptographic algorithms of Block and Stream ciphers like DES, 3DES, AES, BLOWFISH and RC4.**

In this paper Cryptographic algorithms have been compared based on the following factors: input size of data (in the form of text, audio and video), 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, BLOWFISH and RC4).

***Keywords*—Security, Cryptography, Algorithm, DES, 3DES, AES, RC4, 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 terminology used in Cryptography[19]:

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.

Purpose of Cryptography:[8]

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data cryptography it is widely used today due to the great security advantages of it. Here are the various goals of cryptography.

Confidentiality: Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

Authentication: The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

Integrity: Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

Non Repudiation: Ensures that neither the sender, nor the receiver of message should be able to deny the transmission. **Access Control:** Only the authorized parties are able to access the given information.

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,AES, 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[19]

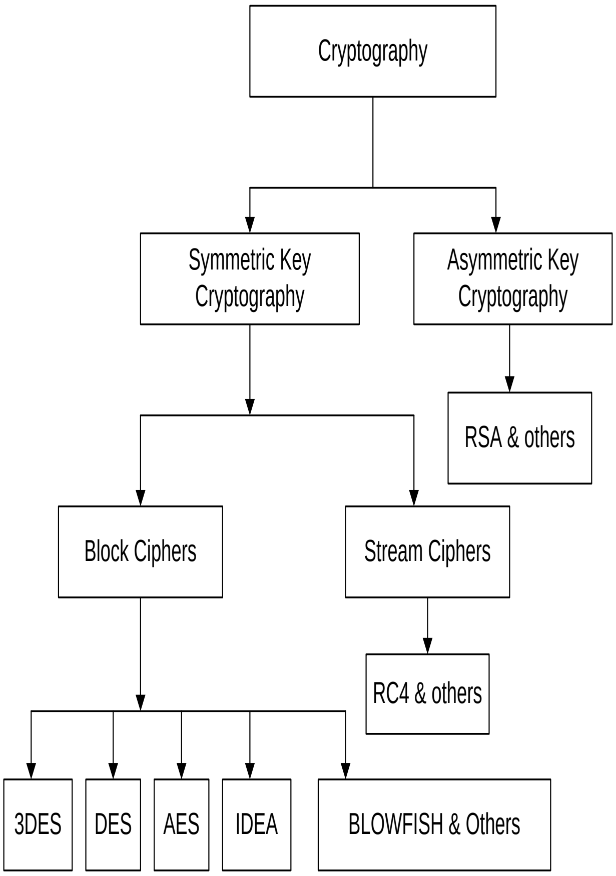


Fig.1 Classifications of Cryptography

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.

Paper[19]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.

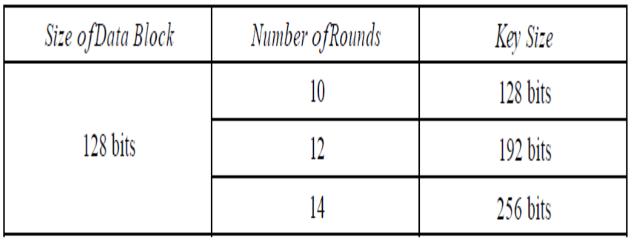
III.CLASSIFICATION OF CRYPTOGRAPHIC ALGORITHMS

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 ofData Block	Number ofRounds	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. RC4: RC4 is a variable-key-size stream cipher developed in 1987 by Ron Rivest for RSA Data Security, Inc. [1]

RC4 is simple to describe. The algorithm works in OFB: The keystream is independent of the plaintext. It has a 8 * 8 S-box: *S*0, *S*1,..., *S*255. The entries are a permutation of the numbers 0 through 255, and the permutation is a function of the variable-length key. It has two counters, *i* and *j*, initialized to zero.

To generate a random byte, do the following: [1]

```
i = (i + 1) mod 256
j = (j + Si) mod 256
swap Si and Sj
t = (Si + Sj) mod 256
K = St
```

The byte *K* is XORed with the plaintext to produce cipher text or XORed with the cipher text to produce plaintext. Encryption is fast—about 10 times faster than DES.

Initializing the S-box is also easy. First, fill it linearly: *S*0 = 0, *S*1 = 1,..., *S*255 = 255. Then fill another 256-byte array with the key, repeating the key as necessary to fill the entire array: *K*0, *K*1,..., *K*255.

Set the index *j* to zero. [1]

Then:

```
for i = 0 to 255:
j = (j + Si + Ki) mod 256
swap Si and Sj
```

RC4 is in dozens of commercial cryptography products, including Lotus Notes, Apple Computer’s AOCE, and Oracle Secure SQL.

IV. PERFORMANCE FACTORS

For our experiment, we used a laptop with i5, 2.53 GHz CPU and 3 GB RAM. We used the Microsoft Visual Studio .Net and Compact Framework as the software development environment. Code of block Ciphers and Stream Cipher algorithms was written using C# language. In the experiment, the laptop encrypts a different file size ranges from 60 KB to 11160 KB.

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

i. Input data (in the form of text, audio and video)
ii. Encryption Time of each algorithm
iii. Decryption Time of each algorithm
iv. Throughput of Encryption of different algorithms with text, audio and video data
v. Throughput of Decryption of different algorithms with text, audio and video 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, RC4,AES and BLOWFISH are shown in Table1 and Table 2.

Table 1:_Comparisons of DES, 3DES, RC4,AES and BLOWFISH based on Encryption Time

Input Size (KB)	DES	3DES	RC4	AES	BLOW -FISH
60	42	123	8	49	16
254	56	174	12	56	32
570	75	236	21	72	64
925	121	389	28	110	74
5615	387	1249	79	374	296
11160	955	2705	205	928	592
Throughput (MB/Sec)	11.36	3.81	52.64	11.69	17.30

Table 2: Comparisons of DES, 3DES, RC4,AES and BLOWFISH based on Decryption Time

Input Size (KB)	DES	3DES	RC4	AES	BLOW -FISH
60	35	107	6	52	14
254	58	169	13	47	36
570	83	217	21	66	73
925	119	357	25	97	82
5615	348	1197	71	364	299
11160	964	2708	194	907	624
Throughput (MB/Sec)	11.56	3.90	56.30	12.12	16.47

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, RC4 and BLOWFISH algorithm.

We also noticed here that encryption and decryption time of RC4 algorithm is the lowest as compared to AES, DES, 3DES and BLOWFISH.

Similarly by using the same sizes of Input data in the form of Audio and Video we have calculated the Encryption & Decryption Throughput of Audio and video 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 and Video).

Throughput (MB/Sec)	Audio		Video	
	ENC	DEC	ENC	DEC
3DES	3.79	3.89	3.78	3.88
DES	11.31	11.48	11.21	11.51
RC4	52.61	55.89	52.13	55.49
AES	11.61	12.05	11.55	11.99
BLOWFISH	17.26	16.42	17.23	16.41

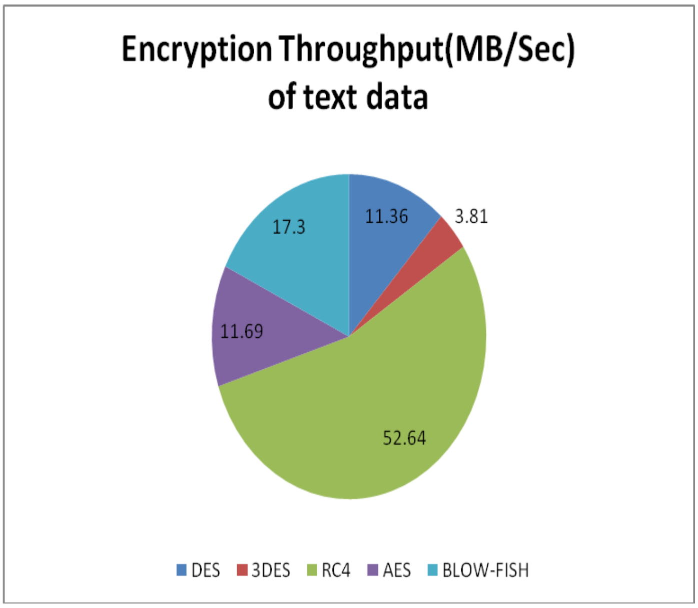


Fig. 2 Encryption Throughput of each Algorithm with Input as Text data

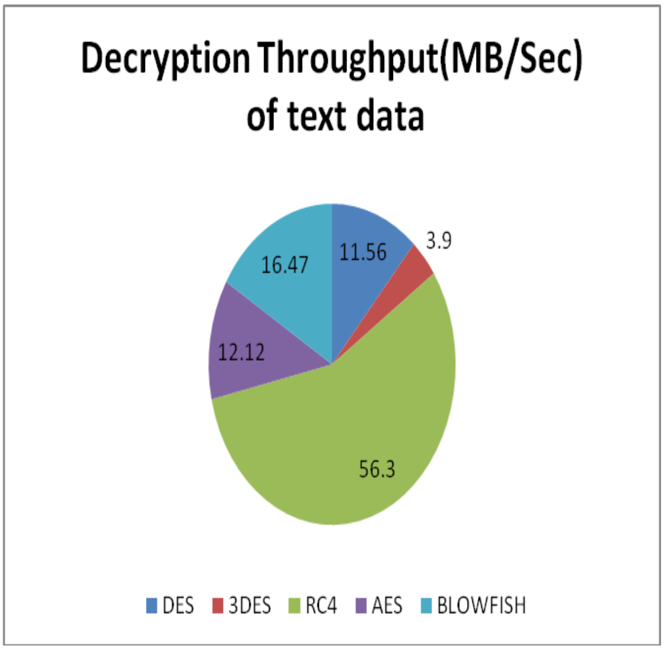


Fig. 3 Decryption Throughput of each Algorithm with Input as Text data

By analyzing fig. 3, it is noticed here that RC4 algorithm is far better than other algorithms (3DES, DES, AES and BLOWFISH) based on throughput value. It is also noticed that DES is better than 3DES. Throughput value of AES is higher than DES and 3DES algorithm but lesser than BLOWFISH and RC4 algorithm.

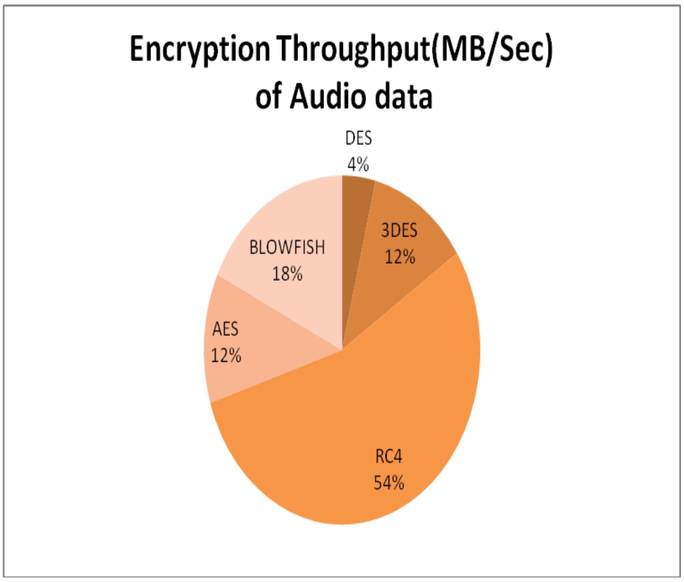


Fig. 4 Encryption Throughput of each Algorithm with Input as Audio data

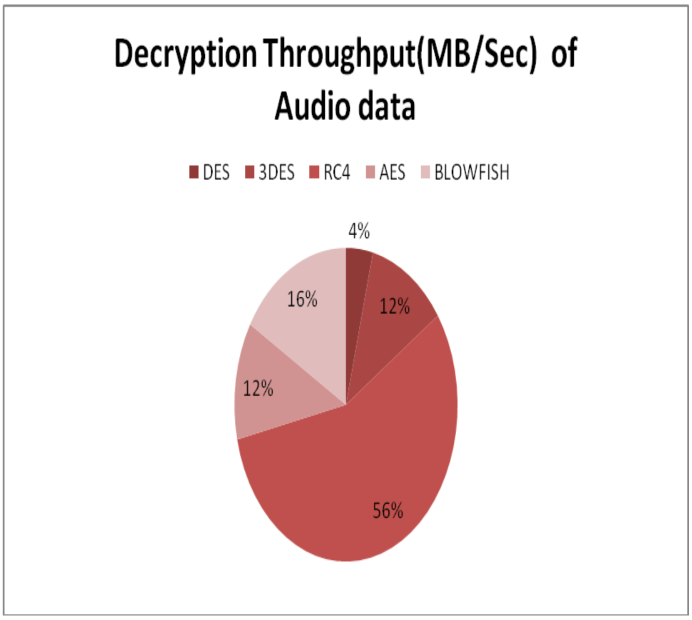


Fig. 5 Decryption Throughput of each Algorithm with Input as Audio data

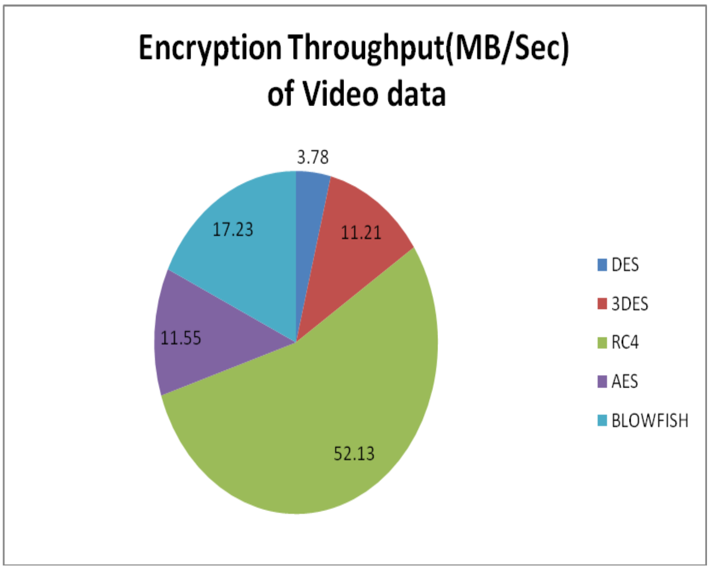


Fig. 6 Encryption Throughput of each Algorithm with Input as Video data

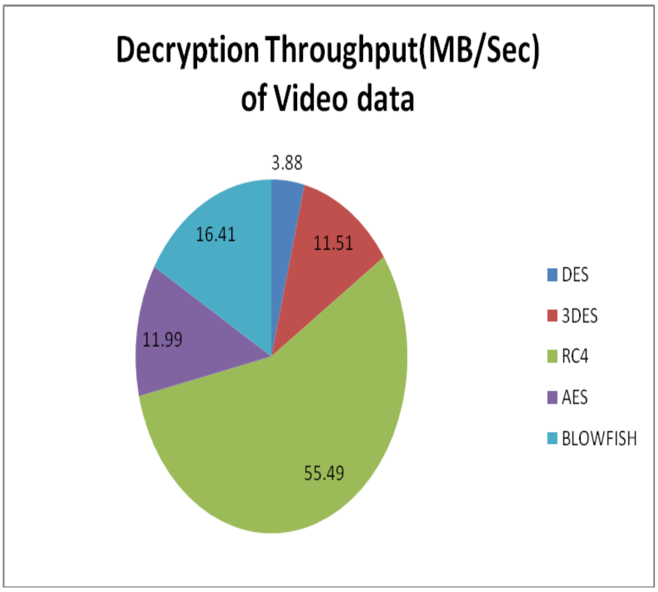


Fig.7 Decryption Throughput of each Algorithm with Input as Video data

By analyzing Fig. 4,5,6 and 7Encryption Throughput and Decryption Throughput of each algorithm with Input data as audio and video is almost same.

VI. Conclusions

This paper evaluates the performance of existing Cryptographic algorithms like DES, 3DES, AES, RC4 and BLOWFISH. By analyzing experimental results several points can be concluded. Throughput of AES is better than throughput of DES and 3DES but lesser than RC4 and BLOWFISH. Encryption and Decryption Throughput of DES is almost 3 times more than 3DES algorithms because of its triple phase characteristics. RC4 algorithm takes least encryption and decryption time as compared to DES, 3DES, AES and BLOWFISH. Throughput value of RC4 is the highest as compared to DES, 3DES, AES and BLOWFISH .Throughput of DES 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 and Video ,we conclude that Throughput of each of these algorithms is almost same in all the above three forms of data.

From the experimental results, we finally conclude that 3DES has least performance efficiency as compared to DES,AES, BLOWFISH and RC4 algorithm. We also conclude that performance of RC4(Stream Cipher) algorithm is best as compared to all other algorithms(Block Ciphers) 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.

[18] Md Imran Alam*, Mohammad Rafeek Khan/ "Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography"/ International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013

[19] Md Imran Alam, Mohammad Rafeek Khan" Performance Evaluation of Different Cryptographic Algorithms: DES, 3DES, AES,IDEA & BLOWFISH"/ International Journal of Advanced and Innovative Research (2278-7844) / #203 / Volume 2 Issue 10