Volume 3, Issue 10, October 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography

Md Imran Alam*, Mohammad Rafeek Khan
Lecturer, Department of Computer Engineering & Networks,
Jazan University, Jazan, Saudi Arabia

Abstract— In the era of information technology, security is essential to transmit confidential information (like credit card details, banking transactions etc) over the unsecured network like internet. It is possibility that the information that is being transferred through network of computers or internet being read by other people. For this we need an efficient and secure way to protect our data. Cryptographic algorithms play a vital role in providing data security. Cryptography algorithms are divided into Symmetric and Asymmetric key cryptography. Symmetric Cryptography is further divided into Block Ciphers and Stream ciphers. This paper discusses Performance and Efficiency Analysis of different block cipher algorithms (DES, 3DES, CAST-128, BLOWFISH, IDEA & RC2) of Symmetric Key Cryptography. Block cipher algorithms has been compared based on the following factors: input size of data (in the form of text, audio and video), encryption time, decryption time, throughput of encryption and decryption of each block ciphers and power consumption. If throughput value of a block cipher is increased then power consumption value of that cipher is decreased and vice versa. From Experimental results, we analysed performance and efficiency of these block cipher algorithms (DES, 3DES, CAST-128, BLOWFISH, IDEA & RC2).

Keywords— Cryptography, Algorithms, Block, Stream ,Ciphers, Symmetric, Asymmetric, DES, 3DES, CAST-128, BLOWFISH, IDEA, RC2

I. INTRODUCTION

Cryptography plays very important role in security of data. 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.. 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 are you?" to his friend Bob. Here the message "Hello, How are you? "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 duh brx@" is a cipher text for the plain text message "Hello, How are you? "

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. Fig.1 shows the Encryption and Decryption flow of cryptography.[6]

Figure-1: Encryption-Decryption Flow

Fig1. Encryption and decryption Flow

Cryptography algorithms are divided into 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 discussed in this paper are: **DES, 3DES, CAST-128, BLOWFISH, IDEA and RC2.**

© 2013, IJARCSSE All Rights Reserved

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 and SEAL are examples 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.

Fig.2 shows classifications of Cryptography.

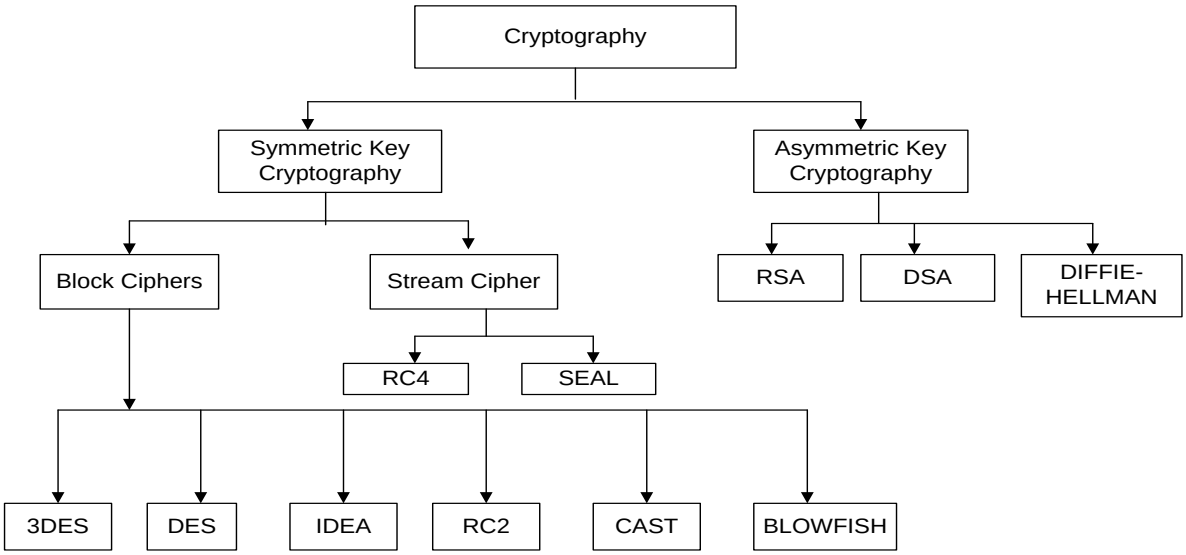

Fig.2 Classification of Cryptography

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

III. COMPARED ALGORITHMS

A. DES: Data Encryption Standard (DES) was designed by IBM and adopted by the U.S. government as the standard encryption method for non-military and non-classified use. The algorithm encrypts a 64-bit plaintext block using a 64-bit key [2]. DES has two transposition blocks (P-boxes) and 16 complex round ciphers (they are repeated). Although the 16 iteration round ciphers are conceptually the same, each uses a different key derived from the original key. The initial and final permutations are keyless straight permutations that are the inverse of each other. The permutation takes a 64-bit input and permutes them according to predefined values.

© 2013, IJARCSSE All Rights Reserved

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. 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.

D. CAST-128: CAST-128 was developed by Carlisle Adams and Stafford Tavares. [2]. CAST algorithm uses a 64-bit block size and a 64-bit key. [1]The structure of CAST should be familiar. The algorithm uses six S-boxes with an 8-bit input and a 32-bit output.To encrypt, first divide the plaintext block into a left half and a right half. The algorithm has 8 rounds. In each round the right half is combined with some key material using function f and then XORed with the left half to form the new right half. The original right half (before the round) becomes the new left half. After 8 rounds (don't switch the left and right halves after the eighth round), the two halves are concatenated to form the cipher text.
Function f is simple: [1]
(1) Divide the 32-bit input into four 8-bit quarters: *a, b, c, d*.
(2) Divide the 16-bit subkey into two 8-bit halves: *e, f*.
(3) Process *a* through S-box 1, *b* through S-box 2, *c* through S-box 3, *d* through S-box 4, *e* through S-box 5, and *f* through S-box 6.
(4) XOR the six S-box outputs together to get the final 32-bit output.
Alternatively, the 32-bit input can be XORed with 32 bits of key, divided into four 8-bit quarters, processed through the S-boxes, and then XORed together [7]. *N* rounds of this appears to be as secure as $N + 2$ rounds of the other option.

E. 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 IDE A. [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.

F. RC2: RC2 is a variable-key-size encryption algorithm designed by Ron Rivest [1]
RC2 is a variable-key-size 64-bit block cipher, designed to be a replacement for DES. According to the company, software implementations of RC2 are three times faster than DES. The algorithm accepts a variable-length key, from 0 bytes to the maximum string length the computer system supports; encryption speed is independent of key size.

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 51 KB to 12100 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
iii. Decryption Time
iv. Throughput of Encryption of different block ciphers with text, audio & video data
v. Throughput of Decryption of different block ciphers with text, audio& video data
vi. Power Consumption to Encrypt different Block Cipher algorithms
vii. Power Consumption to Decrypt different Block Cipher algorithms

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.

© 2013, IJARCSSE All Rights Reserved

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 different Block Ciphers DES, 3DES, CAST-128, BLOWFISH ,IDEA and RC2 are shown in Table1 and Table 2.
Table 1 shows the encryption time of different Block Ciphers where input data is in the form of text of different sizes. In this table encryption throughput of different block ciphers is also calculated.

Table 2 shows the decryption time of different Block Ciphers where input data is in the form of text of different sizes. In this table decryption throughput of different Block Ciphers 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 DES, IDEA, CAST-128, RC2 and BLOWFISH algorithm. We also noticed here that encryption and decryption time of BLOWFISH algorithm is the lowest as compared to 3DES, DES, CAST-128, IDEA and RC2 algorithm.

Table 1: Comparisons of 3DES, DES, CAST-128, BLOWFISH ,IDEA and RC2 based on Encryption Time (in Milliseconds)

Input Size (KB)	3DES	DES	CAST-128	BLOWFISH	IDEA	RC2
51	120	42	45	16	49	14
249	170	61	48	31	69	45
501	232	82	73	62	101	67
911	381	120	91	70	135	73
5601	1240	490	450	302	641	371
11110	2705	1020	740	601	1150	750
12100	3001	1071	790	678	1210	801
Throughput (MB/Sec)	3.88	10.57	13.64	17.34	9.09	14.39

Table 2: Comparisons of 3DES, DES, CAST-128, BLOWFISH, IDEA and RC2 based on Decryption Time(in Milliseconds)

Input Size (KB)	3DES	DES	CAST-128	BLOWFISH	IDEA	RC2
51	60	20	18	14	19	13
249	142	49	41	30	44	32
501	237	71	59	52	65	56
911	321	123	102	62	115	82
5601	1205	480	495	305	612	398
11110	2842	985	690	640	1190	731
12100	2980	1020	730	681	1241	796
Throughput (MB/Sec)	3.91	11.10	14.29	17.10	9.28	14.47

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

© 2013, IJARCSSE All Rights Reserved

Table3: It shows Encryption and Decryption Throughput of Audio and Video data.

Throughput (MB/Sec)	3DES	DES	CAST-128	BLOWFISH	IDEA	RC2
Encryption Throughput of Audio data	3.87	10.58	13.67	17.32	9.11	14.40
Decryption Throughput of Audio data	3.92	11.11	13.65	17.08	9.31	14.46
Encryption Throughput of Video data	3.89	10.61	13.69	17.31	9.14	14.45
Decryption Throughput of Video data	3.90	11.15	13.66	17.09	9.34	14.50

After analysing Fig 1 we conclude that throughput of BLOWFISH algorithm is higher than throughput of all other algorithms like 3DES, DES, CAST-128,IDEA and RC2. It is also noticed here that RC2 algorithm has advantage over DES, 3DES, IDEA, CAST-128 algorithm in terms of the processing time.

By analysing Fig.2, it is noticed here that BLOWFISH algorithm is far better than other algorithms (3DES, DES, CAST-128,IDEA and RC2) based on throughput value. It is also noticed that 3DES is almost 3 times slower than DES. It also shows that Encryption Throughput of BLOWFISH algorithm is greater than its Decryption Throughput.

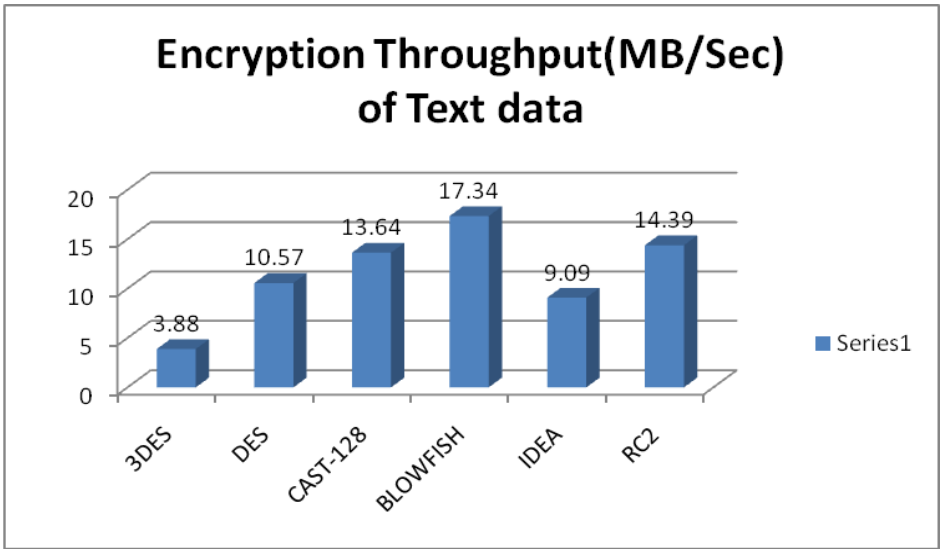

Fig.1 Throughput of Encryption of different Block Ciphers with Text data

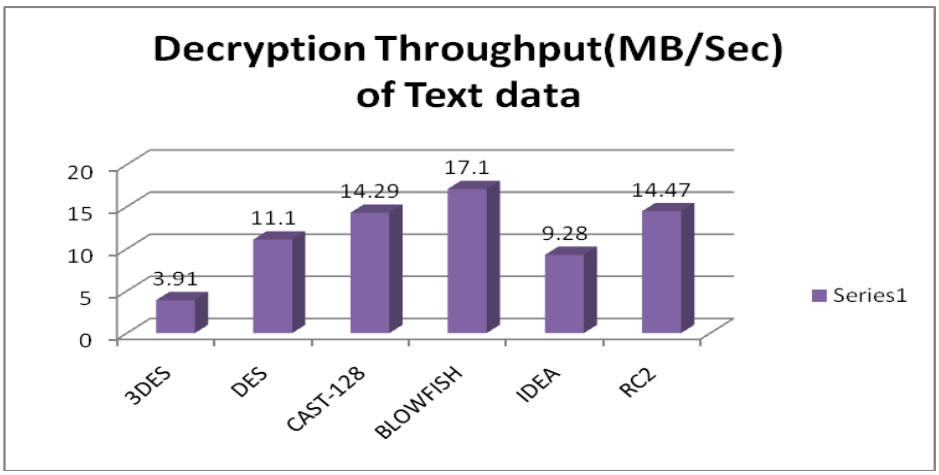

Fig.2 Throughput of Decryption of different Block Ciphers with Text data

© 2013, IJARCSSE All Rights Reserved

After Analyzing Fig.3 and Fig.4 we conclude that Throughput of Decryption of all block ciphers except BLOWFISH and CAST-128 is greater than their throughput of Encryption. Throughput of DES is greater than throughput of 3DES and IDEA.

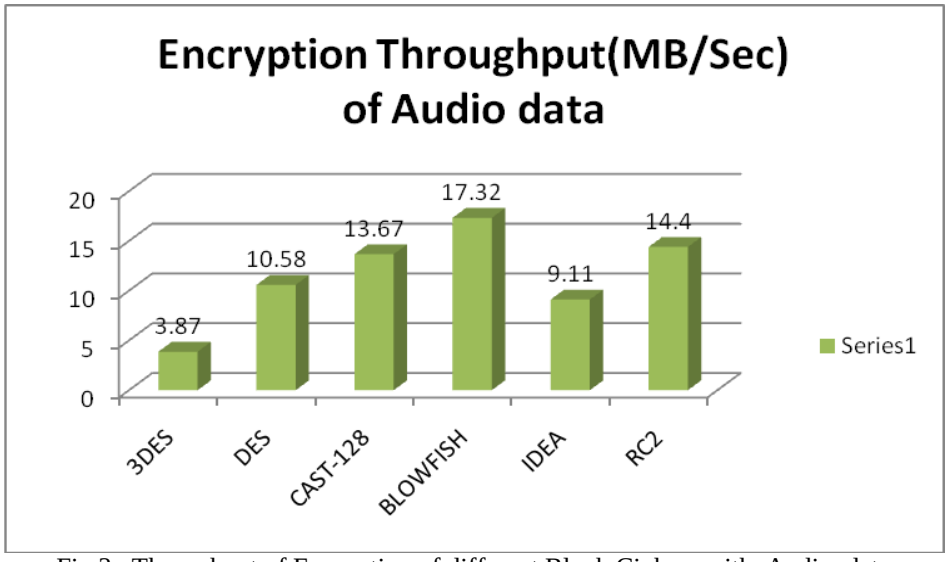

Fig.3 Throughput of Encryption of different Block Ciphers with Audio data

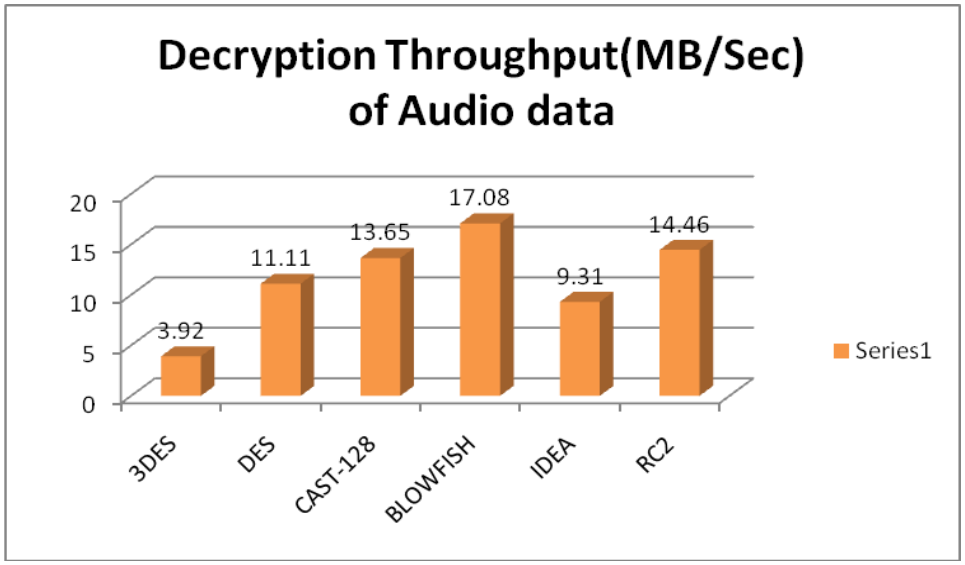

Fig.4 Throughput of Decryption of different Block Ciphers with Audio data

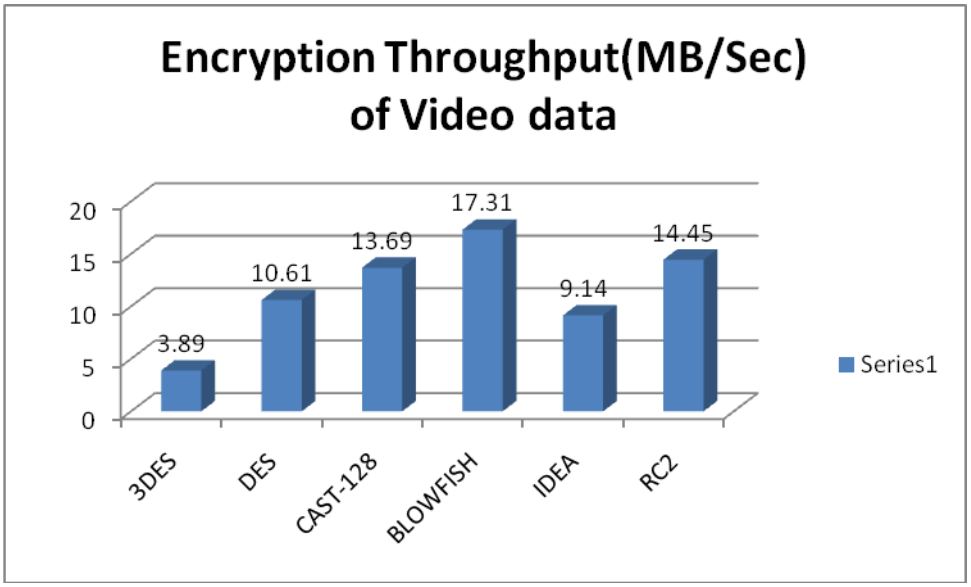

Fig.5 Throughput of Encryption of different Block Ciphers with Video data

© 2013, IJARCSSE All Rights Reserved

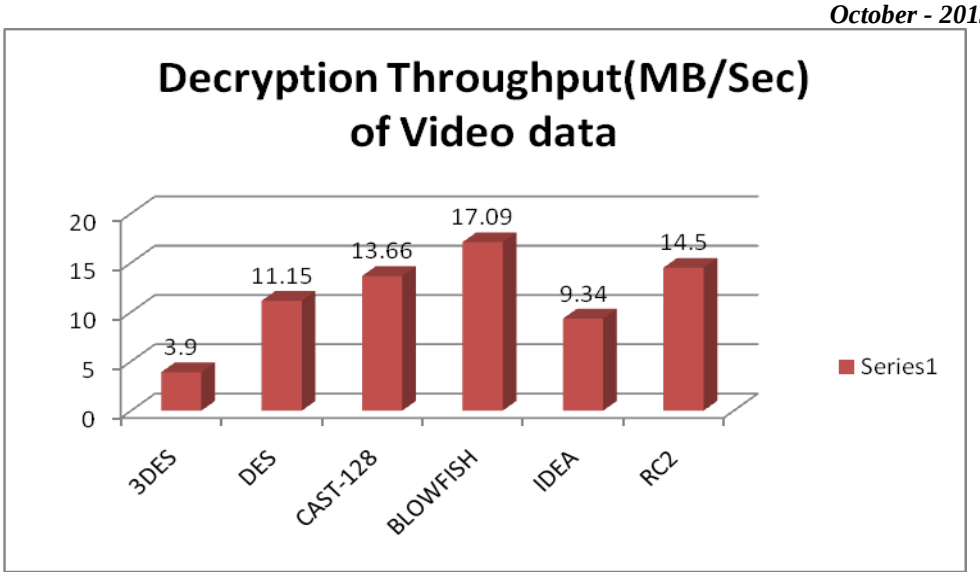

Fig.6 Throughput of Decryption of different Block Ciphers with Video data

By analyzing Fig5. and Fig.6 we conclude that DES is almost 3 times faster than 3DES. CAST-128 has advantages over DES,3DES and IDEA in terms of throughput.

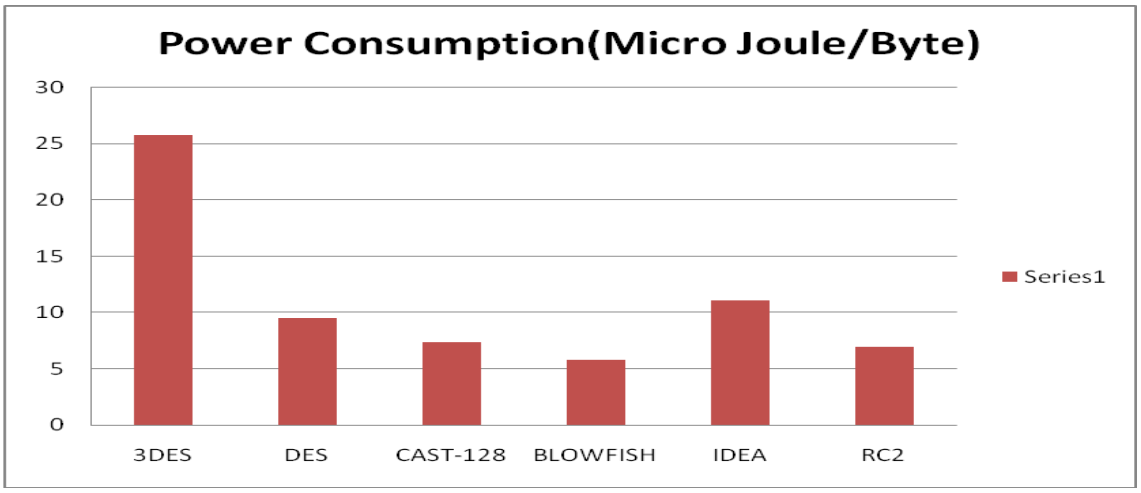

Fig.7 Power Consumption to Encrypt different Block Ciphers with different input data

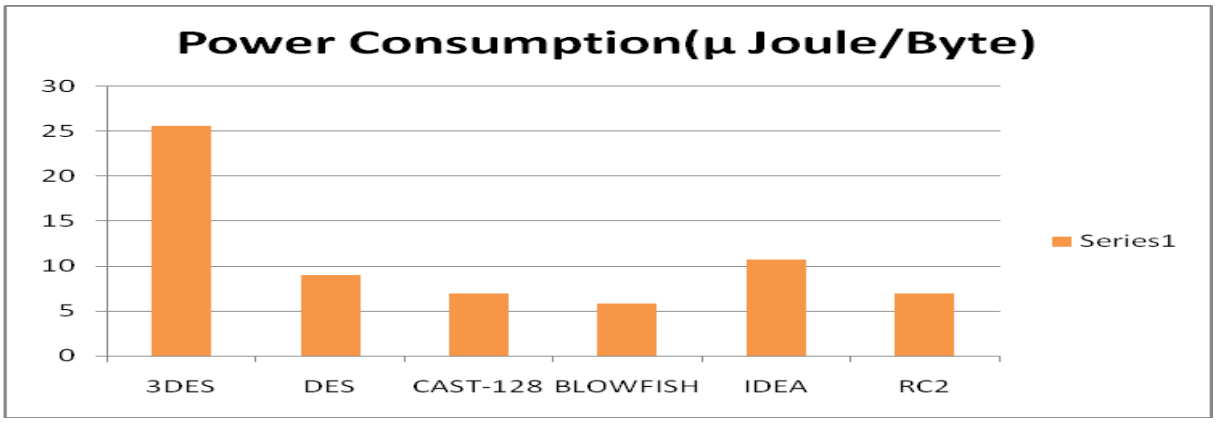

Fig.8 Power Consumption to Decrypt different Block Ciphers with different input data

By analyzing Fig.7. and Fig.8 we conclude that those block ciphers who have more Throughput values their Power Consumption values are less and vice versa.

VI. CONCLUSIONS

This paper presents a performance and efficiency analysis of different block cipher algorithms (3DES, DES, CAST-128, BLOWFISH, IDEA and RC2) of Symmetric Cryptography based on different performance factors. By analyzing experimental results several points can be concluded. We find that 3DES has more power consumption and less throughput than the DES due to its triple phase characteristics. Throughput of CAST-128 is better than DES, 3DES and

© 2013, IJARCSSE All Rights Reserved

IDEA. RC2 is faster for smaller sizes of input data as compared to BLOWFISH algorithm because of it has only one P-box for key expansion loaded into memory as compared to BLOWFISH which has one P-box and four S-boxes. Throughput value of BLOWFISH is greater than 3DES, DES, CAST-128, IDEA and RC2. Power Consumption value of BLOWFISH is least. 3DES having the least throughput value and maximum Power Consumption value as compared to all block ciphers discussed in this paper. From the experimental results it is also concluded that by taking input data in the form of text, audio as well as video throughput of Encryption and Decryption of all block ciphers discussed here is almost same in all three forms of data. Finally by analyzing Encryption/Decryption time, Encryption/Decryption Throughput and Power Consumption value we conclude that BLOWFISH has better performance and efficiency than all other block ciphers compared 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] 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

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

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

[14] 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

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

[16] W. Stallings. Cryptography and Network Security, Prentice Hall, 1995.

© 2013, IJARCSSE All Rights Reserved