Volume 3, No. 8, August 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICAL
Available Online at www.jgrcs.info

Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish

Pratap Chandra Mandal
Department of Computer Application, B.P.Poddar Institute of Management and technology, Kolkata, W.B., India
pcmandal9@gmail.com

***Abstract*:** Internet and networks applications are growing very fast. So the importance and the value of the exchanged data over the internet are increasing. Information Security has been very important issue in data communication. Any loss or threat to information can prove to be great loss to the organization. Encryption technique plays a main role in information security systems. This paper provides a fair comparison between four most common and used symmetric key algorithms: DES, 3DES,AES and Blowfish. A comparison has been made on the basis of these parameters: rounds, block size, key size, encryption/decryption time, CPU process time in the form of throughput and power consumption. These results show that blowfish is more suitable than AES. Simulation program is implemented using Java programming.

Keyword: Cryptography, Symmetric, Encryption, Decryption, DES, 3DES, AES, Blowfish

INTRODUCTION

Cryptography algorithms play an important role in information security. They can be divided into Symmetric and Asymmetric key cryptography [1]. In Symmetric key encryption only one key is used to encrypt and decrypt data. The key should be distributed before transmission between two parties. Key plays an important role in encryption and decryption . If a weak key is used in the algorithm then easily data can be decrypted. The size of the key determines the strength of Symmetric key encryption. Symmetric algorithms are of two types: block ciphers and stream ciphers. The block ciphers are operating on data in groups or blocks. .Examples are of Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish. Stream ciphers are operating on a single bit at a time. RC4 is stream cipher algorithm. Encryption algorithms consume significant amount of computing resources such as battery power, CPU time, etc. Asymmetric key (or public key) encryption is used to solve the problem of key distribution [3]. In Asymmetric key encryption, two keys are used; private keys and public keys. Public key is used for encryption and private key is used for decryption (e.g Digital Signatures). Public key is known to the public and private key is known only to the user. Prior to transmission there is no need for distributing them. Asymmetric encryption techniques are near to 1000 times slower than Symmetric techniques, since they require more computational processing power.

COMPARED ALGORITHMS

DES: (Data Encryption Standard): DES is a block encryption algorithm. It was the first encryption standard published by NIST (National Institute of Standards and Technology) [2][6].It is a symmetric algorithm, means same key is used for encryption and decryption .It uses one 64-bit key. Out of 64 bits, 56 bits make up the independent key, which determine the exact cryptography transformation, 8 bits are used for error detection.DES. The main operations are bit permutations and substitution in one round of DES. Six different permutation operations are used both in key expansion part and cipher part. Decryption of DES algorithm is similar to encryption, only the round keys are applied in reverse order. The output is a 64-bit block of cipher text. Many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher key.

3DES: 3DES is an enhancement of Data Encryption Standard [4]. It uses 64 bit block size with 192 bits of key size. 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.

AES: Advanced Encryption Standard (AES) also known as the Rijndael algorithm is a symmetric block cipher [3]. It was recognized that DES was not secure because of advancement in computer processing power. The purpose of NIST was to define a replacement for DES that can be used in non-military information security applications by US government agencies [1]. It can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. It has variable key length of 128, 192, or 256 bits; default 256. it encrypts the data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices [6]. AES has been tested for many security applications.

Blowfish: It is one of the most public domain encryption algorithms [3]. Blowfish was designed in 1993 by Bruce Schneider as a fast alternative to existing encryption algorithms. Blowfish is a symmetric key block cipher that uses a 64 bit block size and variable key length. It takes a variable-length key from 32 bits to 448 bits. Blowfish has variants of 14 rounds or less [6]. Blowfish is a very secure cipher but it is has been replaced by Twofish and Rijndael due to its small 64 bit block size. Blowfish is one of the fastest block ciphers which has developed to date. Slowness kept Blowfish from being used in some applications. Blowfish was created to allow anyone to use encryption free

of patents and copyrights. Blowfish has remained in the public domain to this day. No attack is known to be successful against it, though it suffers from weak keys problem (Bruce, 1996) (Nadeem, 2005).

Table 1 Comparison of DES, 3DES, AES and Blowfish algorithm

Algorithm	Key Size	Block Size	Rounds
DES	56 bits	64 bits	16
3DES	112 bits or 168 bits	64 bits	48
AES	128 bits, 192 bits, 256 bits	128 Bits	10, 12 or 14
Blowfish	32-448 bit .	64 bits	16

RELATED WORKS

To give more prospective about the performance of the compared algorithms, this section discusses the results obtained from other resources. In [7] we found that after only 600 encryptions of a 5 MB file using Triple-DES the remaining battery power is 45% and subsequent encryptions are not possible due to battery dies rapidly. In [5] they concluded that AES is faster and more efficient than other encryption algorithms. When the transmission of data is considered there is insignificant difference in performance of different symmetric key schemes. Under the scenario of data transfer it would be better to use AES scheme in case the encrypted data is stored at the other end and decrypted multiple times. [8] Discussed for different popular secret key algorithms such as DES, 3DES, AES, and Blowfish. They were implemented, and their performance was compared by encrypting input files of varying sizes and contents.

SIMULATION PROCEDURE

Main purpose here is to calculate the Encryption and Decryption speed of each algorithm for different packet sizes. Their implementation is tried to optimize the maximum performance for the algorithm. The throughput for encryption as well as decryption is calculated one by one. Encryption time is used to calculate the throughput of an encryption scheme .The throughput of the encryption scheme is calculated by dividing the total plaintext in MB by total encryption time in Second for each algorithm. If the throughput value is increased, the power consumption of this encryption technique is decreased .Similar procedure has been followed to calculate the throughput of decryption scheme.

For my experiment, I have used Pentium IV of 2.4 GHz CPU speed with 4 GB RAM. In this experiment the text files sizes range from 50 KB to 22300 KB.
The performance metrics are analyzed by the following:
(a) Encryption/decryption time.
(b) CPU process time – in the form of throughput.
(c)Power consumption.

Throughput = Plain Text (MB) / Encryption or decryption time (Sec.)

EXPERIMENTAL RESULTS

Encryption / decryption algorithms have been tested with different text size files.

Table 2 Throughput of DES and 3DES with different file size (MB/Sec)

Input size(kb)	DES		3DES	
	ENC	DEC	ENC	DEC
50	31	51	56	54
108	35	47	48	50
246	46	71	109	75
320	80	73	165	85
695	145	121	227	149
781	86	121	171	153
900	241	152	301	171
5500	248	166	307	178
7311	1692	954	178	110
22300	1716	119	179	170
Average Time	432	295.	496.	371.
Throughput	8.64	12.6	7.52	10.0

Table 3 Throughput of AES and Blowfish with different file size (MB/Sec)

input size(kb)	AES		Blowfish	
	ENC	DEC	ENC	DEC
50	56	64	38	38
108	40	57	45	29
246	110	75	43	64
320	162	147	44	90
695	212	144	47	91
781	165	152	66	96
900	260	172	66	103
5500	258	170	118	100
7311	1365	880	105	139
22300	1366	883	152	137
Avg Time	399.4	274.	72.	88.7
Throughput	9.35	13.6	51.	42.11

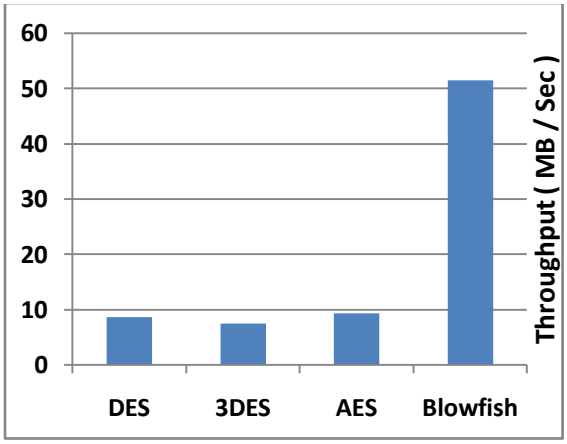

Figure1. Throughput of encryption algorithms

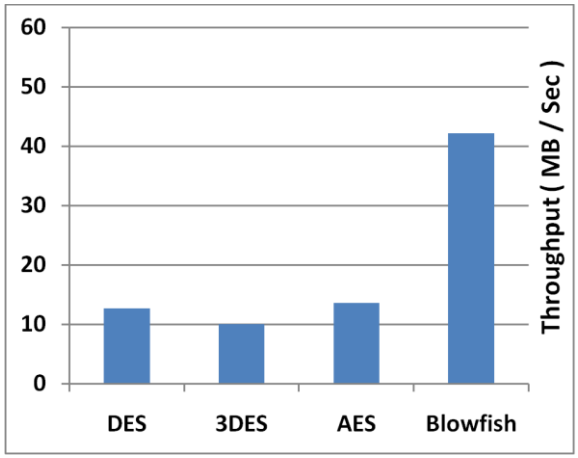

Figure2. Throughput of decryption algorithms

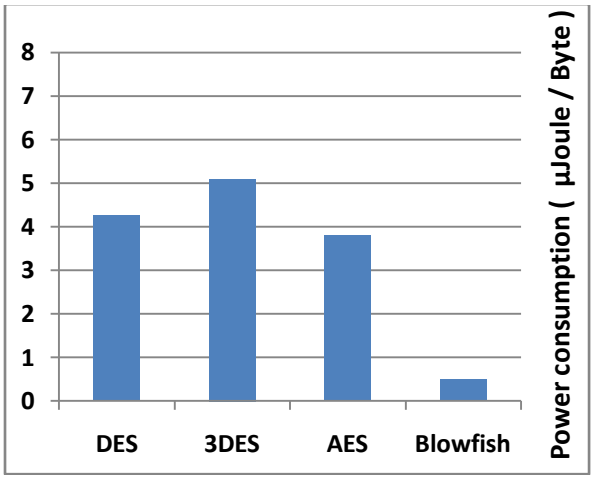

Figure 3. Power consumption(µJule / Byte)

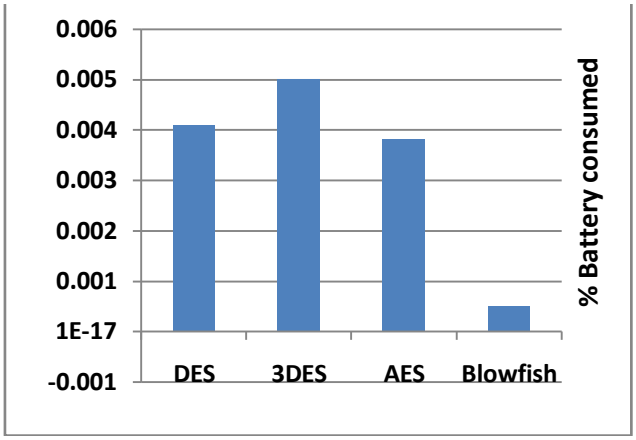

Figure 4. Power consumption (% battery consumed)

SIMULATION RESULTS AND DISCUSSION

All The above results show the superiority of Blowfish algorithm 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. Again, AES has advantage over the 3DES and DES in terms of throughput and power consumption except Blowfish. 3DES has least performance because of its triple phase encryption characteristics. Finally we can conclude that Blowfish is the best of all.

CONCLUSION AND FUTURE SCOPE

This paper presents the performance evaluation of selected symmetric algorithms. From the presented simulation we can conclude that Blowfish has better performance than other algorithms. Secondly, AES has advantage over the other 3DES and DES in terms of throughput & decryption time except Blowfish. Third point is that 3DES has the least performance among all the algorithms mentioned here. In future the work may be extended by including the schemes and techniques over different types of data such as image, sound and video and developing a stronger encryption algorithm with high speed and minimum energy consumption.

REFERENCES

[1] Himani Agrawal and Monisha Sharma "Implementation and analysis various symmetric cryptosystems " in indian Journal of Science and Technology in Vol. 3 No.12 (Dec 2010) ISSN: 0974- 6846.pp.1173-1176

[2] Jawahar Thakur , Nagesh Kumar " DES , AES and Blowfish : Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis" in International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 1,Issue 2,December 2011),pp.6-12

[3] Shanta, yoti Vashishtha on " Evaluating the performance of Symmetric Key Algorithms:AES(Advanced Encryption Standard) and DES(Data Encryption Standard) in IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 ,pp.43-49

[4] S.Pavithra, Mrs. E. Ramadevi " STUDY AND PERFORMANCE ANALYSIS OF CRYPTOGRAPHY ALGORITHMS " International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 5, July 2012 14 pp.82-86

[5] Nagesh Kumar, Jawahar Thakur, Arvind Kalia on "PERFORMANCE ANALYSIS OF SYMMETRIC KEY CRYPTOGRAPHY ALGORITHMS:DES , AES

and BLOWFISH " in An International Journal of Engineering Sciences ISSN: 2229-6913 Issue Sept 2011, Vol. 4 ,pp.28-37.

[6] Monika Agrawal,Pradeep Mishra "A Comparative Survey on Symmetric Key Encryption Techniques"International Journal on Computer Science and Engineering (IJCSE) Vol.4 No. 05 May 2012, pp.877-882.

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

[8] A. Nadeem, "A performance comparison of data en-eryption algorithms, "IEEE information and Communi cation Technologies , pp. 84-89, 2006.

[9] Kallam Ravindra Babu , Dr. S. Udaya Kumar , Dr. A. Vinaya Babu ," Survey on Cryptography and Stegano graphy Methods for Information Security "International Journal of Computer Applications (0975 – 8887)Volume 12– No.2 November 2010.

[10] G. Manikandan, M. Kamarasan "A Hybrid Approach for Security Enhancement by Modified Crypto - Stegno Scheme "European Journal of Scientific Research "ISSN 1450 - 216 X Vol .60 No.2 (2011) , pp. 206 - 212 ©EuroJournals Publishing Inc. 2011

[11] William Stalling, "Cryptography and Network Security Principles and Practice 5th Edition", Pearson.

[12] Mohit Kumar1 ,Reena Mishra ,Rakesh Kumar Pandey and Poonam Singh " Comparing Classical Encryption with Modern Techniques " S-JPSET, Vol.1 , Issue 1 copyright samriddhi, 2010

[13] Gary C. Kessler "An Overview of Cryptography" http ://www.garykessler.net/library/crypto.html (17 November 2006)

[14] Shashi Mehrotra Seth, Rajan Mishra on " Comparative Analysis Of Encryption Algorithms For Data communication " in IJCST Vol. 2, Iss ue 2, June 2011 I ,pp. 292-294

[15] Ali Ahmad Milad ,Hjh Zaiton Muda,Zul Azri Bin Muhamad Noh, Mustafa Almahdi Algaet " Comparative Study of Performance in Cryptography Algorithms (Blowfish and Skipjack) "Journal of Computer Science 8 (7): 1191-1197, 2012 ISSN 1549- 3636 © 2012 Science Publications

[16] Diaa Salama Abd Elminaam , Hatem Mohamed Abdual Kader , and Mohiy Mohamed Hadhoud "Evaluating The Performance of Symmetric Encryption Algorithms" International Journal of Network Security, Vol. 10, No.3, PP.216–222, May 2010.

[17] Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha "Performance Evaluation of Symmetric Cryptography Algorithms " IJECT Vol. 2, Issue 3, Sept. 2011 ISSN : 2230-7109, pp.144-146

[18] Srinivasarao D, Sushma Rani N , Ch. Panchamukesh and S.Neelima " ANALYZING THE SUPERLATIVE SYMMETRIC CRYPTOGRAPHIC ENCRYPTION ALGORITHM (ASCEA) "Journal of Global Research in Computer Science Volume 2, No.7, July 2011 ,pp.101-105

[19] Rishabh Arora, Sandeep Sharma, PhD " Performance Analysis of Cryptography Algorithms " International Journal of Computer Applications (0975 – 8887) Volume 48 No.21, June 2012 ,pp.35-39

[20] Gurjeevan Singh , Ashwani Kr. Singla , K.S. Sandha "Superiority of Blowfish Algorithm in Wireless Networks" International Journal Computer Applications (0975 – 8887) Volume 44 – No11, April 2012,pp.23-26

