Volume 2, Issue 9, September 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Superiority of Blowfish Algorithm

Pratap Chnadra Mandal
Asst. Prof, Dept of Computer Application
B.P.Poddar Institute of Management & technology,
West Bengal, India

Abstract: 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, and encryption / decryption time, CPU process time in the form of throughput and power consumption. These results show that blowfish is better than other algorithm.

Keyword- Encryption, Decryption, DES, 3DES, AES, Blowfish

I. INTRODUCTION

Cryptography algorithms are divided into Symmetric and Asymmetric key cryptography [1]. Symmetric key encryption use only key to encrypt and decrypt data. 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. 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.

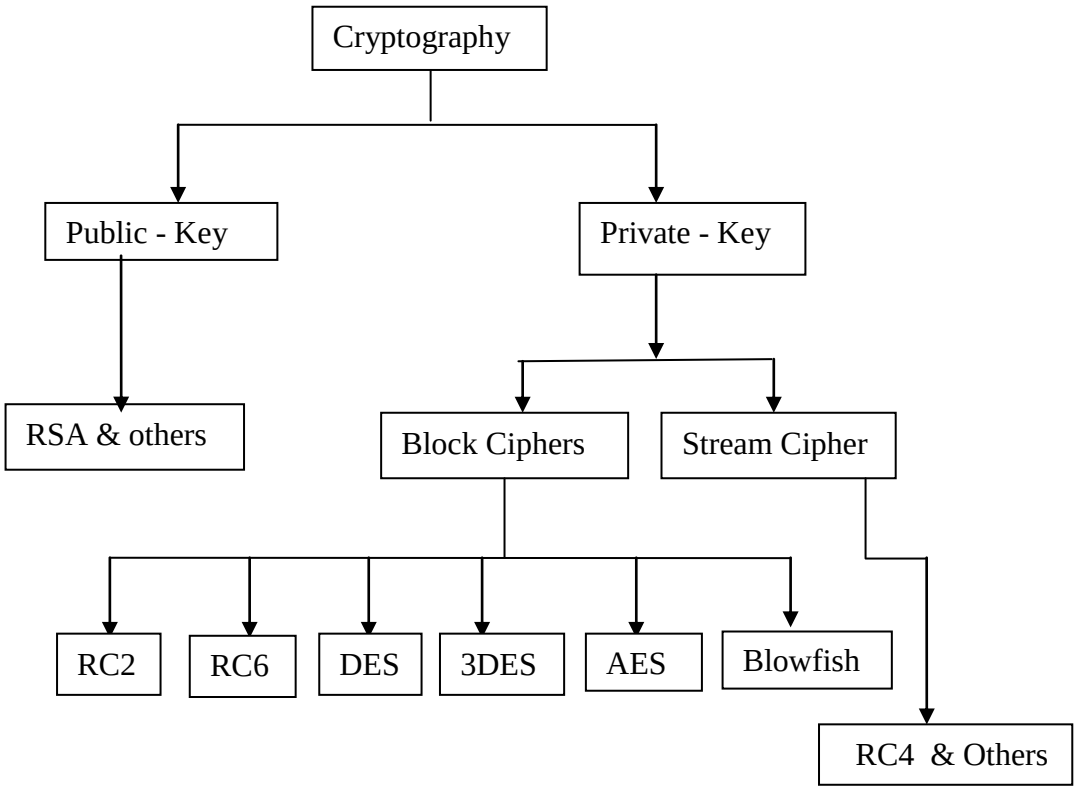


Figure 1 : Overview of the field of Cryptography

A. Basic Terms Used in Cryptography

Plain Text: The original message that we wish to communicate with the others is defined as Plain Text [2]. In cryptography the actual data that has to be send to the other is referred as Plain Text. For example, Alice is a person wishes to send "Congratulation" message to the person Duke. Here "Congratulation" is a plain text message.

Cipher Text: The message which has been converted by the encryption algorithm is called cipher text. In Cryptography the original message is transformed into non readable message

Encryption: A process of converting plain text into cipher text is called as Encryption. Cryptography uses the encryption algorithm and a key to send confidential data through an insecure channel.

Decryption: A reverse process of encryption is called decryption. It is a process of converting cipher text into plain text. Decryption requires decryption algorithm and a key.

B. Purpose of Cryptography

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.

II. COMPARED ALGORITHMS

RC2: RC2 is a block cipher with 64-bits block cipher and a variable key size that range from 8 to128 bits. RC2 is vulnerable to a related-key attack using 234 chosen plaintexts

DES: (Data Encryption Standard): DES was the first encryption standard published by NIST (National Institute of Standards and Technology) [3].It is a symmetric algorithm; 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. 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.

3DES: It uses 64 bit block size with 192 bits of key size [5]. 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: It was recognized that DES was not secure because of advancement in computer processing power [6]. 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.

RC6: RC6 is block cipher derived from RC5. It was designed to meet the necessities of the Advanced Encryption Standard competition. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. Some references consider RC6 as Advanced Encryption Standard

Blowfish: Blowfish was designed in 1993 by Bruce Schneider as a fast alternative to existing encryption algorithms [4]. 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 [7]. 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)

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

Algorithm	Key Size	Block Size	Algorithm Structure	Rounds	Cracked?	Existing Cracks
DES	56 bits	64 bits	Feistel Network	16	Yes	Brute force attack, differential crypanalysis, linear cryptanalysis
TripleDES	112 bits or 168 bits	64 bits	Feistel Network	48	No	Theoretically possible
AES (Rijndael)	128 bits, 192 bits, 256 bits	128 Bits	Substitution-Permutation Network	10, 12 or 14	No	Side channel attacks
Blowfish	32-448 bit in steps of 8 bits. 128 bits by default	64 bits	Feistel Network	16	No	Second-order differential attack

III. RELATED WORKS

This section discusses the performance of the compared algorithms.

. In paper [7] they said 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.

In paper [9] consider the performance of encryption algorithm for text files .AES, DES and RSA algorithm has been evaluated from the parameters like Computation time, Memory usage, Output bytes.
Comparing these three algorithms they found RSA takes more time for computation process. The memory usage of each algorithm is considered as memory byte level. RSA takes more memory than AES and DES. Finally, the output byte is calculated by the size of output byte of each algorithm. The level of output byte is equal for AES and DES, but RSA algorithm produces low level of output byte.

IV. SIMULATION RESULTS

I have calculated the Encryption and Decryption speed of each algorithm for different packet sizes. Their implementation has 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
(a) Encryption/decryption time.
(b) CPU process time – in the form of throughput.

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

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

Input size(kb)	DES		3DES		AES		Blowfish	
	ENC	DEC	ENC	DEC	ENC	DEC	ENC	DEC
50	31	51	56	54	56	64	38	38
108	35	47	48	50	40	57	45	29
246	46	71	109	75	110	75	43	64
320	80	73	165	85	162	147	44	90
695	145	121	227	149	212	144	47	91
781	86	121	171	153	165	152	66	96
900	241	152	301	171	260	172	66	103
5500	248	166	307	178	258	170	118	100
7311	1692	954	1787	1100	1365	880	105	139
22300	1716	1196	1796	1700	1366	883	152	137
Avg. Time	432	295.2	496.7	371.5	399.4	274.4	72.4	88.7
Throughput	8.64	12.65	7.52	10.05	9.35	13.61	51.59	42.11

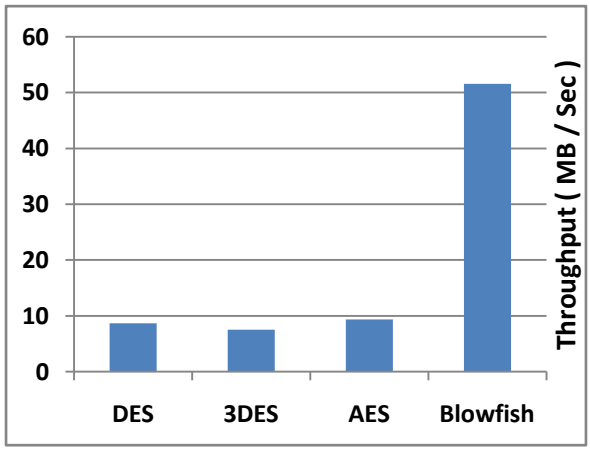


Figure2. Throughput of encryption algorithms

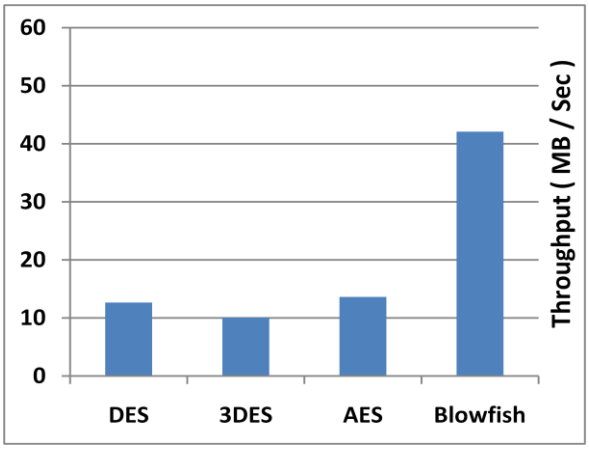
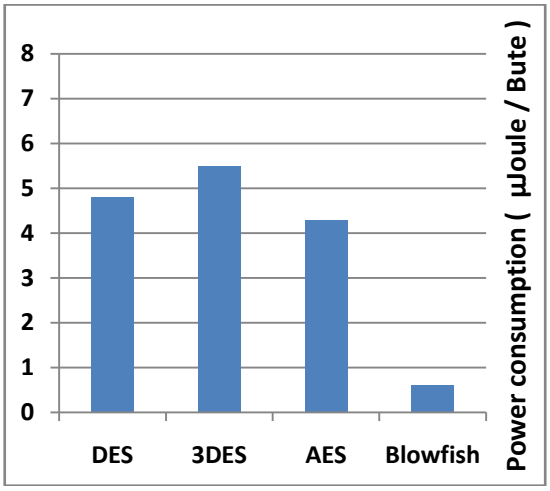
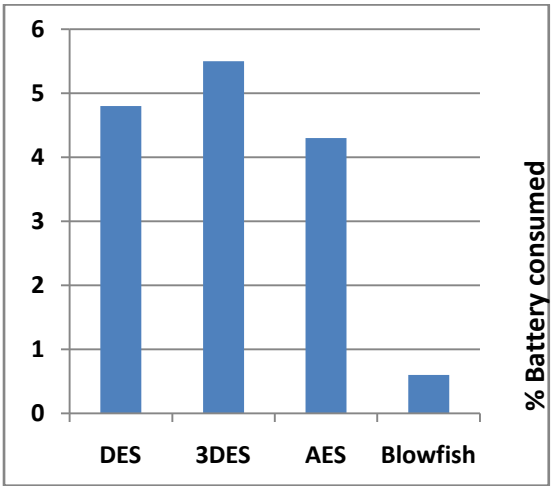


Figure3. Throughput of decryption algorithms



Power consumption
(µ Joule / Byte)



Power consumption
(% Battery consumed)

V. CONCLUSION AND FUTURE SCOPE

The above results show 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.

REFERENCES

[1] Jawahar Thakur, Nagesh Kumar,"DES,AES andBlowfish: 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

[2] E. Thambiraj,G. Ramesh,Dr. R. Umarani , "A survey on Various Most Common Encryption Technique " International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 7, July 2012,pp226-233

[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] 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- 846 ,p.1173-1176

[5] 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

[6] A. Nadeem, "A performance comparison of data encryption algorithms, "IEEE information and Communication Technologies , pp. 84-89, 2006.

[7] Nagesh Kumar, Jawahar Thakur, Arvind Kalia on "PERFORMANCE ANALYSIS OF SYMMETRIC KEY CRYPTOGRAPHY ALGORITHMS:DES , AES and BLOWFISH " in AnInternational Journal of Engineering Sciences ISSN: 2229-6913 Issue Sept 2011, Vol. 4 ,pp.28-37.

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

[9] 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

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

[11] Diaa Salama Abd Elminaam , Hatem Mohamed AbdualKader , 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.

[12] 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

[13] Rishab Arora, Sandeep Sharma, PhD “Performance Analysis of Cryptography lgorithms ” International Journal of Computer Applications (0975 – 8887) Volume 48 No.21, June 2012 ,pp.35-39

[14] 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.

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

[16] 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 cience Publications

