

Encryption Quality and Performance Analysis of GKSB Algorithm

S. Arul jothi^{1*} Dr. M. Venkatesulu²

1. Research Scholar, Department of Computer Applications, Kalasalingam University, Krishnankoil, Srivilliputtur (via), Tamil Nadu, India, 626 190.
2. Senior Professor & Head, Department of SHIP, Kalasalingam University, Krishnankoil, Srivilliputtur (via), Tamil Nadu, India, 626 190.

* E-mail of the corresponding author: s.aruljothi.p@gmail.com

Abstract

In the age of intensive data exchanges, security of data poses a major challenge to the existing communication arrangement. In this context the evolution and evaluation of new encryption system is inextricably linked to the process of realizing ever increasing network security needs. Recently a Generalized Key Scheme in a Block Cipher Algorithm (GKSBC) is found to be robust in cryptanalysis and the result of key sensitivity analysis was found satisfactory. This study compares GKSB with the class of block cipher algorithms viz., RC6, AES and Blowfish, and presents a performance evaluation. To assess the encryption quality two measures viz., Encryption Quality measure and Correlation analysis is applied. Thorough experimental tests with detailed analysis showed the high quality and comparative efficiency of GKSB algorithm.

Keywords: symmetric, generalized, throughput, encryption, correlation.

1. Introduction

In a world of interconnected computers and networks, security is a major challenge in relation to data exchange among them. Unauthorized access poses a great threat to the data exchange across different channels of communication and therefore, the evolution and the studies of crypt algorithms is inextricably linked to the process of advancement in the network security. Encryption schemes of different kinds are at different stages of development and their relative cryptanalytic characteristics are continuously evaluated to pave the way for robust and efficient security algorithms. One of the commonly used crypt scheme is the symmetric key scheme in which same key is used for encryption and decryption. This symmetric encryption scheme is preferred over other schemes because it is simple, fast and prevents widespread message security compromise. Among the two classes of symmetric key crypt schemes, block cipher and stream cipher crypt methods address distinctive requirements. In the block cipher crypt scheme segment competing algorithms are abound in the literature. Recently a generalized key scheme in a block cipher algorithm is found to be robust in cryptanalysis and the result of key sensitivity analysis was found satisfactory in GKSB. Following the tradition of comparing algorithms of same class, comparing the various block cipher schemes with respect to their performance are not common in the literature. This study attempts to compare the newly developed generalized key scheme block cipher algorithm within the class of block cipher algorithms viz., RC6, AES and Blowfish. The issues related to quality of encrypted image and computational speeds are not previously done for the GKSB.

In this study the rest of the paper is organized as follows. The earlier works related to this study is described in section II. The experimental results of the comparison and security analysis are presented in section III. Finally the concluding remarks are given in section IV.

2. Previous studies

To give more prospective about the performance of the compared algorithms, this section discusses the results obtained from other resources.

A study in [2] is conducted for six of the most common encryption algorithms namely: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. Experimental results are given to demonstrate the effectiveness of each

algorithm. In the case of changing key size it can be seen that higher key size leads to clear change in the battery and time consumption.

It was concluded in [3] 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 AES, CAST and IDEA and asymmetric schemes RSA, ElGamal, and ECIES. Even during data transfer it would be advisable to use AES scheme in case the encrypted data is stored at the other end and decrypted multiple times. This paper gives the relationship between encryption at the link layer and at the application layer.

A study in [4] is conducted for different popular secret key algorithms such as DES, 3DES, AES, and Blowfish have been implemented, and their performance is compared by encrypting input files of varying contents and sizes, on different Hardware platforms. The algorithms have been implemented in a uniform language, using their standard specifications, to allow a fair comparison of execution speeds. The algorithms were tested on two different hardware platforms, to compare their performance. They had conducted it on two different machines: P-II 266 MHz and P-4 2.4 GHz. The results showed that Blowfish had a very good performance compared to other algorithms. Also it showed that AES had a better performance than 3DES and DES. It also shows that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data.

In paper [5] a study a comparison has been conducted for AES DES, 3DES, RC2, Blowfish, and RC6 at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, data transmission through wireless network and finally encryption/decryption speed. There is insignificant difference between open key authentications and shared key authentication in ad hoc Wireless LAN connection with excellent signals. In case of poor signal we found transmission time is increased minimum by 70 % over open sheered authentication in ad hoc mod.

Experiments was done in [6] for comparing the performance of various security options available for client authentication, hashing algorithms, cryptography techniques, and digital signatures. For simplicity they have isolated the different categories of security and restricted the performance comparison to the options available with each category; of course in a real secure system, the overall security will be the combination of one or more of these categories. The results shows that basic authentication without SSL could be used for better performance, but no matter how fast it is, it would not be useful in systems that are vulnerable to threats not mitigated by it.

In paper[7] a comparison of three most common symmetric key cryptography algorithms: DES, AES, and Blowfish. Since main concern here is the performance of algorithms under different settings, the presented comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used. The comparison is made on the basis of these parameters: speed, block size, and key size. The results showed that Blowfish has a better performance than other common encryption algorithms used.

In paper[8] the authors made a comparative analysis of AES algorithm with different modes of operation (block cipher) and RC4 algorithm (stream cipher) in terms of CPU time, encryption time, memory utilization and throughput at different settings like variable key size and variable data packet size. Based on the analysis and result, paper[8] concluded that AES algorithm is better to use based on different performance metrics. The various metrics were: Encryption time, Decryption time, Throughput, CPU process time, Memory Utilization.

3. Encryption quality and performance analysis

In this section a series of encryption quality and performance analysis tests were conducted on the GKSBC using video, audio and text files with varying sizes. For experiment, we used Microsoft Windows XP Professional Version 2002 Service Pack 3 on Intel(R) Core(TM) Duo CPU, 1.83GHz to 0.99 GB of RAM and performance data was collected. The algorithm is implemented using NetBeans IDE. The results of the encryption quality were analysed using Matlab 7.0. In the experiment different files size ranges from 1.261 to 3.362 Mega Bytes for text data, the file size ranged from 3.672 to 7.603 Mega Bytes for audio data, and the same ranged from 2.888 to 150.882 Mega Bytes for video files was used. A good encryption scheme should posses high encryption quality and low execution time.

3.1. Encryption Quality

In this scheme, to test the encryption quality we adopted two encryption quality test viz., EQ measure and image correlation analysis. The results of the respective tests were presented in this section.




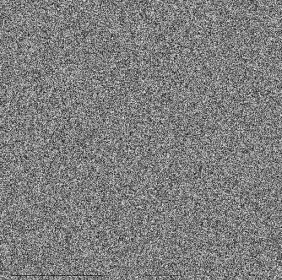
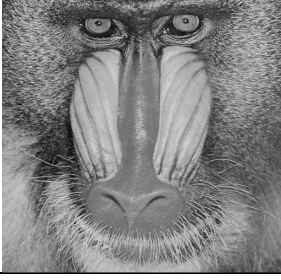
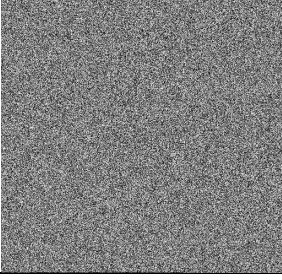
3.1.1. EQ Measure

The encryption process causes a large change in the grey scale value of pixels. These changes would present a grey scale pattern different from that of the original file. The larger deviation is a measure of a quality of encryption.

Let F and F' denote the original image (plain image) and the encrypted image (cipher image) respectively, each of size $M \times N$ pixels with L grey levels. Let $HL(F)$ denote the array of number of occurrences of each grey level L in the original image (plain image) F . Similarly, $HL(F')$ denotes the array of number of occurrences of each grey level L in the encrypted image (cipher image) F' as given in [9]. The encryption quality represents the average number of changes to each grey level L and is expressed mathematically as

$$\text{Encryption Quality} = \frac{\sum_{L=0}^{255} |H_L(F') - H_L(F)|}{256} \quad (1)$$

Table 1. EQ measure of Encryption Quality for different image files using GKSBC

Image Files	Original image	Encrypted image	EQ measure
LENA 512×512			663.82
GIRL 512×512			894.89
BABOON 512×512			773.90

The lower value of 'EQ' means the more effective of image encryption and hence the encryption quality [10,11]. The results of this experiment are shown in Table 1 and it is found that the encryption quality is much high across different images for GKSBC..

3.1.2. Correlation Analysis

Statistical tool such as correlation analysis is used to measure the relationship between the plain and encrypted image.

In this analysis the correlation coefficient is defined over the pixel values of two adjacent pixels, adjacency is described in terms of horizontal, vertical, diagonal and anti diagonal directions. This correlation measure is computed for plain and cipher images. On each image, for every category of adjacent pixels, pixel values of 1000 pairs of positions are randomly selected as evaluated in [11,12,13]. If x and y are grey-scale values of two adjacent pixels in a image, the correlation coefficient is computed for those pairs of data using the following formula.

$$r_{xy} = \frac{\text{Cov}(x,y)}{\sqrt{D(x)D(y)}} \quad (2)$$

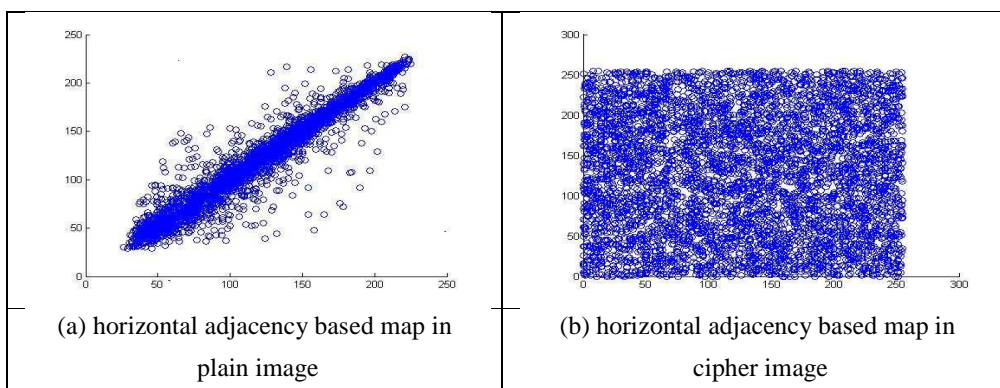
where, $\text{Cov}(x,y) = \frac{1}{N} \sum_{i=1}^N [(x_i - E(x)) (y_i - E(y))]$, $D(x) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)]^2$, $D(y) = \frac{1}{N} \sum_{i=1}^N [y_i - E(y)]^2$

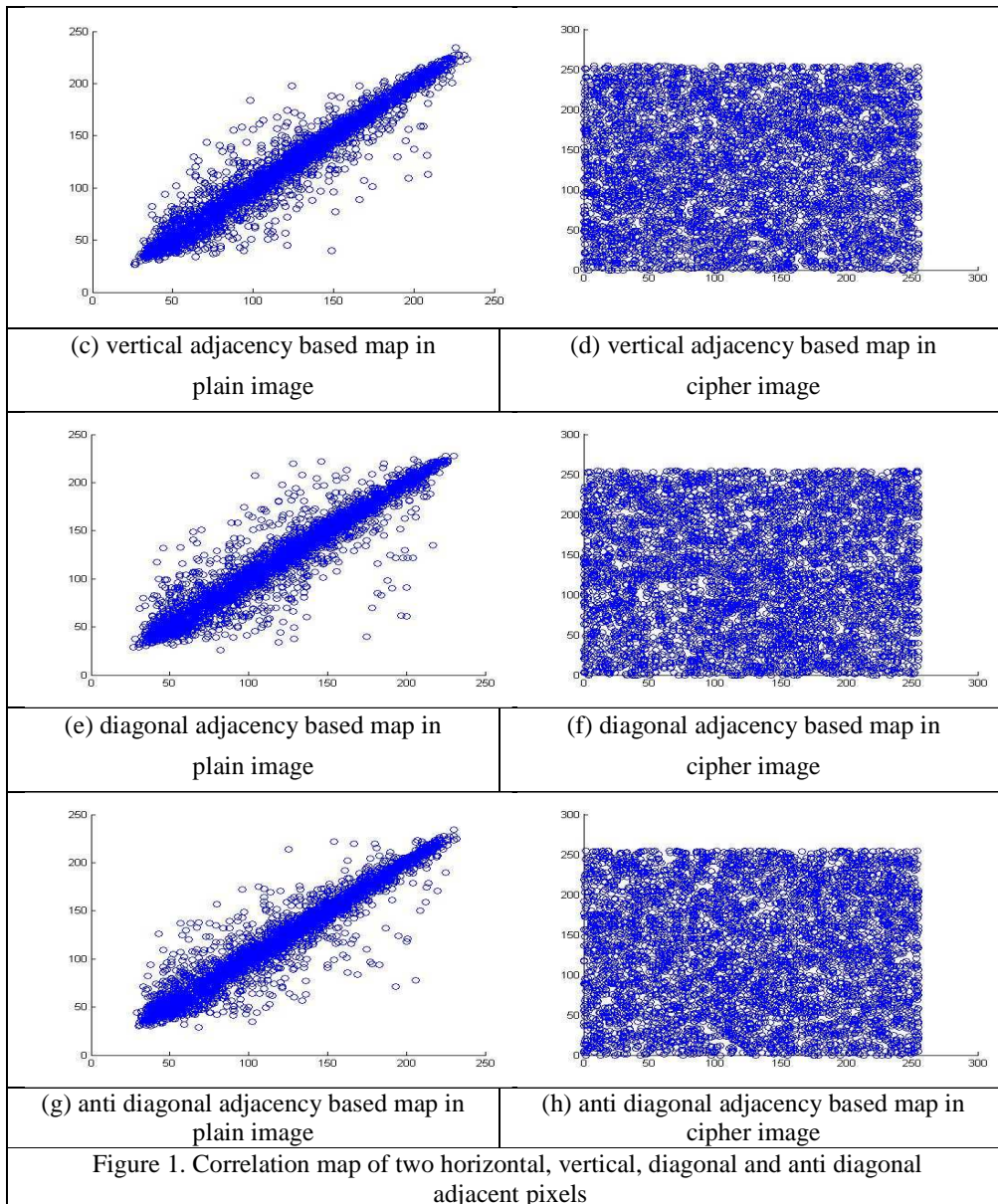
If the correlation coefficient equals one, that means the original image and its encryption is identical. If the correlation coefficient equals zero, that means the encrypted image is completely different from the original. If the correlation coefficient equals minus one that means the encrypted image is the negative of the original image.

Table 2. Correlation coefficients of two adjacent pixels for GKSBC algorithm

Direction of Adjacent Pixels	Plain Image	Cipher Image
Horizontal	0.972797	-0.01559
Vertical	0.975641	0.017019
Diagonal	0.958392	-0.00218
Anti Diagonal	0.967876	0.016248

The results of correlation analysis may also be represented in the correlation maps where the pixel values of pair of adjacent pixels are shown as scatter plot. For the plain image, the scatter points are clustered around the 45° principal axis. If the encrypted image also show the similar pattern the original and cipher image are identical. On the other hand, if the encrypted image does not show any such pattern, it means that the encrypted image is completely different from the original. The Fig. 1(a,b) shows the correlation distribution of two horizontally adjacent pixels in the plainimage/cipherimage and Fig. 1(c,d) shows the correlation distribution of two vertically adjacent pixels in the plainimage/cipherimage for GKSBC.





The correlation map and the correlation coefficient indicate that correlation between pixels of the original image is higher, while there is a little correlation between neighboring pixels in the encrypted image. The picture shows complete diffusion and correlation coefficients are close to zero and negative for each neighborhood. Hence, the results show that the encryption quality of encrypted images from GKSB is high. This analysis also demonstrates to what extent the proposed encryption algorithm could resist statistical attacks.

3.2. Performance Analysis

To investigate the relative performance of proposed algorithm the encryption time and throughput analysis is done. The results of the relevant tests and the discussions are presented in this section.

3.2.1. Encryption time

Another important tool to evaluate the efficiency of algorithms is measuring the amount of time required for

encryption. In this investigation, actual time to encrypt the data will be used as a measure of execution time. Designer should attempt to optimize a cryptosystem to make the execution time as lower as possible. The results of this test are shown in Table 1, 2 & 3 as follows.

3.2.2. Throughput

Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the encryption time as calculated in [14,15].

Table 3. Comparative execution times of encryption algorithms for video files with different file size

Input size in (Kbytes)	RC6 (secs)	AES (secs)	BlowFish (secs)	GKSBC (secs)
2,888	14	15	3	2
3,875	19	21	4	3
4,725	23	27	5	4
5,851	28	32	6	5
6,389	32	40	7	6
7,603	42	47	9	7
35,830	170	178	38	27
64,404	340	455	77	70
142,738	792	834	151	115
150,882	820	892	189	150
Average Time in secs	228	254.1	48.9	38.9
Throughput (Megabytes/sec)	0.18	0.16	0.84	1.06

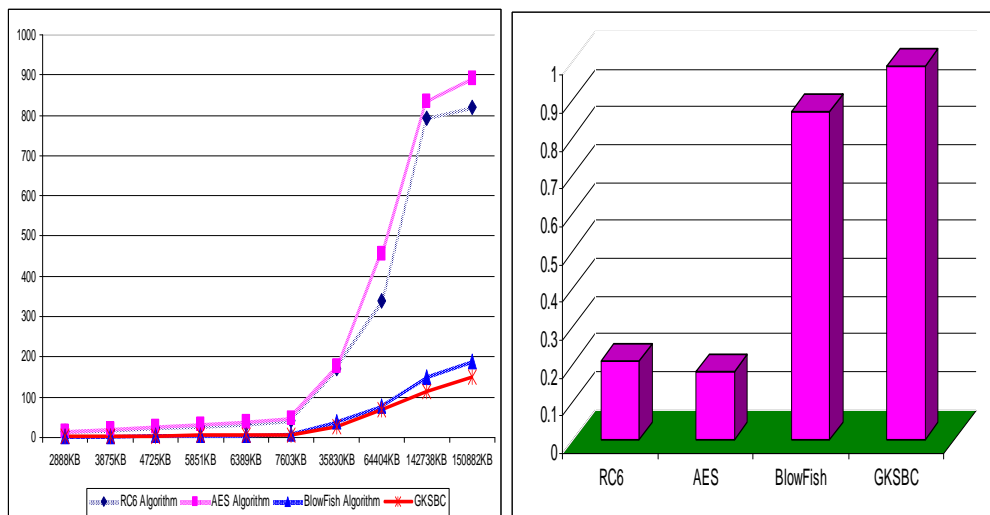


Figure 2. Encryption and throughput for video files

Table 3 clearly indicates that the average encryption time for video files was least for GKSBC(38.9) compared to RC6(228), AES(254.1) and Blowfish(48.9) in the experiment. The throughput was maximum for GKSBC(1.06) compared to RC6(0.18), AES(0.16) and Blowfish(0.84) in the experiment.

Table 4. Comparative execution times of encryption algorithms for text files with different file size

Input size in (Kbytes)	RC6 (secs)	AES (secs)	BlowFish (secs)	GKSBC (secs)
1,261	5.223	6.421	1.421	1.122
1,357	5.822	7.847	1.547	1.234
1,589	6.472	8.062	1.812	1.512
1,605	7.349	8.793	1.797	1.557
1,634	8.132	9.032	1.844	1.763
1,679	8.678	9.844	2.032	2.003
2,388	10.132	11.220	2.360	2.156
2,505	10 830	12 875	2 875	2 344
2,636	11.436	13.953	2.953	2.765
3,362	15.592	18.564	3.750	3.233
Average Time in secs	8.96	10.66	2.23	1.96
Throughput (Megabytes/sec)	0.21	0.18	0.87	0.99

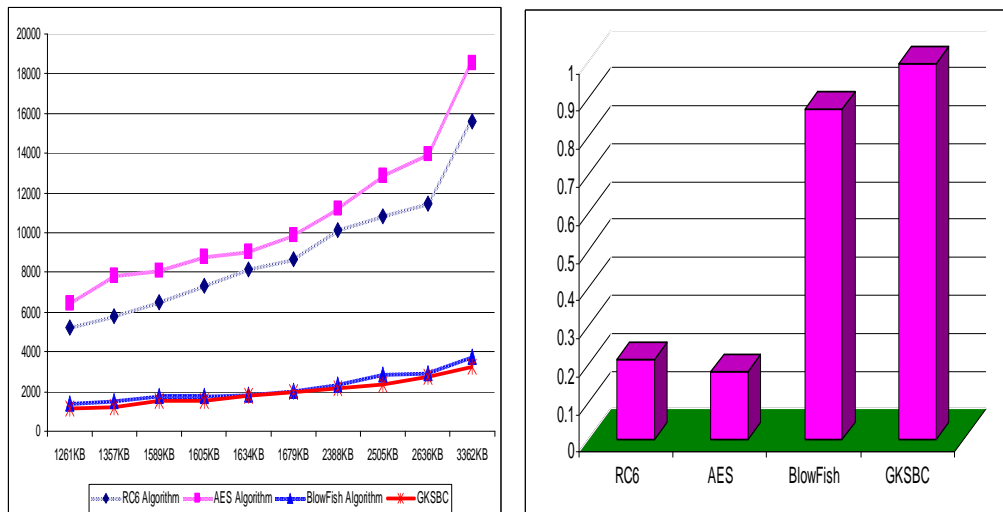


Figure 3. Encryption and throughput for text files

Table 4 clearly indicates that the average encryption time for text files was least for GKSBC(1.96) compared to RC6(8.96), AES(10.66) and Blowfish(2.23) in the experiment. The throughput was maximum for GKSBC(0.99) compared to RC6(0.21), AES(0.18) and Blowfish(0.88) in the experiment.

Table 5. Comparative execution times of encryption algorithms for audio files with different file size

Input size in (Kbytes)	RC6 (secs)	AES (secs)	BlowFish (secs)	GKSBC (secs)
3,672	20.281	21.345	4.656	3.543
4,175	21.562	23.322	5.125	4.768
4,484	22.233	24.534	4.859	4.534
4,883	24.431	25.981	5.297	5.112
5,107	25.622	26.734	5.515	5.322
5,287	26.342	28.523	5.718	5.813
5,775	28.482	30.382	6.281	6.543
6,100	30.639	31.982	6.766	7.113
6,389	33.871	43.549	6.890	7.235
7,603	37.563	38.721	8.250	7.312
Average Time in secs	27.10	29.50	5.93	5.72
Throughput (Megabytes/sec)	0.19	0.17	0.88	0.91

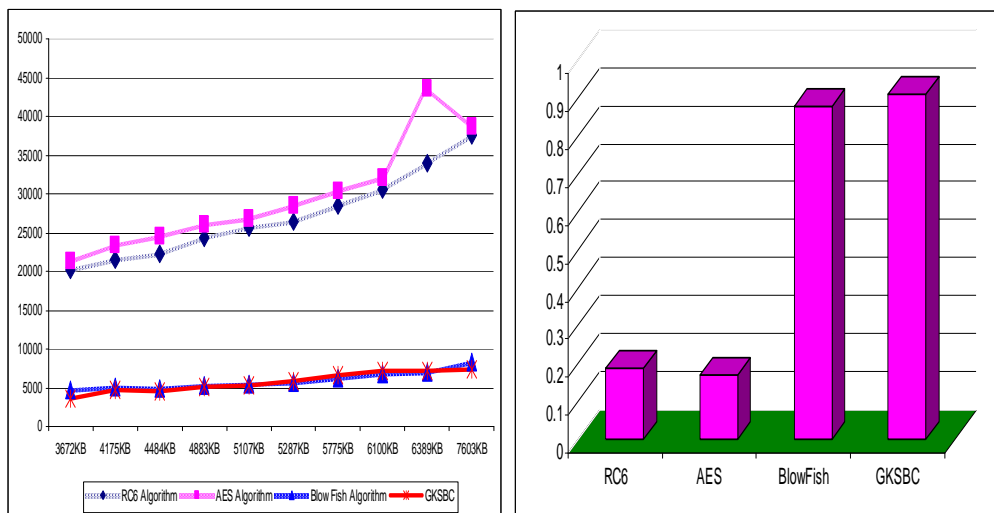


Figure 4. Encryption and throughput for audio files

Table 5 clearly indicates that the average encryption time for audio files was least for GKSBC(5.72) compared to RC6(27.10), AES(29.50) and Blowfish(5.93) in the experiment. The throughput was maximum for GKSBC(0.91) compared to RC6(0.19), AES(0.17) and Blowfish(0.88) in the experiment.

4. Conclusion

This paper presents a performance evaluation of GKSBC algorithm in relation to selected symmetric encryption algorithm (RC6, AES and Blowfish). To assess the encryption quality two measures viz., Encryption Quality measure and Correlation analysis is applied. Both the measures indicate that the GKBC algorithm performed well. GKSBC algorithm and other algorithm were applied on a set of files of different types and sizes for encryption and decryption. The encryption / decryption time analysis and throughput analysis clearly indicated that GKSBC outperformed all the select encryption algorithm Thorough experimental tests with detailed analysis showed the high quality and comparative efficiency of GKSBC algorithm.

References

- [1] Aruljothi S, Venkatesulu M. (2012). A Generalized Key Scheme in a Block Cipher Algorithm and its Cryptanalysis. *International Journal of Computer Applications*, 49(9).
- [2] Abdul_Elminaam D S, Abdul_ kader H M, Hadhoud M M. (2010). Evaluating The Performance of Symmetric Encryption Algorithm. *International Journal of Network Security*, 10: 216–222.
- [3] Hirani S. (2003). Energy consumption of encryption Schemes in wireless devices. Thesis, University of Pittsburgh.
- [4] Nadeem A. (2006). A performance comparison of data encryption algorithm. *IEEE Information and Communication Technologies*. 84–89.
- [5] Abdul_Elminaam D S, Abdul_ kader H M, Hadhoud M M. (2009). Performance Evaluation of Symmetric Encryption Algorithm on Power Consumption for Wireless Devices. *International Journal of Computer Theory and Engineering*, 1(4).
- [6] Priya Dhawan. (2002). Performance Comparison: Security Design Choices. Microsoft Developer Network.
- [7] Jawahar Thakur, Nagesh Kumar. (2011). DES, AES and Blowfish: Symmetric Key Cryptography Algorithm Simulation Based Performance Analysis. *International Journal of Emerging Technology and Advanced Engineering*, 1(2).
- [8] Nidhi Singhal, Raina J P S. (2011). Comparative Analysis of AES and RC4 Algorithm for Better Utilization. *IJCTT International journal of computer trends and technology*, 1(3).
- [9] Hossam El-din H Ahmed, Hamdy M Kalash, Osama S Farag. (2007). Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images. *International Journal of Computer and Information Engineering* , 1(1).
- [10] Alireza Jolfaei, Abdolrasoul Mirghadri. (2011). Image Encryption Using Chaos and Block Cipher. *Computer and Information Science*, 4(1).
- [11] Saeed Bahrami, Majid Naderi. (2012). Image Encryption Using a Lightweight Stream Encryption Algorithm. *Advances in Multimedia*.
- [12] Ismail I A, Mohammed Amin, Hossam Diab. (2010). A Digital Image Encryption Algorithm Based A Composition Of Two Chaotic Logistic Maps. *International Journal of Network Security*, 11(1): 1–10.
- [13] Krishnamurthy G N, Ramaswamy V. (2009). Performance Analysis of Blowfish and its Modified Version using Encryption quality, Key sensitivity, Histogram and Correlation coefficient analysis. *International Journal of Recent Trends in Engineering*, 1(2).
- [14] Nidhi Singhal, Raina J P S. (2011). Comparative Analysis of AES and RC4 Algorithm for Better Utilization. *International Journal of Computer Trends and Technology*,.
- [15] Ramesh G, Umarani R. (2012). Performance Analysis of Most Common Symmetrical Encryption Algorithm. *International Journal of Power Control Signal and Computation*, 3(1).