www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-4, Issue-3, Jun- 2016
Research Paper

Int. J. Sc. Res. in Network Security and Communication
ISSN: 2321-3256

Comparative Analysis of Performance Characteristics of well-known Symmetric Key Encryption Algorithms

[1*]OKOLIE, Samuel O. and [2]ADETOBA, Bolaji T.

[1,2]Babcock University, Department of Computer Science,
Ilishan, Remo, Ogun State, Nigeria
[1]okolies@babcock.edu.ng, [2]tiwabj@yahoo.com

Received: May/12/2016 Revised: May/24/2016 Accepted: Jun/21/2016 Published: Jun/30/2016

Abstract- Security of data in data communication has become an important issue over the years. Consequently, various encryption schemes have come up as a solution, thus making encryption play an important role in information security system. These encryption schemes use some algorithms to scramble data into unreadable text which can only be decoded or decrypted by those that possesses the associated key. These algorithms consume significant amount of computing resources such as CPU time and storage (memory and primary storage). This paper therefore performs comparative analysis of four symmetric key encryption algorithms; AES, DES, 3DES and Blowfish by considering four parameters, encryption time, decryption time, memory usages and number of output bytes. Experimental results using Data Security Model Analyser was used in analysing the effectiveness of each of these algorithms.

Keywords*: Encryption, Performance characteristics, AES, DES, 3DES, Blowfish*

1. INTRODUCTION

Security of data in data communication plays a vital role and as such a comparative study of various cryptography methods or algorithms is of great importance. Cryptography is the art of transforming the information on the applications into scrambled or unintelligible format [1]. It involves mathematical techniques related to the aspects of information security such as Confidentiality, Integrity, and Authentication (CIA) of the data.

Encryption, which is a process of converting a plain text (readable form) into a scrambled text (cipher text), is a fundamental tool for the protection of sensitive information. The purpose of encryption is privacy (preventing disclosure or confidentiality) in communications. Encryption is a way of talking to someone while other people are listening but cannot understand what you are saying [2]. Encryption algorithms play a vital role in providing data security against malicious attacks. The algorithms can be categorised into symmetric key (private) and asymmetric (public) key [3].The most important type of encryption algorithm is the symmetric key encyrption in that the same key is used for both encryption and decryption. Hence the secrecy of the key is maintained and it is kept private. The symmetric key encryption can either be in block ciphers or as the stream ciphers. One of the main advantages of using the symmetric key encryption is that the computational power is small. Some of the well known symmetric algorithms are Advanced Encryption Standard (AES) algorithm, Data Encryption Standard (DES) algorithm, Triple Data Encryption Standard (Triples DES or 3DES) and Blowfish algorithm.

In asymmetric key encryption, different keys are used for encryption and decryption process; i.e. private and public keys. Public key is used for encyrption while private key is used for decryption. Asymmetric key encryption is also known as public key encryption. Asymmetric algorithms are generally slow and it is impractical to use them to encrypt large amounts of data. The keys used in public-key encryption algorithms are usually much longer, thereby increasing the security of the data being transmitted. Some of the asymmetric algorithms are RSA (Rivest Shamir Adleman) algorithm, Diffie-Hellman algorithm, El-Gamar algorithm, etc.

However, over the years, many known and unknown encryption algorithms have evolved and these algorithms consume a significant amount of computing resources such as CPU time, memory and battery power [4]. Thus, it becomes imperative to analyze some of these algorithms based on their performance so as to know which one of them to use in a particular domain of interest. Hence, this study provides a fair performance evaluation and

comparison between AES, DES, 3DES and Blowfish algorithms.

2. LITERATURE REVIEW

In this section, an overview of the algorithms (AES, DES, Triple-DES and Blowfish) is briefly discussed and some analysis conducted to compare each of the algorithms.

2.1 The AES Algorithm

Advanced Encryption Standard (AES) is a secret key block cipher encryption algorithm. This means that the number of bytes that it encrypts is fixed. AES can currently encrypt blocks of 16 bytes (128 bits) at a time, but if the bytes being encrypted are larger than the specified block, then it is executed concurrently. Thus, AES encrypts a minimum of 16 bytes. However, if the plaintext is smaller than 16 bytes, then it must be padded.

AES is an iterated symmetric block cipher. This means that AES works by repeating the same defined steps multiple number of times.

The operations performed during this iterative process can be categorized under the following functions:

- ADD ROUND KEY
- BYTE SUB
- SHIFT ROW
- MIX COLUMN

The schematics of AES structure is given in the figure 1

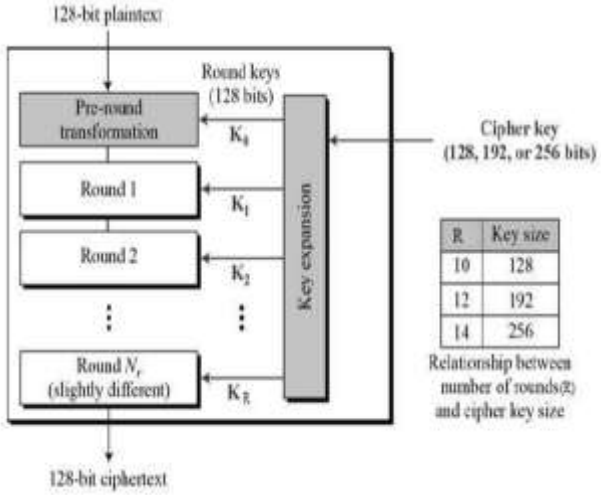

Figure 1: AES Algorithm Structure (Badlawala et. al. [5])

2.2 The DES Algorithm

Data Encryption Standard (DES) is the block cipher which takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another text bit string of the same length. It is a symmetric encryption technique which means that both sender and receiver use a shared key to encrypt and/or decrypt the data.

DES works on bits, or binary numbers 0s and 1s, by encrypting groups of 64 message bits, which is the same as 16 hexadecimal numbers. To do the encryption DES uses "keys" which are also apparently 16 hexadecimal numbers long, or apparently 64 bits longs. However, every 8th key bit is ignored in the DES algorithm, so that the effective key size is 56 bits.

DES encryption transformation scheme employs two operations on the plain text, which are:

- Create 16 subkeys, each of which 48-bits longs
- Encode each 64-bit block of data

Decryption is simply the inverse or opposite of encryption, following the same steps as for encryption, but in reverse order in which the subkeys are applied.

2.3 Triple DES (3DES) Algorithm

Triple-DES (variously called 3DES, 3-DES, TDES) is just DES with three 56-bit keys applied. Given a plaintext message, the first key is used to DES-encrypt the message. The second key is used to DES-decrypt the encrypted message, and since the second key is not the right key, this descryption just scrambles the data further. The twice-scrambled message is then encrypted again with the third key to yield the final ciphertext. The encryption scheme is illustrated in the figure 2.

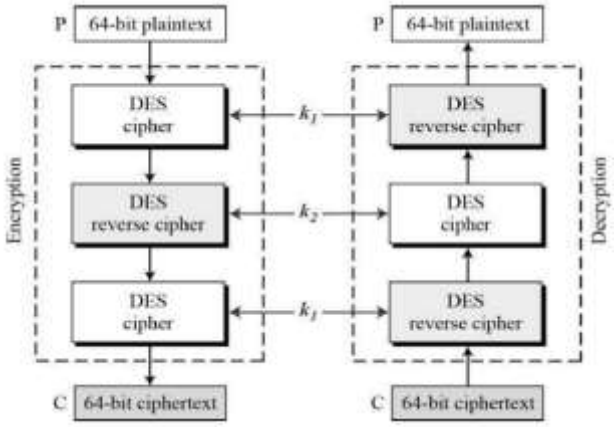

Figure 2: Triple-DES encryption scheme

(Source:http://www.tutorialspoint.com/cryptography/triple_des. htm [11])

Decryption of a ciphertext is a reverse process. Triple-DES first decrypt using k_3, then encrypt with k_2 and finally decrypt with k_1.

2.4 Blowfish Algorithm

Blowfish is a symmetric block cipher designed in 1993 by Bruce Schneider. It is fast and free alternative to existing encryption algorithms, which can be effectively used for encryption and safeguarding of data. It takes a variable-

length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish algorithm is a Feistel Network, which uses a 16-round Feister cipher and uses large key-dependent S-boxes. Each round consists of a key-dependent permutation, and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words.

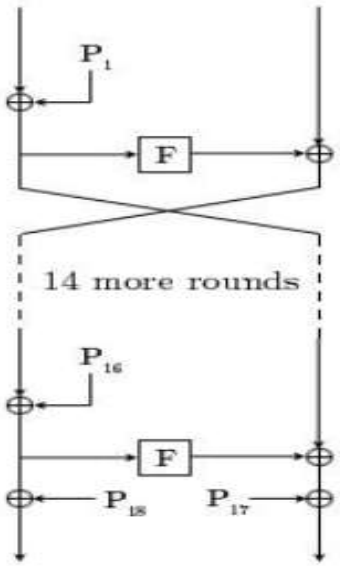

Fig 3: The Feistel structure of Blowfish
[Source: en.wikipedia.org/wiki/File:BlowfishDiagram.png]

3. RELATED WORK

In this paper, different methodologies and techniques for encryption used by various researchers are provided. Al Tamimi [6], carried out a performance comparison between four most common encryption algorithms: DES, 3DES, Blowfish and AES. The comparison was conducted by running several encryption settings to process different sizes of data blocks to evaluate the algorithm's encryption and decryption speed. Simulation has been conducted using C# language. The simulation results showed that Blowfish has a better performance than other common encryption algorithms used. Since Blowfish has not any known security weak points so far, which makes it an excellent candidate to be considered as a standard encryption algorithm. AES showed poor performance results compared to other algorithms since it requires more processing power. The same test was also conducted by Sachin & Jeevan [7].

Thakur, Kumar and Kalia [8] provides a fair comparison between three most common symmetric key cryptography algorithms: DES, AES, and Blowfish. Since the 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. Simulation program is implemented using Java programming. The results showed that Blowfish has a better performance than other common encryption algorithms used.

A study conducted by Yousif, et. al. [9], on the performance of different encryption techniques using encryption and decryption speed, power consumption, throughput as parameters. It was concluded that the encryption or decryption speed for DES algorithms is faster than RSA, AES is found to be more secure compared to DES, the throughput rates for blowfish is greater than all symmetric algorithms while the power consumption of BLOWFISH is the least among all algorithms. Adekanmbi et, al., [10] evaluates the effect(s) of common encryption algorithms on throughput, processing time and power consumption of a wireless system. Three different encryption algorithms commonly used for Wireless Local Area Network (WLANs) namely; Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Blowfish were evaluated and studied. The three algorithms were simulated and compiled using the default settings in .NET 2010 visual studio. The results show that Blowfish algorithm outperforms other algorithms in terms of energy consumption, processing time and throughput for Text data, Audio files and Image files. While DES is optimal both in its throughput and energy requirement

In this work, four of the well-known encryption algorithms were compared using different parameters and employing Java programming language, a data security model analyzer was built to analyze these algorithms.
.

4. METHODOLOGY

The comparative analysis of the encryption algorithms discussed in section 2, were simulated using a DataSecurity model analyzer. The analyzer was built in Java programming language using Netbean IDE 7.2 as the application development environment. The analyzer allows the user to select five test files (which are in rich text format) of different sizes and also allows the user to select the encryption algorithms to use. The button inscribed the word “Analyze” would be pressed to compute the encryption time, decryption time, memory usage and output bytes of each of the encryption algorithms selected. The screenshot of the analyzer is shown in figure 3.

3.1 DATA SECURITY MODEL ANALYSER

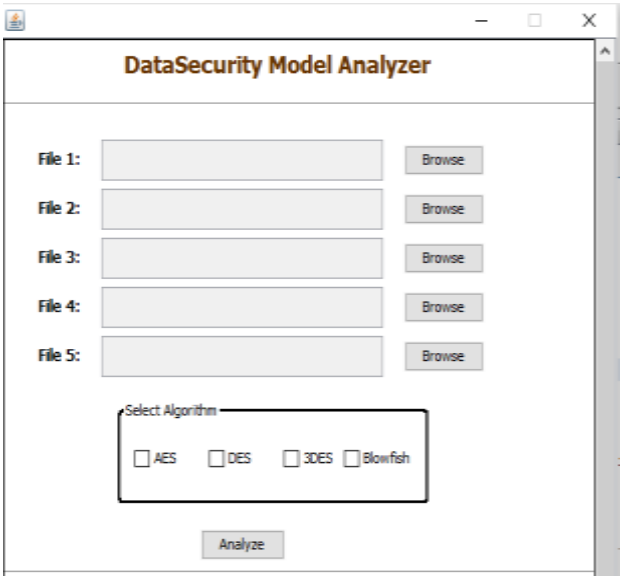

Figure 3: DataSecurity Model Analyzer for analyzing encryption algorithms

3.2 EVALUATION FACTORS

The following factors such as encryption time, decryption time, memory usage, and output bytes, are used as the performance evaluation metrics on five text files of different sizes (63KB, 127KB, 259KB, 319KB and 383KB).

Encryption Time

The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plain text. This is used to calculate the throughput of an encryption algorithm, which is the total plaintext in bytes encrypted divided by the encryption time.

Decryption Time

The decryption time is consdered to be the time taken for an encryption algorithm to produce a plain text from a cipher text

Memory Usage

This is used to measure the amount of memory space utilized by an encryption algorithm. Memory usage determines how an encryption algorithm affects the performance of the system being used. This is computed by using the getRuntime(). totalMemory() and getRuntime().freeMemory() functions in java inbuilt class Runtime.

Output Bytes

The output bytes is considered to be a measure of how much space is required on the storage device for storing the cipher text. Thus, by getting the output bytes, we can tell the rate at which an encryption algorithm will use up the storage space.

4. EXPERIMENTAL RESULTS AND DISCUSSION

This section presents performance and comparision of the identified algorithms with respect to the various parameters mentioned in section 3.1. Experimental results for AES, DES, 3-DES and Blowfish are shown in Table 1.

By analyzing the data in Table 1, we noticed that for each of all the four algorithms, encryption time, decryption time and output byte is directly proportional to the file size. However, the time taken by AES and Blowfish to encrypt or decrypt a file is much smaller than the time taken by DES and 3-DES to encrypt or decrypt the same file. We noticed also that 3-DES has much smaller output byte compare to AES, Blowfish and DES algorithms. Also, in terms of memory usage, DES consumed more memory than other algorithms while AES consumed least amount of memory space.

Table 1: Comparison of AES, DES, 3-DES and Blowfish with respect to Encryption Time, Decryption Time, Memory Usage and Output Bytes.

Result for AES

File_Size	Encryption_Time (s)	Decryption_Time (s)	Memory_Usage (KB)	Output Byte
63KB	0.105	0.106	-1.414	64576
127KB	0.15	0.169	0.141	130656
255KB	0.251	0.301	0.102	261600
319KB	0.301	0.366	-6.406	326960
383KB	0.346	1.103	0.102	393056

Result for DES

File_Size	Encryption_Time (s)	Decryption_Time (s)	Memory_Usage (KB)	Output Byte
63KB	12.62	0.127	43.188	63560
127KB	51.775	0.207	76.648	128676
255KB	221.352	0.377	148.961	258773
319KB	344.118	0.484	191.844	333779
383KB	717.574	0.631	222.203	391402

Result for 3-DES

File_Size	Encryption_Time (s)	Decryption_Time (s)	Memory_Usage (KB)	Output Byte
63KB	15.189	0.6	8.484	47232

127KB	58.132	1.112	8.234	95872
255KB	225.729	2.315	8.836	191896
319KB	339.365	2.674	14.984	247360
383KB	732.337	3.437	24.07	291992

Result for Blowfish

File_Size	Encryption_Time (s)	Decryption_Time (s)	Memory_Usage (KB)	Output Byte
63KB	0.116	0.139	0.117	64576
127KB	0.2	0.179	0.102	130656
255KB	0.295	0.431	0.148	261592
319KB	0.471	0.417	0	326960
383KB	0.385	0.51	-0.102	393056

By analyzing Figures 4 and 5 , which shows time taken for encryption and decryption on various sizes of text files by the algorithms, it is shown that 3-DES took 50.4% and 64.6% of the total encryption and decryption time taken respectively compare to the time taken by AES , Blowfish and DES algorithms. AES algorithm consumes least time for encryption (0.04%) with a minor difference compare to Blowfish algorithm which took 0.05% of the total encryption time while DES consumes least amount of decryption time (11.6%) with a minor difference compare to Blowfish algorithm (10.9%).

Figure 6 shows the size of output byte for each algorithm used in the experiment. It is noticed that 3-DES has least size of output byte on various sizes of text files by using 19.9% of the total space used by the algorithms. However, there is a slight difference in the size of output byte for both AES (26.72%) , Blowfish (26.71%) and DES (26.70%).

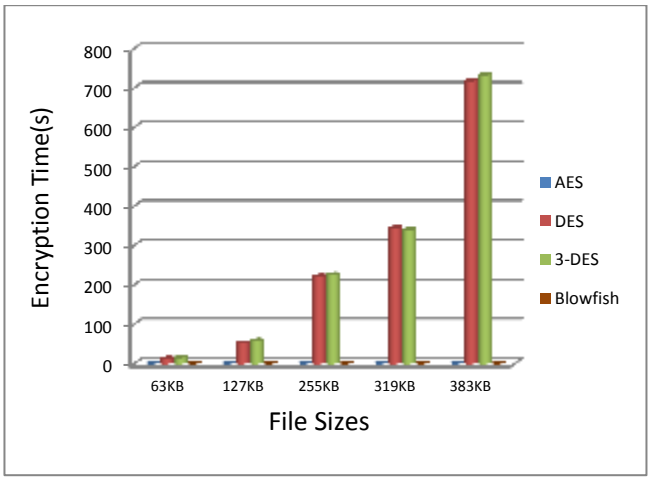

Figure 4: Comparsion of Encryption time

As shown in figure 4 above, encryption time for each of the algorithm increases as the text file increases with AES and Blowfish algorithms consuming least amout of time in encrypting the text files. Thus with respect to encryption time, AES outperforms other algorithm with a slight difference compare to Blowfish algorithm.

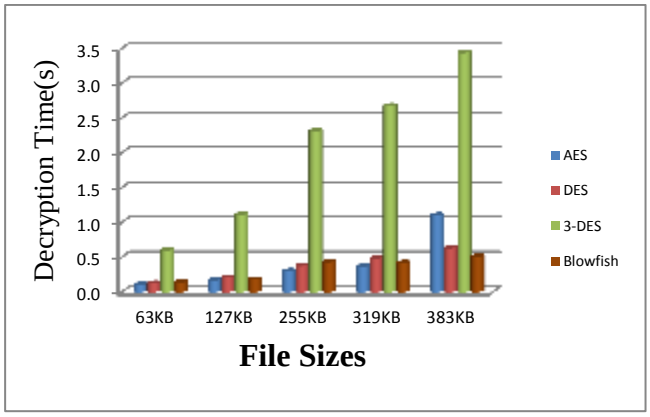

Figure 5: Comparison of Decryption Time

Figure 5 shows the decryption time of each of the algorithm on various sizes of data. It was shown that 3-DES took longer time to decrypt a data file as compare to other algorithms. Thus, 3-DES cannot be easily broken into since it takes time to decrypt a particular message. However, in an environment where response time is of great importance, 3-DES performs poorly.

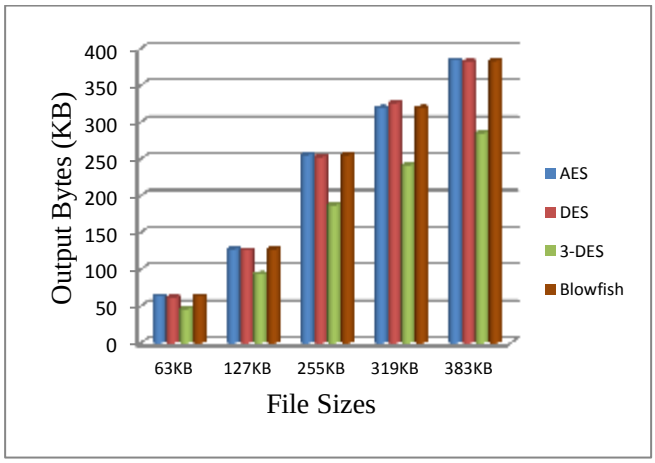

Figure 6: Comparison of Output Byte

As shown in figure 6, AES and blowfish consume much storage space as compare to other algorithms.

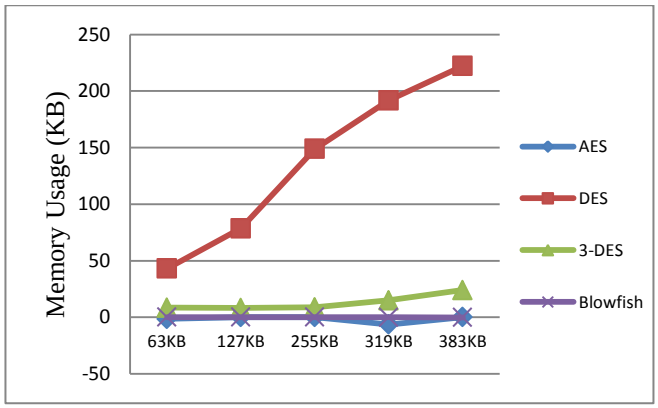

Figure 7: Comparison of Memory Usage

It can be seen from figure 6 that DES utilized more memory than other algorithms while AES consumes least amount of memory space. As opposed to the positive values displayed by DES and 3-DES, AES and Blowfish displayed negative values along the line. This is due to the fact that the memory allocated before encryption was not totally used up by these algorithms at some point after encryption. Therefore, based on the function used to compute the memory usage which is stated below, End < Start, hence a negative value is gotten as the result.

Start = Runtime.getRuntime().totalMemory() – Runtime.getRuntime().freeMemory()
End = Runtime.getRuntime().totalMemory() – Runtime.getRuntime().freeMemory()
memoryUsed = End – Start

5. CONCLUSION

Encryption algorithms play an important role in communication where encryption time, decryption time, memory usages, and output bytes are the major issue of concern. Performance evaluation of the selected encryption algorithms (AES, DES, 3DES and Blowfish) are done and from the experimental result obtained, it was concluded that AES consumes the least encryption time while DES consumes least decryption time. 3-DES has least size of output byte while there is a minor difference in encryption and decryption time for both DES and 3-DES. In terms of memory usage, it is concluded that AES consumes the least amount of memory size during encryption.

REFERENCES

[1] Jeeva, A., Palanisamy V., Kanagaram K.. "Comparative analysis of performance efficiency and security measures of some encryption algorithms". *International Journal of Engineering Research and Applications (IJERA*), ISSN: 2248-9622, Vol. 2 Issue 03, Page No. (3033-3037) May-Jun., 2012.

[2] Marshall, D. A., and Harold J. P. *" Cryptography". Tutorial: Computer and Network Security*, IEEE Computer Society Press, Los Alamitos, Calif., 1987.

[3] Diaasalama A., HatemMohamadAbdual K., Mohly M. H. "Evaluating the performance of symmetric encyrption algorithms". *Internatiional Journal of Network Security, Vol. 10 Issue 0*3, Page No. (213-219). May, 2010

[4] Diaasalama, Abdul K., MohiyHadhoud. "Studying the effect of most common encryption algorithms". *International Arab Journal of e-technology, Vol. 2 Issue 0*1, Page No (12-20), January, 2011.

[5] Badlawala, M., Ansari, F., Shaikh, I. and Chaskar, N. "Image Steganography with Double Stegging by PVD and AES Encryption". *IJSRD - International Journal for Scientific Research & Development*| Vol. 4, Issue 02,| ISSN (online): 2321-0613, 2016.

[6] Al-Tamimi, A. "Performance analysis of data encryption algorithms". Feb. 2014. http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/

[7] Sachin and Jeevan. "Performance Analysis of Data Encryption Algorithms". *International Journal of Scientific Research in Network Security and Communication.* Vol. 3 issue 1. Page N0. (2321-3256), Feb., 2015.

[8] Shivlal Mewada, Sharma Pradeep, Gautam S.S., "Classification of Efficient Symmetric Key Cryptography Algorithms", *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 14, No. 2, pp (105-110), Feb 2016

[9] Yousif, Y. E., Babiker, A., Mustafa, A., Mohammed, G. "Review on Comparative Study of Various Cryptography Algorithm". *International Journal of Advanced Research in Computer Science and Software Engineering*. Volume 5, Issue 4, ISSN: 2277 128X, 2015.

[10] Olusegun O. Omitola et al.,"Performance Evaluation of Common Encryption Algorithms for Throughput and Energy Consumption of a Wireless System". *J. of Advancement in Engineering and Technology*. Vol-3, Issue-1. 2015, DOI: 10.15297/JAET.V3I1.05

[11] V. Kapoor, "A New Cryptography Algorithm with an Integrated Scheme to Improve Data Security", *International Journal of Scientific Research in Network Security and Communication*, Volume-01, Issue-02, Page No (39-46), May -Jun 2013

Authors Profile

Dr. S. O. Okolie is a Senior Lecturer in Computer Science Department, Babcock University, Ilishan-Remo, Ogun State; Nigeria. He holds a Ph.D. in Computer Science and his research I Interests are in the area of Computation and Data Structures. He is a member of Nigeria Computer Society (NCS)

Mrs. B. T. Adetoba, a Postgraduate student at Babcock University, Ilishan, Ogun State, Nigeria. She has Bachelor of Science and Master of Science in Computer Science from Obafemi Awolowo University and University of Lagos, Nigeria in year 1994 and 1999. She is currently pursuing Ph.D. and currently working as a Lecturer in the Department of Computer Science, Yaba College of Technology, Lagos, Nigeria since 2007. She is a member of CPN (Computer Professionals of Nigeria) and NCS (Nigeria Computer Society).

