ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

Performance Evaluation of Symmetric Encryption Algorithms for Information Security

Madhumita Panda
Assistant Professor in Computer Science.
SUIIT, Sambalpur University.
Odisha, India

Abstract: In today's internet era, with the fast progression of digital data exchange in electronic way, securing information has become a challenge. Cryptography plays an important role in information security systems. It is a process of making information indecipherable to an unauthorized person. There are various cryptographic algorithms that can be used. Although security is important, but on the other side these algorithms consume a significant amount of computing resources such as CPU time, memory and computation time. This paper provides an analysis and comparison of some symmetric key cryptographic ciphers (DES, Triple DES, AES, Blowfish) on the basis of encryption and decryption time with text files and image files using Java as the programming language.

Keywords: Encryption, Decryption, DES, 3DES, AES, Blowfish.

I. INTRODUCTION

Security plays an important role in our life as well as in the area of networking for transmission of data from one device to other. Cryptography provides a method for securing and authenticating the transmission of information across insecure communication channels. It enables us to store sensitive information or transmit it over insecure communication networks so that unauthorized persons cannot read it. [1]. The main goal of cryptography is to keep the data secure from unauthorized access [2]. In cryptography, original message is called plaintext. The method of scrambling the plaintext in such a way that hides its substance is called encryption. Encrypting plaintext makes the information in unreadable form called cipher text. The process of converting cipher text to its original information is called decryption. A system that performs encryption and decryption is called cryptosystem. On the basis of key used, cipher algorithms are classified as asymmetric key algorithms, in which encryption and decryption is done by two different keys and symmetric key algorithms, where the same key is used for encryption and decryption [3]. Symmetric key algorithms are much faster computationally than asymmetric algorithms as the encryption process is less complicated. Examples are AES, 3DES etc. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [4]. We here focus only on symmetric cryptography due to the assumption that symmetric cryptography has a higher effectiveness and require less energy consumption, in contrast to asymmetric key cryptography. The main objective of this paper is to analyze time taken for encryption and decryption by various symmetric key cryptographic algorithms for different sizes of text files and image files.

II. CRYPTOGRAPHIC ALGORITHMS

This section provides information about the various symmetric key cryptographic algorithms to be analyzed for performance evaluation, to select the best algorithm to provide security for data. Symmetric key cryptographic ciphers come in two varieties, stream ciphers and block ciphers. Stream ciphers works on bitwise on data while block ciphers performs encryption or decryption on fixed size block of data. The plaintext is not always in multiple of block size, therefore padding bits are needed to compensate partially filled block. A stream cipher can be seen as a block cipher with a block length of 1 bit.

There are different symmetric cryptographic algorithms in the literature [5] [6]. Out of them, the algorithms listed in the Table 1 are selected for detailed study in this paper.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

TABLE 1.
CRYPTOGRAPHIC ALGORITHMS INFORMATION

Scheme	Algorithm Type	Structure	Contributor	Key Length	Rounds	Block Size
DES	Symmetric	Balanced Feistel network	IBM75	56 bits	16	64 bits
3DES	Symmetric	Feistel network	IBM78	168, 112 or 56 bits	48	64 bits
AES	Symmetric	Substitution-permutation network	Rijindael	128, 192, 256 bits	10 or 12 or 14	128 bits
BLOWFISH	Symmetric	Feistel network	Bruce Schneier	32-448 bits	16	64 bits

III. RELATED WORKS

This section provides the information and results which are obtained from the numerous sources. Cryptographic algorithms have been compared with each other for performance evaluation on basis of throughput Memory utilization, energy consumption, attacks, encryption time, decryption time etc. This paper [7] provides evaluation of six of the most common encryption algorithms namely: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. A comparison has been conducted on these 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. Several points has been concluded from the experimental results. Firstly there was no significant difference when the results were displayed either in hexadecimal base encoding or in base 64 encoding. Secondly in the case of changing packet size, it was concluded that Blowfish had better performance than other common encryption algorithms used, followed by RC6. Thirdly authors have concluded that, 3DES still has low performance compared to algorithm DES. Fourthly they found out that RC2, has disadvantage over all other algorithms in terms of time consumption. Fifthly it was found that AES has better performance than RC2, DES, and 3DES. In the case of audio and video files they found the result as the same as in text and document. Finally, in the case of changing key size, it was seen that higher key size leads to clear change in the battery and time consumption.

The paper [8] provides evaluation of both symmetric (AES, DES, Blowfish) as well as asymmetric (RSA) cryptographic algorithms by taking different types of files like binary, text and image files. A comparison has been conducted for these encryption algorithms using evaluation parameters such as encryption time, decryption time and throughput. From the presented simulation results, it was concluded that AES has better performance than other algorithms in terms of both throughput and encryption-decryption time.

In this paper [9], the performance of three Symmetric Key based algorithms-AES, Blowfish and Salsa20 has been evaluated based on execution time, memory required for implementation and throughput across two different operating systems. Based on the simulation results, it was concluded that AES and Salsa20 are preferred over Blowfish for plain text data encryption.

In [10] the author compared AES and RC4 algorithm and the performance metrics were encryption throughput, CPU work load, memory utilization, and key size variation and encryption and decryption time. Results show that the RC4 is fast and energy saving for encryption and decryption. RC4 proved to be better than AES for larger size data.

In [11] author compared AES and DES algorithms on image file, MATLAB software platform was used for implementation of these two cipher algorithms. AES took less encryption and decryption time than DES. In [4] the author compared cipher algorithms (AES, DES, Blowfish) for different cipher block modes (ECB, CBC, CFB, OFB) on different file sizes varying from 3kb to 203kb. Blowfish algorithm yield better performance for all block cipher modes that were tested and OFB block mode gives better performance than other block modes.

In [12] the author compared cipher algorithms (AES, DES, 3-DES and Blowfish) for varying file size and compared the encryption time on two different machines Pentium-4, 2.4 GHz and Pentium-II 266 MHz in EBC and CFB Mode. The author concluded that Blowfish is fastest followed by DES and Triple DES and CFB takes more time than ECB cipher block mode.

From the above related works, it is realized that none of the work has been carried out on the performance of various symmetric algorithms on different type of files. The main objective of this paper is to analyze the time taken for encryption and decryption by various symmetric cryptographic algorithms on different sizes of text files and image files using JAVA as the programming language.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

IV. Evaluation Parameters

In this paper, analysis is done with following metrics under which the cryptosystems can be compared.

Encryption time- The time required to convert plaintext to cipher text is encryption time. Encryption time depends upon key size, plaintext block size and mode. In our experiment we have measured encryption time in milliseconds. Encryption time impacts performance of the system. This time must be less making the system fast and responsive.

Decryption time- The time to recover plaintext from cipher text is called decryption time. The decryption time is desired to be less similar to encryption time to make system responsive and fast. Decryption time impacts performance of system. In our experiment, we have measured decryption time is milliseconds.

V. Simulation Results

Performance of encryption algorithm is evaluated considering the following system configuration.

1. **Software Speciation**: Experimental evaluation on Geany with Java Development Kit 8, Windows 8 Pro64 bit Operating System.
2. **Hardware Speciation**: All the algorithms are tested on Intel® Core™ i5 3337U (1.80 GHz) fourth generation processor with 4GB of RAM with 1 TB-HDD

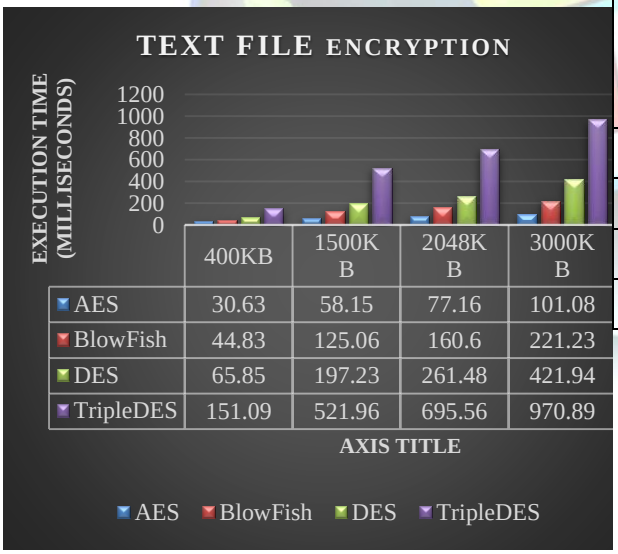

Fig.1 Encryption Time of different Algorithms for Text Files

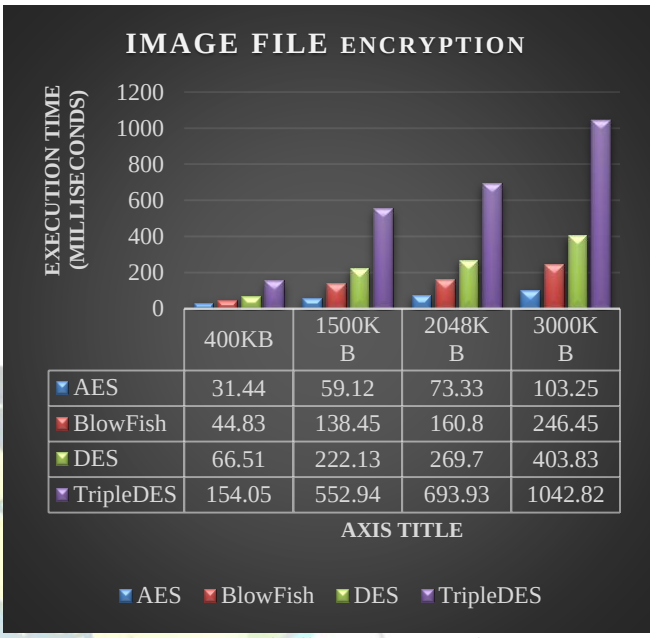

Fig.2. Encryption Time of different Algorithms for Image Files

Text File Size	ALGORITHMS							
	AES		BLOWFISH		DES		T_DES	
	Average Encryption Time (MS)	Average Decryption Time (MS)	Average Encryption Time (MS)	Average Decryption Time (MS)	Average Encryption Time (MS)	Average Decryption Time (MS)	Average Encryption Time (MS)	Average Decryption Time (MS)
400 kb	30.63	28.41	44.83	44.54	65.855	66.67	151.09	146.64
1500 kb	58.15	60.79	125.06	136.90	197.23	206.37	521.96	505.81
2048 kb	77.16	81.93	160.60	166.23	261.48	274.53	695.56	680.23
3000 kb	101.08	109.69	221.23	238.31	421.94	460.06	970.89	985.32

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

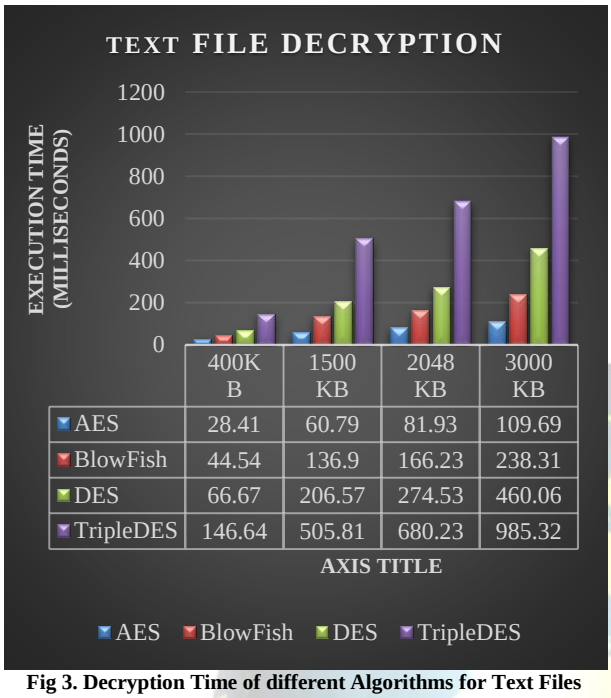

Fig 3. Decryption Time of different Algorithms for Text Files

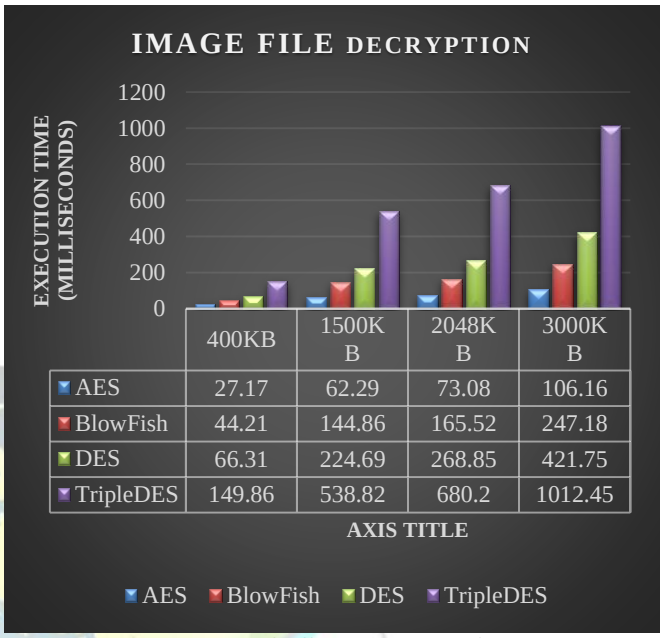

Fig 4. Decryption Time of different Algorithms for Image Files

Image File Size	ALGORITHMS							
	AES		BLOWFISH		DES		T_DES	
	Average Encryption Time (MS)	Average Decryption Time (MS)	Average Encryption Time (MS)	Average Decryption Time (MS)	Average Encryption Time (MS)	Average Decryption Time (MS)	Average Encryption Time (MS)	Average Decryption Time (MS)
400 kb	31.44	27.17	44.83	44.21	66.51	66.31	154.05	149.86
1500 kb	59.12	62.29	138.45	144.86	222.13	224.69	552.94	538.82
2048 kb	73.33	73.08	160.80	165.52	269.07	268.85	693.93	680.20
3000 kb	103.25	106.16	246.45	247.18	403.83	421.75	1042.82	1012.45

VI. CONCLUSION AND FUTURE WORK

We have done the analysis of execution time of different algorithms in terms of Encryption time and Decryption time with different sizes of text files and image files. The results shows that AES algorithm is the best and takes less time to encrypt and decrypt a file (Text or Image) as compared to other algorithms (Blowfish, DES and Triple DES). After AES, Blowfish algorithm performs better as compared to the DES and Triple DES. From this analysis we also conclude that Triple DES algorithm is worst as compare to the other algorithms as it takes a lot of time to encrypt as well as decrypt a data. Also we conclude that the image file takes more encryption and decryption time as compared to the text files. The future work can be done to compare performance of these algorithms on audio and video files. Also we can do the same comparison on different operating systems.

REFERENCES

[1]. P.Karthigaikumar, Soumiya Rasheed" Simulation of Image Encryption using AES Algorithm" IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011.

[2]. Diaa Salama Abd Elminaam, Hatem Mohamad Abdual Kader, Mohiy Mohamed Hadhoud, "Evalution the Performance of Symmetric Encryption Algorithms", International journal of network security vol.10,No.3,pp,216-222,May 2010.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 11, November 2017

[3]. Jonathan Knudsen, Java Cryptography, 2nd Edition, O'Reilly, 2011.

[4]. Hardjono, "Security In Wireless LANS And MANS,"Artech House Publishers 2005.

[5]. Jonathan Knudsen, Java Cryptography, 2nd Edition, O'Reilly, 2011.

[6]. Behrouz A. Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, 2nd Edition, Tata McGraw Hill, 2012.

[7]. Elminaam, Diaa Salama Abd, Hatem Mohamed Abdual-Kader, and Mohiy Mohamed Hadhoud. "Evaluating the performance of symmetric encryption algorithms." IJ Network Security 10.3 (2010): 216-222.

[8]. Panda, Madhumita. "Performance analysis of encryption algorithms for security." Signal Processing, Communication, Power and Embedded System (SCOPES), 2016 International Conference on. IEEE, 2016.

[9]. Panda, Madhumita, and Atul Nag. "Plain Text Encryption Using AES, DES and SALSA20 by Java Based Bouncy Castle API on Windows and Linux." Advances in Computing and Communication Engineering (ICACCE), 2015 Second International Conference on. IEEE, 2015.

[10]. Nidhi Singhal and J.P.S.Raina, "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, Vol 2, Issue 6, July-Aug,2011, pp.177-181.

[11]. S. Soni, H. Agrawal, M. Sharma, "Analysis and comparison between AES and DES Cryptographic Algorithm", International Journal of Engineering and Innovative Technology, Vol 2, Issue 6,December 2012, pp.362-365.

[12]. Aamer Nadeem, Dr M. Younus Javed, "A Performance Comparison of Data Encryption Algorithms", First International Conference on IEEE Information and Communication Technologies (ICICT), Vol 1, Issue 6, 27-28 Aug. 2005, pp 84-89.