A Comprehensive Evaluation of Symmetric Cryptographic Algorithms on Windows and Ubuntu using Java

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

Abstract
Data security has been a major concern in the today's information technology era. Cryptography plays an important role in information security system against malicious attacks. It is a process of making information indecipherable to an unauthorized person. Cryptographic algorithms are classified as Symmetric and Asymmetric. With Symmetric encryption, the same key is used to cipher and decipher data whereas with Asymmetric algorithms, we have different key for encryption and decryption. Symmetric algorithms tend to be less complicated than Asymmetric and hence are more widely used. Although Cryptographic algorithms play a main role in information security systems, on the other side, these algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. 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 different sizes text files on two different operating system using Java as the programming language.

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

1. INTRODUCTION

Cryptography is an effective way for protecting hypersensitive details. It is a process of making information indecipherable to an unauthorized person hence, providing confidentiality to genuine users Cryptography means "secret writing" which is the science and art of transforming messages to make them secure and immune to attacks by unauthorized user. The original data/message, before being transformed is called cipher text. An encryption is a process to transform the plaintext into cipher text and decryption transforms the cipher text back into plaintext. The sender uses an encryption algorithm and the receiver uses a decryption algorithm. Thus, encryption and decryption help to secure transmission of the message and protect the message from unauthorized users [1].Many encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. These algorithms are much faster than asymmetric algorithms in terms of computation as the encryption process is less complicated. Also the memory requirement of Symmetric algorithm is lesser as compared to Asymmetric. [2]These algorithms can be directly implemented on hardware easily. The weakness of symmetric algorithms is in sharing of symmetric key between sender and receiver. In Asymmetric algorithms, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption. The key exchange is not a problem in this approach but Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [3].

This paper provides details of the performance analysis of some symmetric key algorithms using different sizes of text files on two different platforms that are WINDOWS and UBUNTU, using JAVA as the programming language.

II. ALGORITHMS IN OUR EXPERIMENT

A. Advanced Encryption Standard (AES)

AES (Advanced Encryption Standard) is a symmetric block encryption standard recommended by NIST (National Institute of Standards and Technology) [4] [5] is used for securing information. It encrypts 128 bit block size with 128/192/256 bit key for 10/12/14 rounds. The complete specification and the above structure of AES encryption scheme can be found in [6]. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices [7]. Also, AES has been carefully tested for many security applications [8], [9].

B. Blowfish

Blowfish was designed in 1994 by Bruce Schneier,it works on 64-bit units with key lengths from 32-bits up to 448-bits [10] . This standard has a simple structure,which is easy to implement and use. It is unpatented, license-free, and is available free for all uses. Blowfish is the better than other algorithms in throughput and power consumption [11] [12].

C.DES

DES (Data Encryption Standard) is a symmetric block encryption standard to be recommended by NIST [13]. The DES algorithm is the most broadly used encryption algorithm in the world. The same algorithm and key are used for encryption and decryption, with minor differences. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block [14] [15].

D.3DES

Triple Data Encryption Algorithm (TDEA or Triple DEA) is a symmetric-key block cipher standard which is similar to DES method but increase encryption level 3 times than DES [16]. As a result this is slower than other block cipher methods. The block size of 3DES is 64 bit with 192 bits key size [17] [18].

III. EXPERIMENTAL METHODOLOGY AND ENVIRONMENT

a). 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.

b) Evaluation Platforms

The encryption algorithms are evaluated considering the following system configuration.
1. Software Specification: Experimental evaluation on Different Encryption algorithm with Java Development Kit 8, Ubuntu Mate and Windows 8 64bit Operating System.

2. Hardware Specification: All the algorithms are tested on Intel(R) Core(TM) i3-6100T CPU @ 3.20GHz processor with 4GBof RAM and 1TB HDD.

IV. EXPERIMENTAL RESULTS AND ANALYSIS:

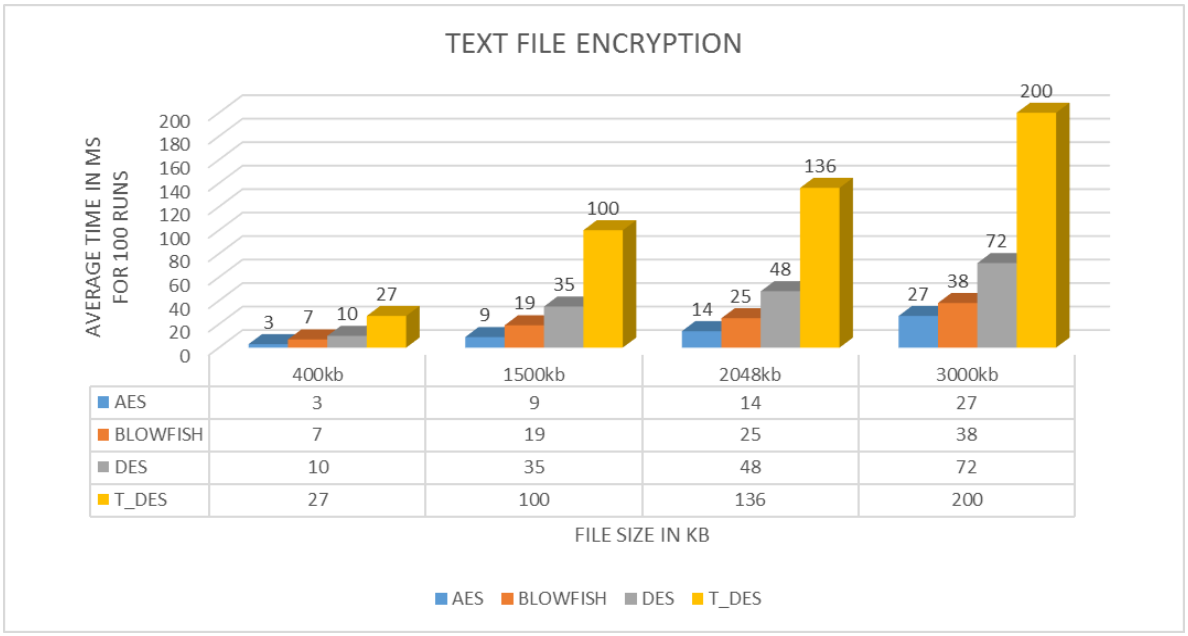

Fig.1 Encryption Time of Different Algorithms for Text Files in Ubuntu OS

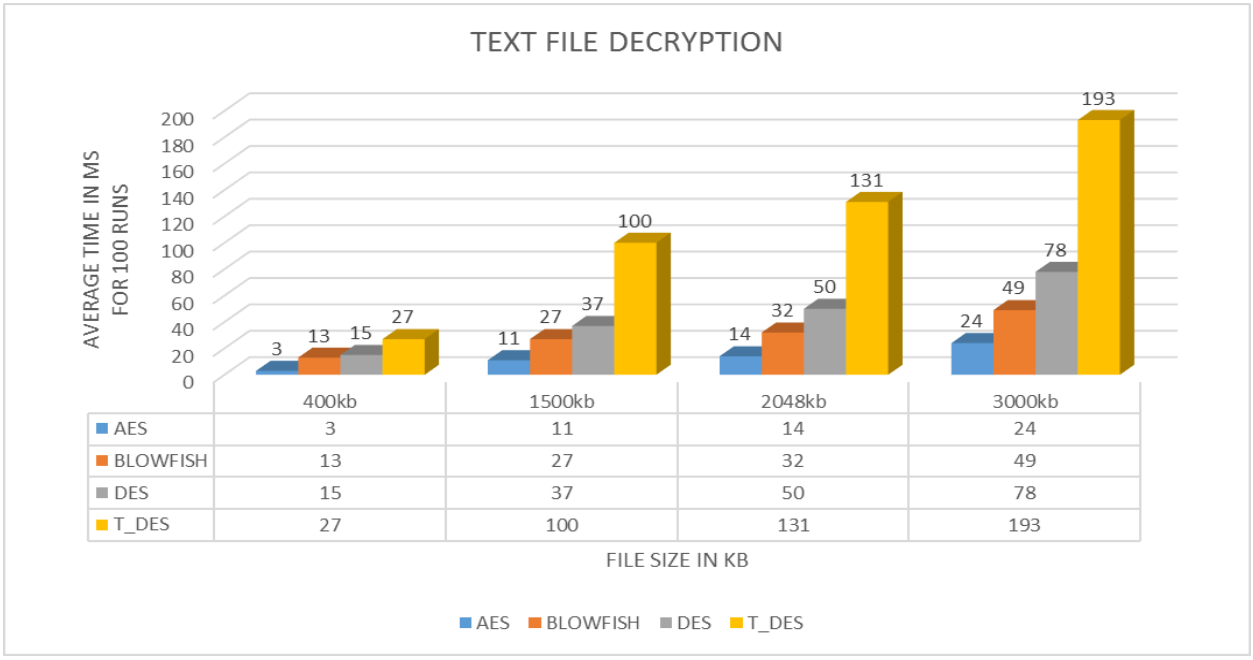

Fig.2 Decryption Time of Different Algorithms for Text Files in Ubuntu OS

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)
400kb	3	3	7	13	10	15	27	27
1500kb	9	11	19	27	35	37	100	100
2048kb	14	14	25	32	48	50	136	131
3000kb	27	24	38	49	72	78	200	193

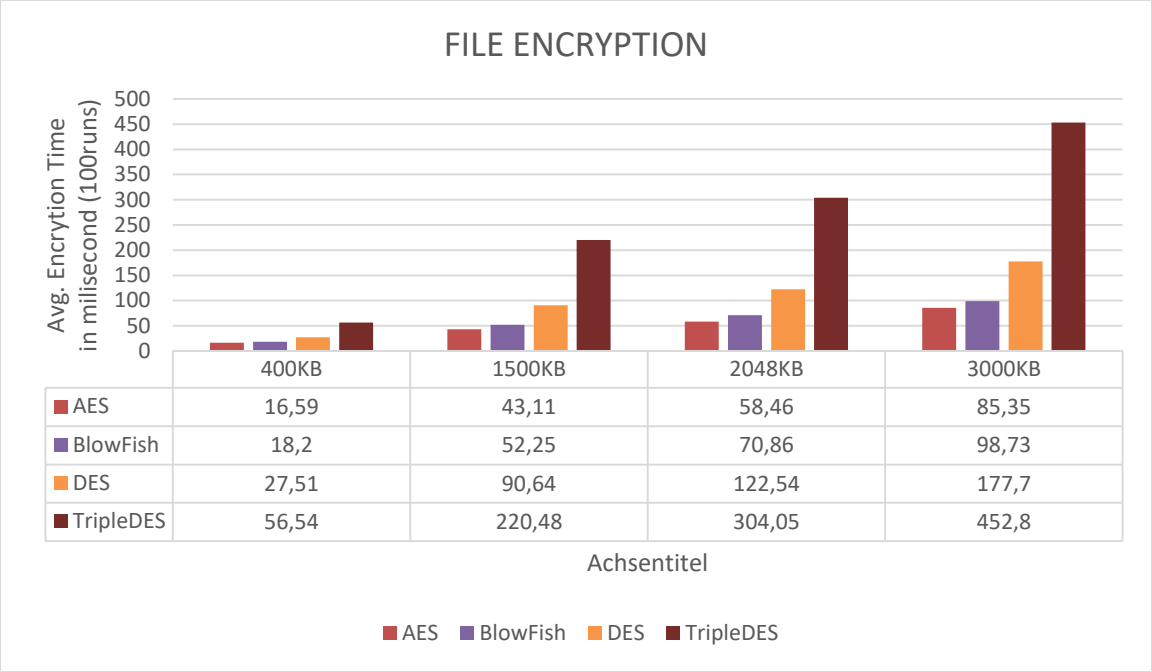

Fig.3 Encryption Time of Different Algorithms for Text Files in Windows OS

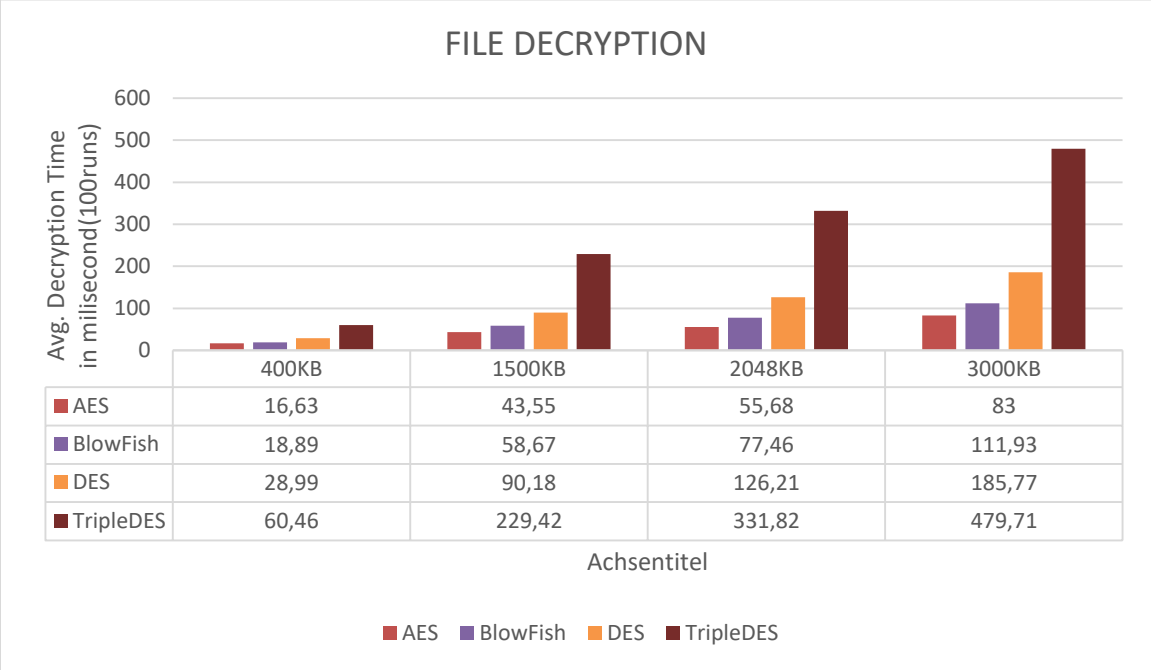

Fig-4: Decryption Time of Different Algorithm for Text Files in Windows OS

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)
400kb	16.59	16.63	18.2	18.89	27.51	28.99	56.54	60.46
1500kb	43.11	43.55	52.25	58.67	90.64	90.18	220.48	229.42
2048kb	58.46	55.68	70.86	77.46	122.54	126.21	304.05	331.82
3000kb	85.35	83	98.73	111.93	177.7	185.77	452.8	479.71

V. 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 . The results shows that AES algorithm is the best and takes less time to encrypt and decrypt a file 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 in terms of Operating system, we see that Ubuntu operating system gives much better results compared to Windows. The future work can be done to compare performance of these algorithms on image, audio and video files on different operating systems.

References

[1]. Mudassar Aslam, Christian Gehrmann, Mats Bj¨orkman, “Security and Trust Preserving VM Migrations in Public Clouds”, Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference, Liverpool, 25-27 June 2012, pp 869 - 876, Print ISBN: 978-1-4673-2172-3, DOI: 10.1109 /TrustCom.2012.256.

[2]. Ketu File white papers, “Symmetric vs Asymmetric Encryption”, a division of Midwest Research Corporation.

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

[4] Vineet Kumar Singh, Dr. Maitreyee Dutta “ANALYZING CRYPTOGRAPHIC ALGORITHMS FOR SECURE CLOUD NETWORK” International Journal of advanced studies in Computer Science and Engineering IJASCSE Volume 3, Issue 6, 2014.

[5] Dr. Prerna Mahajan & Abhishek Sachdeva , “A Study of Encryption Algorithms AES, DES and RSA for Security ”, Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350.

[6] J. Daemen and V.Rijmen, “AES Proposal: Rijndael”,1999.

[7] K. Naik, D. S.L. Wei, Software Implementation Strategies for Power-Conscious Systems,” Mobile Networks and Applications - 6, 291-305, 2001.

[8] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309.

[9] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard."D r. Dobb's Journal, March 2001,PP. 137-139.

[10] Schneier, Bruce. "Description of a new variablelength key, 64-bit block cipher (Blowfish)." Fast Software Encryption. Springer Berlin Heidelberg, 1994, pp. 191-204.

[11] Mr. Gurjeevan Singh, , Mr. Ashwani Singla and Mr. K S Sandha “ Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System” International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.

[12] Manpreet Kaur, Rajbir Singh “Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing”, International Journal of Computer Applications (0975 – 8887) Volume 70– No.18, May 2013.

[13] Vineet Kumar Singh, Dr. Maitreyee Dutta “ANALYZING CRYPTOGRAPHIC ALGORITHMS FOR SECURE CLOUD NETWORK” International Journal of advanced studies in Computer Science and Engineering IJASCSE Volume 3, Issue 6, 2014.

[14] http://www.vocal.com/cryptography/rc4-encryption-algoritm/

[15] Prashanti.G, Deepthi.S & Sandhya Rani.K. ”A Novel Approach for Data Encryption Standard Algorithm”. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249- 8958, Volume-2, Issue-5, June 2013, pp. 264.

[16] https://en.wikipedia.org

[17] Randeep Kaur, Supriya Kinger “Analysis of Security Algorithms in Cloud Computing”, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 3, March 2014, ISSN 2319 – 4847

[18] Nagesh M.Wankhade, Kiran A. Sahare, Prof. Vaishali G. Bhujade, “SECURE CLOUD SIMULATION USING TRIPLE DES”, International Journal of Research in Advent Technology, Volume 2, Issue 1, January 2014