# Text And Image Encryption Decryption Using Symmetric Key Algorithms On Different Platforms

**Madhumita Panda**

**Abstract**: In today's era we need to secure information stored in our computer or transmitted through internet against various attacks. Cryptography is an important tool to protect our information against malicious attacks of today. There are several cryptographic algorithms available to secured our information. Each algorithm has its own strong and weak points. 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 and also image files on two different operating system using Java as the programming language.

**Keywords**: Symmetric Key algorithms AES, Blowfish, DES, 3DES, Encryption, Decryption.

## 1. INTRODUCTION

Cryptography means "secret writing" which is the science and art of transforming messages to make them secure and immune to attacks by unauthorized user. Cryptographic algorithms falls into two categories: symmetric and asymmetric. In symmetric or also called as private key cryptography only one key is used to encrypt and decrypt the data. But in asymmetric which is also called as public key cryptography, two separate keys (public and private) are used. Public key is used for encryption while private key is used for decryption. Symmetric Key algorithms are less complex ,require less memory and are also much faster, but the main disadvantage is in sharing the key between the sender and the receiver. The key exchange is not a problem in asymmetric but asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [1]. In this paper we have compared symmetric key algorithms(AES, Blowfish, DES, 3DES) based on encryption and decryption time using different sizes of text as well as image files on two different platforms WINDOWS and UBUNTU, using JAVA as the programming language The rest of the paper is organized as follows: Section 2 gives the related works. The experimental methodology and environment used for comparing all the algorithms is discussed briefly in section 3, whereas section 4 shows the simulations results and analysis .Finally, section 5 concludes the paper with some future scope of research work.

## 2. RELATED WORKS

To give more prospective about the performance of the compared algorithms, this section discusses the results obtained from other resources The paper[2] provides evaluation of AES, DES, 3DES, RC2, Blowfish, and RC6 on different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption and decryption speed. Experimental results are given at the end to demonstrate the effectiveness of each algorithm.

- *Madhumita Panda; Assistant Professor, Computer Science, SUIIT, Sambalpur University, Odisha, India*

In paper[3], the authors have implemented and analyzed in detail the cost and performance of DES, 3DES, AES, RSA and blowfish to show an overall performance analysis. The paper[4], provides evaluation of both symmetric (AES, DES, Blowfish) as well as asymmetric (RSA) cryptographic algorithms by taking Binary, text and image files using evaluation parameters like encryption time, decryption time and throughput. Simulation results are given at the end to demonstrate the effectiveness of each. In the paper[5], the authors review Symmetric and Asymmetric algorithms but emphasis has been given on Symmetric Algorithms for security consideration on which one should be used for Cloud based applications and services that require data and link encryption. The paper[6] discusses AES and DES and their comparison on basis of avalanche effect, simulation time and memory required using MATLAB software. As seen from the above, none of the work has been done on comparing symmetric algorithms on two different operating systems. So in this paper, we compare some commonly used symmetric algorithms(DES, Triple DES, AES, Blowfish)by taking different sizes of text and image files on Windows and Ubuntu using java as a programming language.

## 3. EXPERIMENTAL METHODOLOGY AND ENVIRONMENT

### a).Evaluation Parameters

In this paper, analysis is done on the following metrics.

**Encryption time**- It's the time taken to convert a plain text to cipher text.
**Decryption time**- It's the time required to recover the plain text from cipher text.
Algorithms must have less encryption and decryption time to make the system fast and responsive.
.

### b) Evaluation Platforms

The algorithms are evaluated considering the following system configuration.
**1. Software Specification:** Experimental evaluation is done 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.

## 4. SIMULATIONS RESULTS AND ANALYSIS

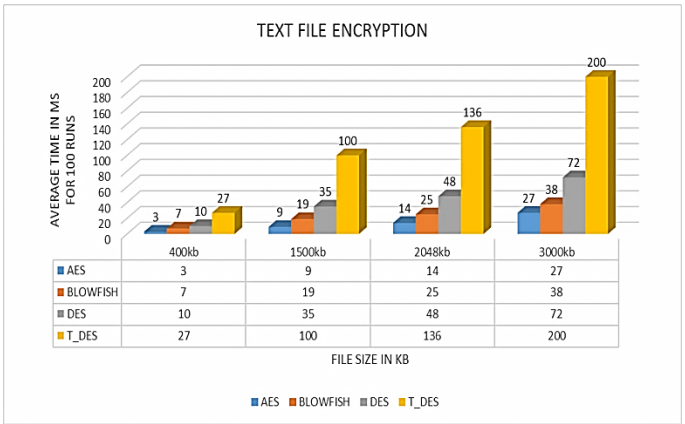


*Fig.1 Encryption Time of Different Algorithms for Text Files in Ubuntu OS*

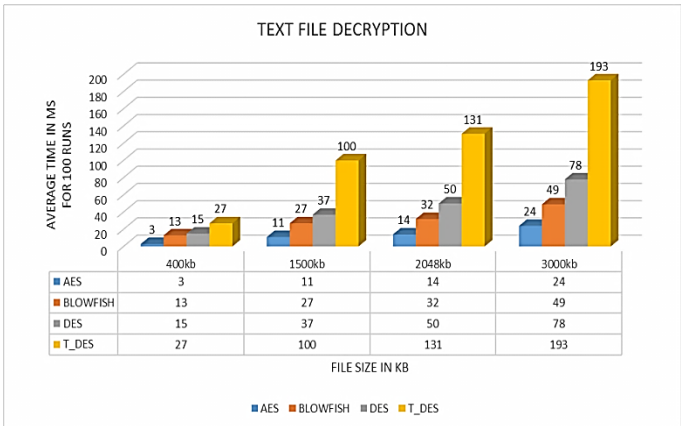


*Fig.2 Decryption Time of Different Algorithms for Text Files in Ubuntu OS*

| 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 |

*Table.1.Comparision Summary of Text Files Encryption Decryption(Ubuntu OS)*

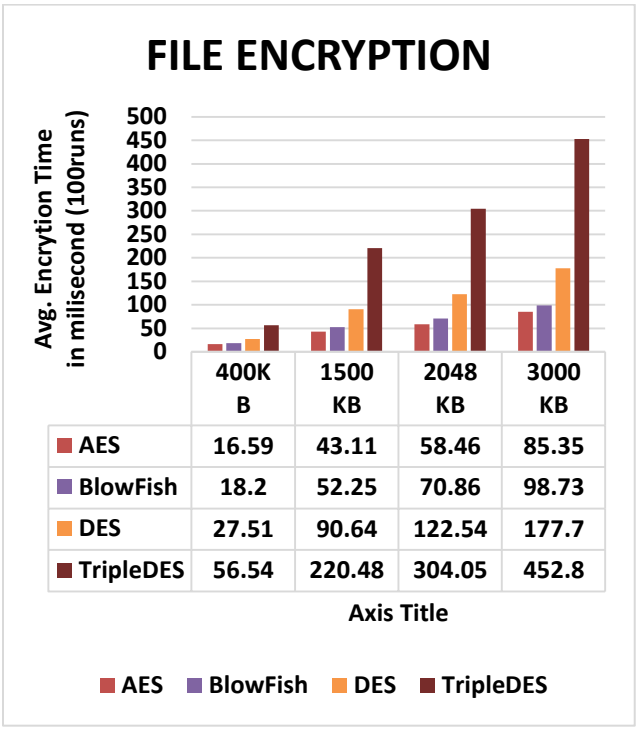


*Fig.3 Encryption Time of Different Algorithms for Text Files in Windows OS*

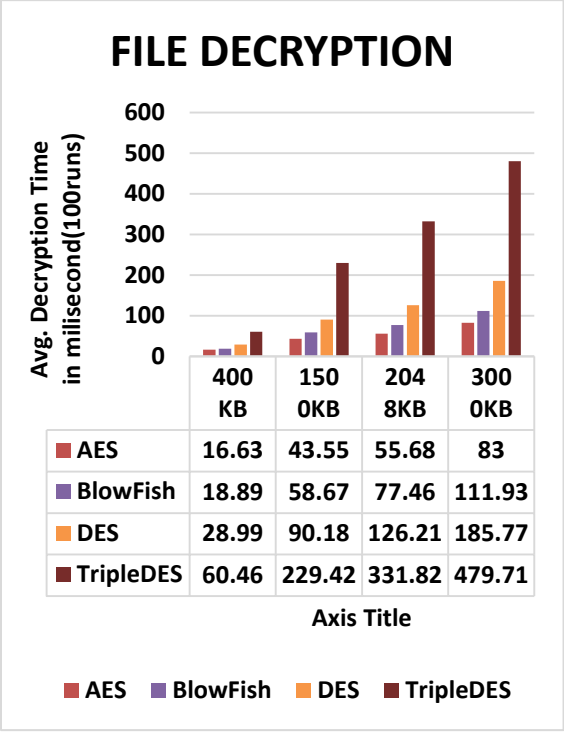


*Fig-4 Decryption Time of Different Algorithms for Text Files in Windows OS*

| 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 |

***Table.2.Comparision Summary of Text Files Encryption Decryption(Windows OS)***

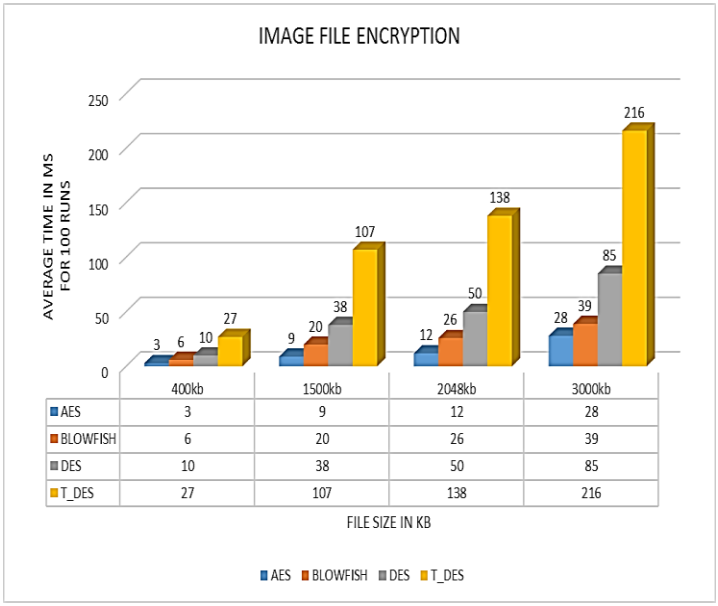


***Fig.5 Encryption Time of Different Algorithms for Image Files in Ubuntu OS***

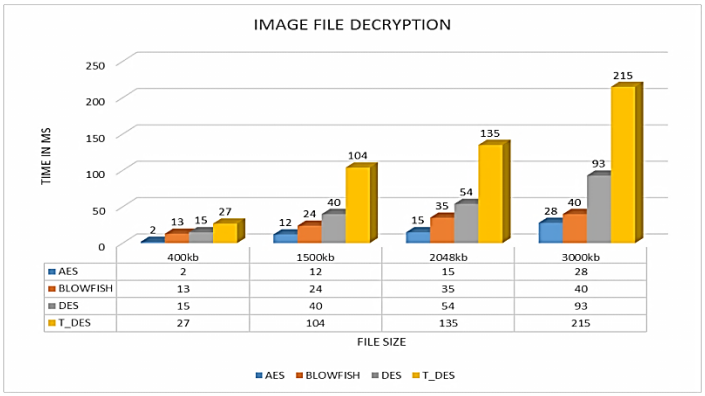


***Fig.6 Decryption Time of Different Algorithms for Image Files in Ubuntu OS***

| 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) |
| 400kb | 3 | 2 | 6 | 13 | 10 | 15 | 27 | 27 |
| 1500kb | 9 | 12 | 20 | 24 | 38 | 40 | 107 | 104 |
| 2048kb | 12 | 15 | 26 | 35 | 50 | 54 | 138 | 135 |
| 3000kb | 28 | 28 | 39 | 40 | 85 | 93 | 216 | 215 |

***Table.3.Comparision Summary of Image Files Encryption Decryption(Ubuntu OS)***

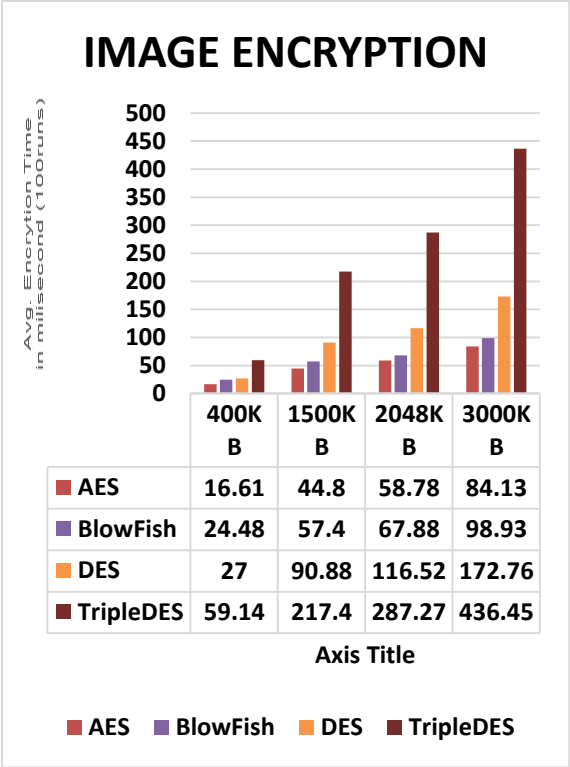


***Fig.7 Encryption Time of Different Algorithms for Image Files in Windows OS***

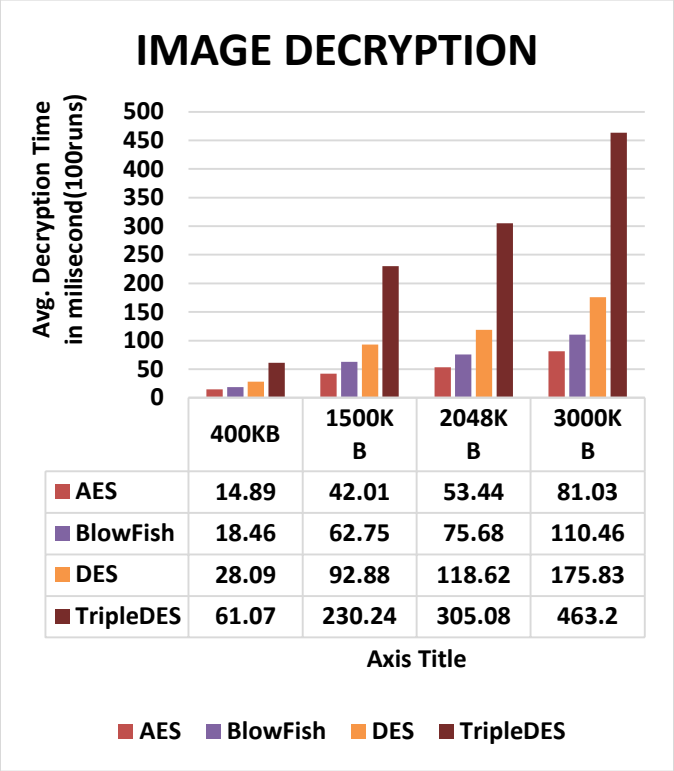


***Fig.8 Decryption Time of Different Algorithms for Image Files in Windows OS***

| 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) |
| 400kb | 16.61 | 14.89 | 24.48 | 18.46 | 27 | 28.09 | 59.14 | 61.07 |
| 1500kb | 44.8 | 42.01 | 57.4 | 62.75 | 90.88 | 92.88 | 217.4 | 230.24 |
| 2048kb | 58.78 | 53.44 | 67.88 | 75.68 | 116.52 | 118.62 | 287.27 | 305.24 |
| 3000kb | 84.13 | 81.03 | 98.93 | 110.46 | 172.76 | 175.83 | 436.45 | 463.2 |

***Table.4.Comparision Summary of Image Files Encryption Decryption(Windows OS)***

## 5. CONCLUSION AND FUTURE WORK

All the symmetric key algorithms are run on two different operating systems (WINDOWS and UBUNTU) using different sizes of text and image files.From the results we conclude that performance of UBUNTU is much better then Windows. Also in both the operating system AES is the best for both image and text files encryption decryption and Triple DES is the worst. The future work can be done to compare performance of AES along with some asymmetric algorithms on audio and video files**.**

## References

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

[2]. 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

[3]. Patil, Priyadarshini, et al. "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish." Procedia Computer Science 78 (2016): 617-624.

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

[5]. Bhardwaj, Akashdeep, et al. "Security algorithms for cloud computing." Procedia Computer Science 85 (2016): 535-542.

[6]. Bhat, Bawna, Abdul Wahid Ali, and Apurva Gupta. "DES and AES performance evaluation." International Conference on Computing, Communication & Automation. IEEE, 2015.