Performance Analysis of Symmetric Cryptographic Algorithms

Madhumita Panda

Assistant Professor in Computer Science.
SUIIT, Sambalpur University.
Odisha, (India)

ABSTRACT

Internet and networks applications are growing very fast, so the needs to protect such applications are increased. Cryptography is the one of the main categories of computer security that converts information from its normal form into an unreadable form. The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. This paper provides a fair comparison of some symmetric key cryptographic ciphers (AES,BLOWFISH, DES ,T.DES) on the basis of encryption and decryption time with different sizes of text files using Java as the programming language .

Keywords*: *Cryptography, Encryption, Decryption , DES, AES, 3DES, 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 is a science of secret writing. It provides a method for securing and authenticating the transmission of information across insecure communication channels. In cryptography, the data that can be read and understood without any special measures is called plaintext or clear text. The method of disguising 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 [1]**.** 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 [2]. 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 some commonly used symmetric key cryptographic algorithms for different sizes of text files.

The rest of this paper is organized as follows: Section 2 gives a brief introduction of the algorithms that have been chosen for implementation, Section 3 provides evaluation parameters and platforms chosen for comparing the algorithms, Section 4 presents performance results and analysis. Finally , Section 5 concludes the paper listing the future work.

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. Block Ciphers operate with a fixed transformation on large blocks of plain text data while stream ciphers operate with the time varying transformation on individual plain text bits. There are different symmetric cryptographic algorithms in the literature [3] [4]. Out of them, the algorithms listed in the Table 1 are selected for detailed study in this paper.

TABLE 1.CRYPTOGRAPHIC ALGORITHMS INFORMATION

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

III. 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.

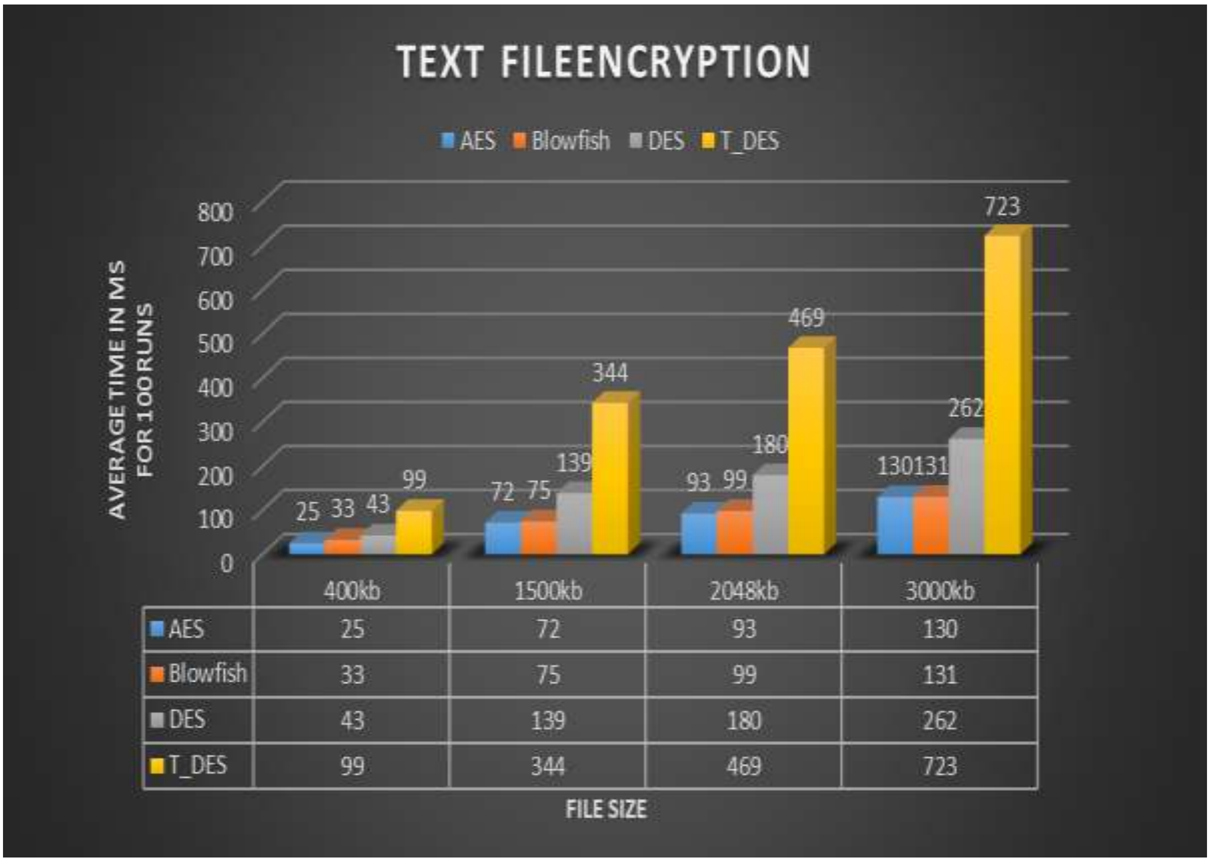
Evaluation Platforms

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

1. Software Speciation: Experimental evaluation on different encryption algorithm with Java Development Kit 8, Windows 8 Pro32 bit Operating System with 1.2 GHz clock speed.

2. Hardware Speciation: All the algorithms are tested on Intel(R) Core(TM) Duo processor with 3GB of RAM with300 GB HDD.

IV.EXPERIMENTAL RESULTS AND ANALYSIS



	400kb	1500kb	2048kb	3000kb
AES	25	72	93	130
Blowfish	33	75	99	131
DES	43	139	180	262
T_DES	99	344	469	723

Fig.1 Encryption Time of Different Algorithms for Text Files

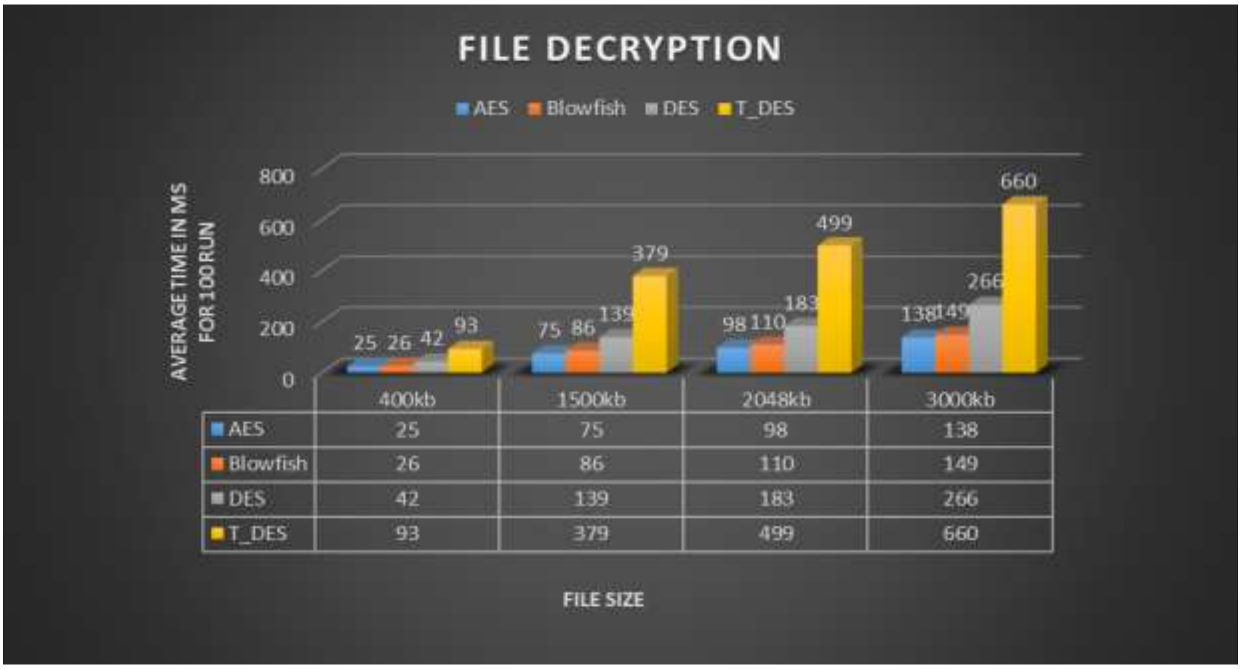


Fig 2. Decryption Time of Different Algorithms for Text Files

TABLE 2-COMPARATIVE SUMMARY OF TEXT FILES ENCRYPTION AND DECRYPTION

Text File Size	ALGORITHMS							
	AES		**BLOWFISH**		**DES**		**T_DES**	
	Average Encryption time	Average Decryption time	Average Encryption time	Average Decryption time	Average Encryption time	Average Decryption time	Average Encryption time	Average Decryption time
400kb	25	25	33	26	43	42	99	93
1500kb	72	75	75	86	139	139	344	379
2048kb	93	98	99	110	180	183	469	499
3000kb	130	138	131	149	262	266	723	660

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 text 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. The future work can be done to compare performance of these algorithms on image,audio and video files.

REFERENCES

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

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

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

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