ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 9(27), DOI: 10.17485/ijst/2016/v9i27/86580, July 2016*

Comparative Analysis of Symmetric Cryptographic Algorithms on .Net Platform

B. Nithya*[1] and P. Sripriya[2]

[1]Vels University, Pallavaram, Chennai, Tamil Nadu, India;
nithyababu.rch@gmail.com
[2]Department of Computer Applications, Vels University, Pallavaram, Chennai, Tamil Nadu, India;
sripriya.phd@gmail.com

Abstract

Objectives: To find which cryptographic algorithm would produce fine result. **Methods**: This survey mainly focuses to an analysis of symmetric cryptographic algorithms DES, 3DES, AES, RC4 in the basis of encryption/decryption time, memory and throughput. Here .net platform has been used to simulate the results to find the best algorithm for text file transmission. **Findings**: Simulation tests are conducted for text files in different file sizes. These text files are given as input to each specified algorithms and calculated the results. The tests have taken seven different sizes of text files. How the above algorithms affect system resources while encryption and decryption process are explained in this project. The key focus of the project is to find the performance of the algorithms. **Applications/Improvements**: If the algorithm shows lowest performance in throughput/memory/encryption time, new algorithm has to be developed to give better performance with all of these metrics.

Keywords: Advanced Encryption Standard, Data Encryption Standard, Decryption Time, Encryption Time, Performance, Throughput

1. Introduction

It is shown[1] that IBm_RSA is best in encryption time, throughput and processing time when compared to Blowfish, Twofish, RC2 and RSA. The simulation has taken place at .net platform. Also concluded[2] that encryption time does not vary according to the file type. It depends upon the size of file. This was analyzed at Java Cryptography Extension and the results of RC4 are fastest in encryption time than AES, DES, TDES, RC3, Blowfish and Skipjack.

A study[3] was conducted for executable, document, audio, video and image files to find the best in performance of these algorithms. Founded that Blowfish is best in throughput and also gave better results if it is .exe files. It was identified[4] that TDES needs more time for encryption/decryption process and DES has higher throughput. While changing the key size also shows changes in time consumption and battery usage. A research has been made[5] on AES and RC4 (Block Cipher and Stream Cipher). This was to find CPU usage, encryption time, memory utilization and throughput and said that RC4 is fast and better than AES.

The different web browsers used[6,7] and different algorithms' performance in the basis of time it takes for encryption/decryption. The outcome concluded that Internet Explorer and Netscape Navigator were best for DES algorithm. Mozilla gives fast result to RC6, Opera is

*Author for correspondence

best for UR5 algorithm. Another study was there[8] by considering two different operating systems Windows 7 and MAC to find the performance of algorithms. The result said that AES is best but DES takes less CPU usage than AES.

The research found that larger key space will give more security than smaller key space since the all the existing algorithms have lowest key space[9]. Almost of the cryptographic algorithm are compared[10] with their parameters like key size, block size, rounds and structure. Blowfish showed the least power consumption and better in performance. Comparisons[11] made on speed, throughput, encryption time, decryption time of symmetric and asymmetric algorithms. When compared to asymmetric, symmetric is finest in all of these parameters. Due to less number of rounds SHA provided better security[12]. Also there was tests made on different type of platforms like JCE and JCA, and said[13] that TDES takes less memory and proved low throughput but takes more time to encrypt/decrypt.

2. Performance Metric and Simulation Environment

2.1 Performance Metric

To find algorithm efficiency, performance metrics are needed to be evaluated for an algorithm on certain criteria. DES, 3DES, AES and RC4 algorithms' efficiency are evaluated by the following four performance metrics:

2.1.1 Encryption Time

Plain text is converted as cipher text is called encryption. The time which needs to convert original text to cipher text is known as encryption time. This time is important to identify the algorithm's speed that how much fast it can perform.

2.1.2 Decryption Time

The time taken to convert Cipher text to Plain text is known as decryption time.

2.1.3 Usage of Memory

Each algorithm takes some amount of memory to encrypt/decrypt the data. This also decides the performance of an algorithm. This is to be calculated in kb.

2.1.4 Throughput

The disk drives and networks are measured that how much data it can transfer during a time period called throughput. Throughput is calculated in kbps, mbps and gbps. Here in this paper, two types of throughputs are measured and showed the results. Formulas are,

Encryption Throughput = Plain Text in MB/ Encryption Time

Decryption Throughput=Cipher Text in Mb/ Decryption Time

2.2 Simulation Environment

The simulation described using a Laptop with Intel core i3 CPU @ 2.40 GHZ, 4 GB RAM Processor and Windows 7. With these specifications the performances are gathered. In this paper the simulation have taken place for text files from the size 108 kb – 2618 kb. The C#.net has been chosen to analyze encryption time, decryption time, encryption memory, decryption memory, encryption throughput and decryption throughput.

.Net platform is used widely for creating reliable and secure network. Also it has predefined classes for cryptographic algorithms like, DES Crypto Service Provider, AES Crypto Service Provider. These sub classes are available in System. Security.Cryptography Classes.

2.2.1 Finding Encryption/Decryption Time

The predefined classes for each algorithm have been called to process the basic algorithm. The class Stopwatch is used to get the Encryption/Decryption time. Methods of the class Stopwatch, start (), stop () are called before and after to the coding of algorithm. The time of results are considered as encryption/decryption time.

2.2.2 Finding Memory Usage

To find the space that each algorithm takes to encrypt/decrypt is calculated as taking the measurement of memory before encryption/decryption processes and after the encryption/decryption processes. The result will be subtracted from before to after usage of memory in kilo bytes.

To get the space in C# platform it has a method System. Diagnostics.Process.GetcurrentProcess().

2.2.3 *Finding Throughput*

After calculated the encryption/decryption time, throughput is measured as per the formula described above. The simulation gets the results in kbps that is kilo bytes per second the network can transfer at a period of time.

3. Results and Discussions

3.1 Encryption Time

Encryption time is calculated with text files in different sizes. The simulation shown in Figure 1 showed that DES and TDES have least encryption time. AES has high encryption time. RC4 is also has least when compare to AES but higher than DES and TDES.

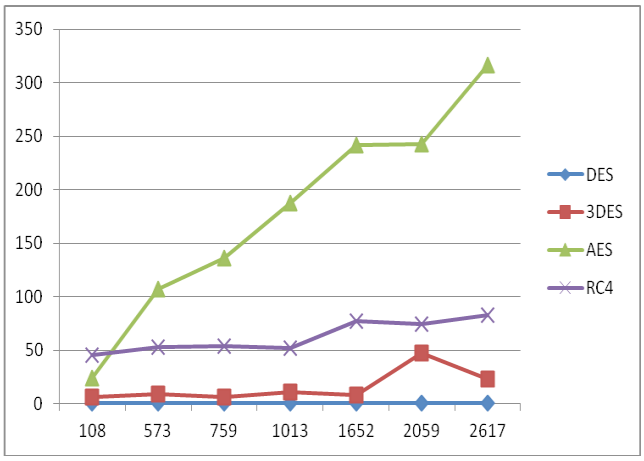

Figure 1. Encryption time.

3.2 Decryption Time

Decryption process is simulated with same file sizes and their corresponding cipher text. Here in Figure 2 also DES has least decryption time. RC4 decryption time is higher than DES but lower than AES. TDES has highest decryption time when compared to other. When encrypting plain text shown in Figure 1 TDES takes least time, but it takes more time when decryption process.

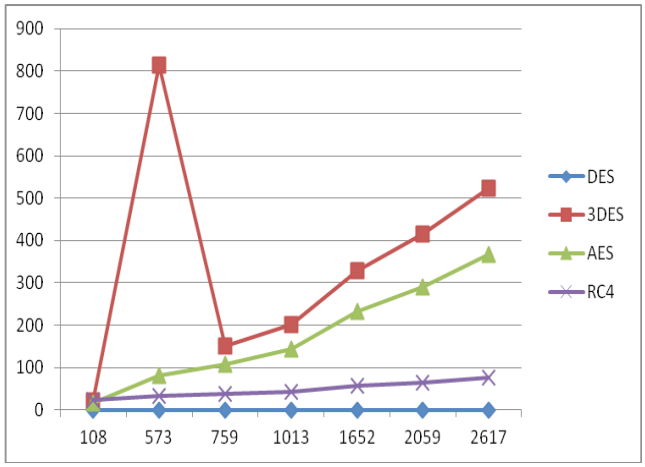

Figure 2. Decryption time.

3.3 Memory used for Encryption

While each process done by CPU it takes some amount of memory, and it will release after the process has been completed. When the encryption process the simulation shows the amount of memory used by each algorithms are shown in Figure 3. AES has least memory result when compared to other algorithms of DES, 3DES and RC4.

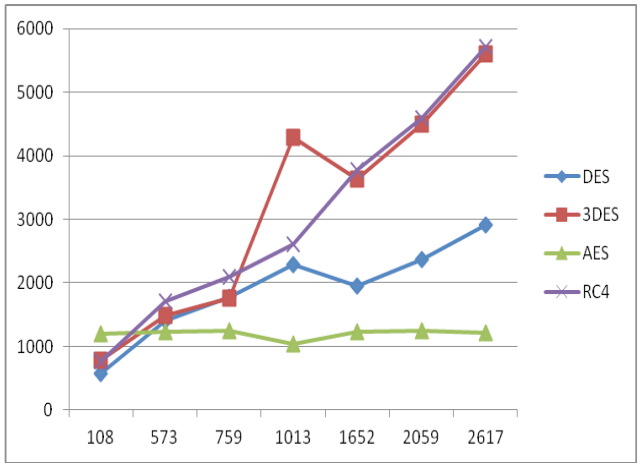

Figure 3. Memory used for encryption.

3.4 Memory used for Decryption

At the Decryption end, memory has been calculated for each algorithm takes for decrypting the file. Here DES

and AES are shown in Figure 4 take same space for different file sizes. But RC4 and 3DES takes different memory sizes when varying file sizes. DES and AES use memory space for decryption depends upon file size.

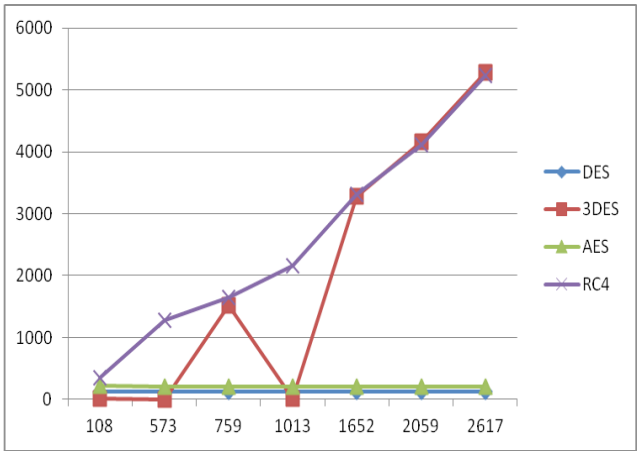

Figure 4. Memory used for decryption.

3.5 Encryption Throughput

The received encryption time from the simulation result, the throughput is calculated as per the formulas that plain text in mb/ encryption time. The investigated results are shown in Figure 5 described that AES is best in throughput than other algorithms of DES, TDES and RC4. DES had least encryption time and consumed less memory for both encryption and decryption. But here the throughput of DES is low.

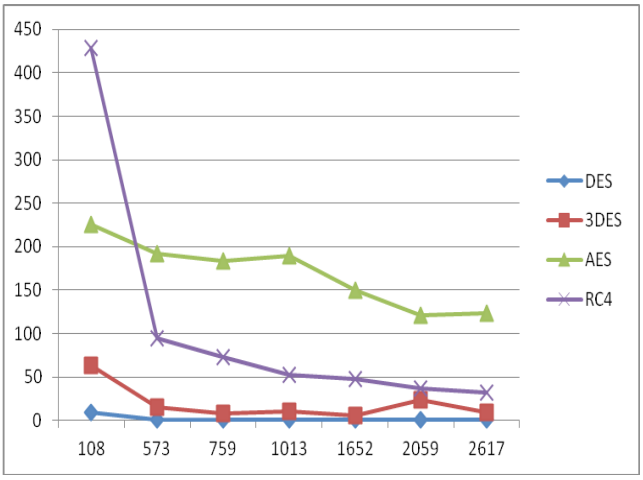

Figure 5. Encryption throughput.

3.6 Decryption Throughput

The performance of throughput at decryption end also shows that AES has high throughput than all others. DES and TDES are shown in Figure 6 never change their throughput even change of file size. RC4 has high throughput when file size is small, but while increasing file size throughput went down.

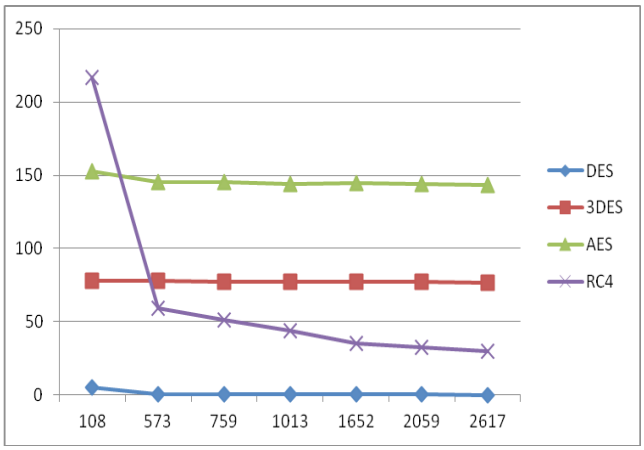

Figure 6. Decryption throughput.

4. Conclusion

Four symmetric algorithms DES, TDES, AES and RC4 are compared and analyzed by its performance metrics. Performance metrics are in the basis of encryption time, decryption time, usage of memory by the algorithms then the throughput has taken by them. The simulation resulted using the .net environment and predefined classes of each algorithm produced cryptographic techniques. The simulation described that DES has least encryption time and also it takes less memory for decryption but low throughput. TDES has high decryption time and also it uses more space to encrypt/decrypt. But TDES throughput is better than DES and RC4. RC4 uses less memory, high encryption/decryption time but low throughput. When compared to all of before mentioned algorithms AES has better throughput and it needs only less space for encryption/decryption process.

This article presents result for text files with sizes from 108 kb to 2618 kb. Future work may be done for bigger file sizes and different types of files with different size of keys to find a better algorithm to generate better performance.

5. References

1. Singh L, Bharti RK. Comparative performance analysis of cryptographic algorithms. International Journal of Advanced Research in Computer Science and Software Engineering. 2013; 3(11):43-52.
2. Masram R, Shahare V, Abraham J, Moona R. Analysis and comparison of symmetric key cryptographic algorithms based on various file features. International Journal of Network Security and its Applications. 2014; 6(4):563-8.
3. Sharma RAS. Performance analysis of cryptography algorithms. International Journal of Computer Applications. 2012; 48(21):35-9.
4. Lemma A, Telentino M, Mehari G. Performance analysis on the implementation of data encryption algorithms used in network security. International Journal of Computer and Information Technology. 2015 Jul; 4(4):711-7.
5. Singhal N, Raina JPS. Comparative analysis of AES and RC4 algorithms for better utilization. International Journal of Computer Trends and Technology. 2011 Jul-Aug; 177-81.
6. Srinivas BL, Shanbhag A, D'Souza AS. A comparative performance analysis of DES and BLOWFISH symmetric algorithm. International Journal of Innovative Research in Computer and Communication Engineering. 2014; 2(5):77-88.
7. Kumar A, Sinha S, Chaudhary R. A comparative analysis of encryption algorithms for better utilization. International Journal of Computer Applications. 2013; 71(14):19-23.
8. Rihan SD, Khalid A, Osman SEF. A performance comparison of encryption algorithms AES and DES. International Journal of Engineering Research and Technology. 2015; 4(12):151-4.
9. Mohan M, Devi MKK, Prakash VJ. Security analysis and modification of classical encryption scheme. Indian Journal of Science and Technology. 2015; 8(S8):542-8.
10. Gupta A, Walia NK. Cryptography algorithms: A review. International Journal of Engineering Development and Research. 2014; 2(2):1667-72.
11. Rejani R, Krishnan DV. Study of symmetric key cryptography algorithms. International Journal of Computer Techniques. 2015; 2(2):45-50.
12. Nivetha MB, Sivaramakrishnan S. A comparative analysis of cryptography algorithms. International Journal of Innovative Research in Electrical Electronical and Instrumentation Control Engineering. 2014; 2(10):2102-5.
13. Harinath D, Murthy MVR, Chitra B. Cryptographic methods and performance analysis of data encryption algorithms in network security. International Journal of Advanced Research in Computer Science and Software Engineering. 2015; 5(7):680-8.
14. Kashyap S, Madan N. A review on: Network security and cryptographic algorithm. International Journal of Advanced Research in Computer Science and Engineering. 2015; 5(4):1414-8.
15. Bhanot R, Hans R. A review and comparative analysis of various encryption algorithms. International Journal of Security and its Applications. 2015; 9(4):289-306.
16. Nithya B, Sripriya P. A review of cryptographic algorithms in network security. International Journal of Engineering and Technology. 2016; 8(1):324-31.