Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

Stream Cipher and Block Cipher Based Performance Analysis of Symmetric Cryptography Algorithms: AES and DES

Dr. Preeti Mehta[1], Ms. Monika Bansal[2], Ms. Akanksha Upadhyaya[3]
[1, 2, 3] *Department of MCA, Rukmini Devi Institute of Advanced Studies*

Abstract— Security and risk management are considered to be data centric. Data, systems and network can be protected for three possible outcomes: confidentiality, integrity and availability. In today's scenario security of data has become an important issue. Most of the security problems are caused by malicious attackers to cause harm to the sensitive information which is transmitted for specific purpose. The only solution to the problem is cryptographic technique. A theoretical study was made on the DES and AES symmetric encryption algorithms. This research paper majorly focuses on evaluation of performance of two different symmetric encryption techniques on the basis of execution time. Secondary experimental data [1] will be given and hence analyzed for effectiveness of each algorithm.

Keywords – Network Security, Cryptography, Symmetric Cryptography, Encryption.

I. INTRODUCTION

In today's era security of data is most important. Various techniques under cryptography have been proposed and developed for secure sharing and transmission of data. Cryptography refers to converting a plain text into a form which cannot is not easily readable. The technique uses no key, one key or two key for converting a data into encrypted form. Use of no key refers to Hash algorithm, symmetric key cryptography uses one key i.e. Private Key while asymmetric uses two keys, private and public for enciphering/deciphering of data. Various application areas use this technique for protecting their data from data theft or unauthorized access. The overall data and network security area is broadly categorized is four major aspects i.e. secrecy, authenticity, non-repudiation and integrity. As a whole we can say that cryptography is the most prominent area for providing security to any kind of data at its best level.

II. OBJECTIVE

Objective of the study is to analyze the data for symmetric encryption algorithms namely DES and AES on following aspects:

Case 1: Analysis for Block cipher.
Case 2: Analysis for stream cipher.
Case 3: Analysis between Stream cipher and Block cipher.

III. ORGANISATION OF PAPER

This paper has been divided into eight sections. Section IV defines cryptography and different symmetric cryptography algorithms, with special focus on DES and AES. Section V describes previous work done in the field of security. In Section VI, analysis of two symmetric key algorithms has been presented, with the help of graphs. Conclusion and Future Scope are presented in section VII and VIII respectively.

IV. SYMMETRIC KEY CRYPTOGRAPHY ALGORITHMS

With the advancement of technologies, there is greater need for securely transmitting and storing of information. Cryptography is a science of applying complex mathematical logics for converting

meaningful data into meaningless data. Majorly cryptography can be categorized in three techniques: Symmetric, asymmetric and hybrid.
Symmetric key cryptography techniques use same key to encrypt or decrypt the data. Various symmetric key cryptography techniques used are DES, Triple-DES, AES, blowfish, RC2 etc.

V. LITERATURE REVIEW

The performance of DES, AES, Blowfish and 3DES algorithms is discussed in [1] on the basis of execution time and file sizes on machines with different hardware specifications including P-II 266 MHz and P-IV 2.4 GHz. Analysis shows that Blowfish is superior over other algorithms and AES has better performance when compared with DES and 3DES only. Moreover, one-third of processing time is required by DES in comparison of 3DES. The paper is taken as a base paper and a source for secondary data also. Further, Cornwell [2] discussed another type of blowfish symmetric key cryptographic technique based on the design of Bruce Schneier's. Author [2] has also discussed performance analysis and possible attacks encountered in this technique. Blowfish algorithm was found to be more effective in comparison to DES, 3DES, and AES. Tamimi [5] also performed comparative analysis on DES, 3DES, AES and Blowfish symmetric algorithms. Under different settings, and different data loads, the performance of these algorithms was analysed. Two modes of operation were considered in the study namely ECB and CBC, for calculating execution time of each.

VI. ANALYSIS

On the basis of secondary data taken [1] for analysis: input file size (bytes), execution time per second following analysis has been done in MS-Excel 2010.
Analysis was done on two machines namely Pentium-II 266 MHz machine (with Microsoft Windows operating system) and Pentium-IV, 2.4 GHz machine (running Microsoft Windows XP operating system)

A. *Case1: Analysis for Block Cipher:*

1. As the file size increases, execution time of both algorithms i.e. DES and AES also increase.
2. The average proportion of AES over DES in terms of encryption time is 1.6 (approx.) as shown in table 1. This signifies that DES is 1.6 times faster than AES and this proportion lies between 1.5 sec and 1.7 sec.
3. More is the execution time wider is the distance between AES and DES.

TABLE I . EXECUTION TIME OF DES AND AES IN BLOCK CIPHER ON PENTIUM II AND PENTIUM IV MACHINE [1]

	Pentium-II Machine			Pentium-IV Machine		
INPUT SIZE	**DES**	**AES**	**AES/ DES**	**DES**	**AES**	**AES/ DES**
20527	24	39	1.625	2	4	2
36002	48	74	1.542	4	6	1.5
45911	57	94	1.649	5	8	1.6
59862	74	126	1.703	7	11	1.571
69646	83	143	1.723	9	13	1.444
137325	160	285	1.781	17	26	1.529
158959	190	324	1.705	20	30	1.5
166364	198	355	1.793	21	31	1.476
191383	227	378	1.665	24	36	1.5
232398	276	460	1.667	30	44	1.467

Average Time	133.7	227.8	1.7	14	20.9	1.5

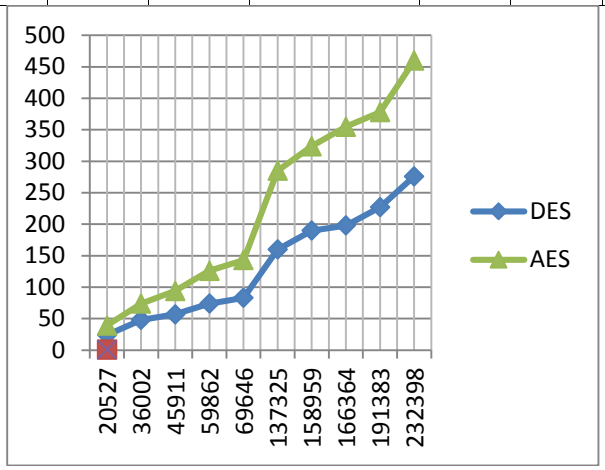

Fig. 1: Analysis of DES and AES in Block Cipher on Pentium II machine

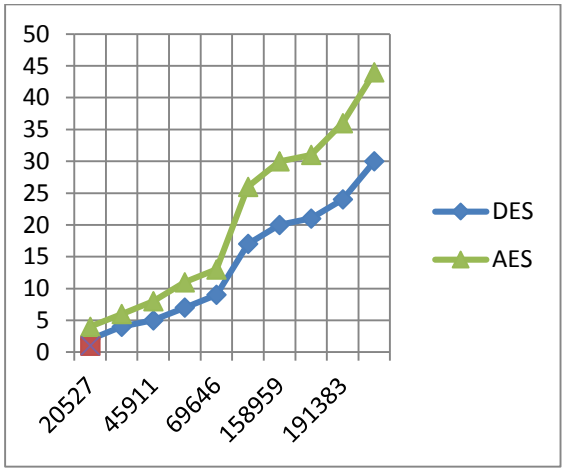

Fig. 2 Analysis of DES and AES in Block Cipher on Pentium IV machine

B. Case 2: Analysis for Stream Cipher:

1. As the file size increases, execution time of both algorithms i.e. DES and AES also increase.
2. The average proportion of AES over DES in terms of encryption time is 3.1 (approx.) as shown in table 2.i.e. DES is 3 times (approx.) faster than AES and this proportion lies between 2.8 sec-3.8 sec.
3. More is the execution time wider is the distance between AES and DES.

TABLE 2. EXECUTION TIME OF DES AND AES IN STREAM CIPHER ON PENTIUM II AND PENTIUM IV MACHINE[1]

	Pentium-II Machine			**Pentium-IV Machine**		
INPUT SIZE	DES	AES	AES/ DES	DES	AES	AES/ DES
20527	188	598	3.181	17	62	3.647
36002	362	1123	3.102	30	94	3.133
45911	431	1484	3.443	41	125	3.049
59862	570	1932	3.389	52	174	3.346
69646	629	2251	3.579	69	200	2.899
137325	1203	4419	3.673	129	409	3.171

158959	1405	5044	3.59	151	473	3.132
166364	1511	5501	3.641	159	489	3.075
191383	1714	5923	3.456	185	567	3.065
232398	2139	7231	3.381	229	687	3
Average Time	133.7	227.8	3.443	106	328	3.152

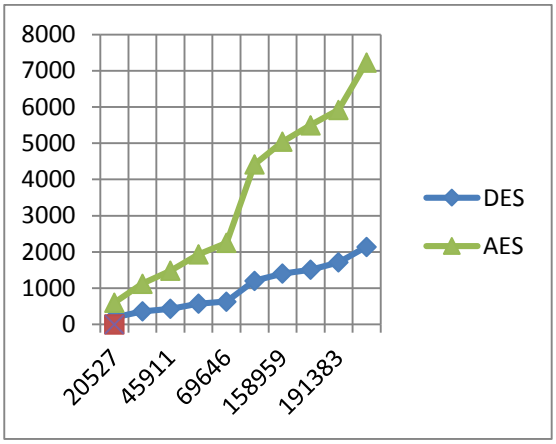

Fig. 3 Analysis of DES and AES in Stream Cipher on Pentium II machine

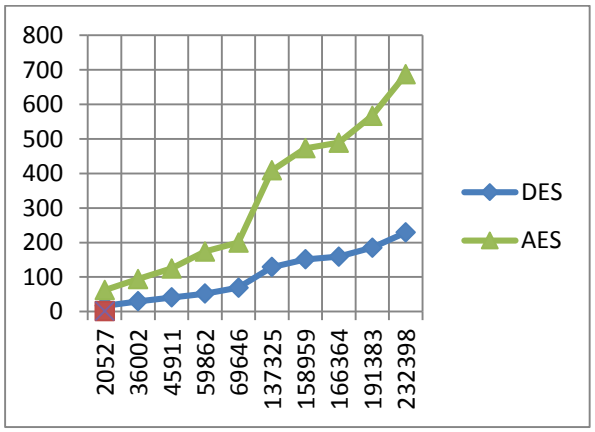

Fig. 3 Analysis of DES and AES in Stream Cipher on Pentium II machine

C. Case 3: Analysis between Block and Stream Cipher:

The comparative analysis is done on two different machines. In general[1],

1. Block size and key size both varies in Block Cipher. As the block size increases, time taken by the algorithm will decrease because in a single execution cycle of the algorithm, a large group of data will get encrypted due to large block size. Similarly, bigger is the key size, slower will be the algorithm. Moreover, in a smaller key a less number of key bits are involved and hence, it reduces the time to complete one round.

Hence,

Large Block size → Decreased execution time (fast speed)

Small Block Size → Increased execution time (slow speed)

Large Key size → slow speed

Small Key Size → fast speed

While in case of stream cipher, with large block size, the algorithms have to do more work for same amount of input data (a bit or byte) in a single execution cycle of the algorithm. Hence,
Large Block size → Increased execution time (slow speed)
Small Block Size →Decreased execution time (fast speed)

Effect of large key size in stream cipher is same as in block cipher i.e.
Large Key size → slow speed
Small Key Size → fast speed

Both in Block cipher and stream cipher, key size plays more important role in terms of execution time in comparison to block size. The key size of AES i.e. 128 bits is approximately two times of DES key size i.e. 56. Because of this key size gap DES execution is faster than AES execution as shown by all graphs (Fig.1- Fig.4).
In case of Block Cipher, execution gap between AES and DES is smaller than in case of Stream Cipher. The reason is, DES has less block size (64 bits) and key size in comparison to AES block size (128 bits) and key size which makes the difference wider in case of Stream Cipher (Fig. 3, Fig. 4) in comparison to Block Cipher (Fig. 1, Fig. 2).

VII. CONCLUSION

In this paper, performance of two most popular symmetric key algorithms AES and DES were analyzed on the basis of their execution time on two different machines using secondary data. On the basis of analysis we conclude that in terms of time taken for encryption, DES performance is better than AES.

VII. FUTURE SCOPE

Though security was not cater for, in practice, however, one could consider security first. A proposed direction for the future work could be to analyze trade-off between security and performance. For instance, an algorithm with greater number of rounds and complex rounds are considered to be more secure. The impact of these and other such factors on the overall performance also needs to be measured. Since we have used secondary data for analysis, hence next step will be in the direction of analyzing difference between symmetric and asymmetric algorithm in terms of execution time, security, different key sizes, different machines and many more parameters. The future work will be based on strong experimental data set .

REFERENCES

[1] Nadeem Aamer, “Performance Comparison of Data Encryption Algorithms”, IEEE xplore, Oct 2008.
[2] Cornwell Jason W, “Blowfish Survey”, Department of Computer science, Columbus State university, Columbus, GA, 2010.
[3] Singh S Preet, Mani Raman, “Comparison of Data Encryption Algorithms”, International Journal of Computer science and Communications, Vol. 2, No.1, January-June 2011, pp. 125-127.
[4] Tamimi A. Al., “Performance Analysis of Data Encryption Algorithms”, IEEE xplore, Oct 2008.
[5] Jaber A.N. and Zolkipli F.B. Md.,“Use of cryptography in cloud computing” IEEE International conference on Control system, Computing and Engineering, Malaysia, 2013 pp179-184