A Performance Comparison of Encryption Algorithms AES and DES

Shaza D. Rihan
Omdurman Islamic University
College of Higher Education
Omdurman, Sudan

Ahmed Khalid
Najran University
Community College
Najran, KSA

Saife Eldin F. Osman
Emirates College for Science and Technology
Computer science Department
Khartoum, Sudan

***Abstract:*- There is a considerable increase in the exchange of data over the Internet and other media types. this Data may contain confidential information that need to be secured from any third party access. Encryption algorithms play a main role for securing these type of data. The encryption algorithms are varied in their performance. This paper evaluate the performance the two encryption algorithms: AES and DES. The performance measure of encryption algorithms will be conducted in terms of processing time, CPU usage and encryption throughput on Windows and Mac platform for a different text size. Experimental results are given to demonstrate the performance of each algorithm.**

Keywords— Encryption, Decryption, DES, AES

I-INTRODUCTION

Cryptography algorithm is the technique used for concealing the content of message from all users except the sender and the receiver and to authenticate the correctness of message to the recipient [10]. Information security could be implemented with many known security algorithms [13,1,15,16]. The most common of these are Encryption algorithms [9, 7, 8]. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption[5]. Symmetric key cryptography involves the usage of the same key for encryption and decryption. But the Asymmetric key cryptography involves the usage of one key for encryption and another different key for decryption [17]. Secret key cryptography includes DES, AES, 3DES, IDEA, Blowfish algorithms etc, and public key cryptography includes RSA, Digital Signature and Message Digest algorithms [2,4].

This paper evaluates two encryption algorithms namely; AES and DES. The performance measure of encryption schemes will be conducted in terms of processing time, CPU usage encryption throughput on Windows and Mac platform for a different text size.

The rest of this paper is organized as follows: section II gives a brief introduction of the algorithms that have been chosen for implementation; section III provides the related works, section IV discuss the implementation details; section V presents performance results and finally section VI concludes the work.

II- IMPLEMENTED ALGORITHMS

1- Data Encryption Standard (DES)

The main standard for encrypting data was a symmetric algorithm known as the Data Encryption Standard (DES). DES is a 64 bit block cipher which means that it encrypts data 64 bits at a time. This is contrasted to a stream cipher in which only one bit at a time (or sometimes small groups of bits such as a byte) is encrypted. DES is based on a cipher known as the Feistel block cipher. This was a block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70's. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. DES expects two inputs - the plaintext to be encrypted and the secret key. The manner in which the plaintext is accepted, and the key arrangement used for encryption and decryption, both determine the type of this cipher. DES is therefore, a symmetric, 64 bit block cipher as it uses the same key for both encryption and decryption and only operates on 64 bit blocks of data at a time [18]. The overall scheme for DES encryption is illustrated in figure1.

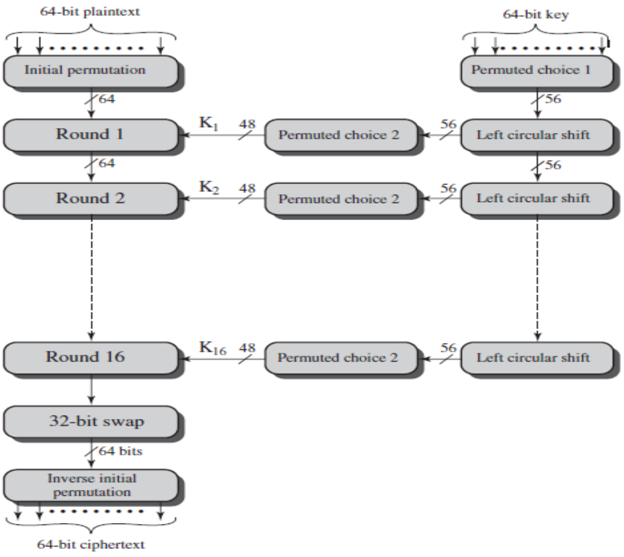


Figure 1 : General Depiction of DES Encryption algorithm

2--ADVANCED ENCRYPTION STANDARD(AES):

AES is a block cipher with a block length of 128 bits. AES allows for three different key lengths: 128, 192, or 256 bits. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and in addition the round key. The order in which these four steps are executed is different for encryption and decryption. Unlike DES, the decryption algorithm differs substantially from the encryption algorithm. Although, the overall, same steps are used in encryption and decryption, the order in which the steps are carried out is different, as mentioned previously [3]. Figure2 show, the overall structure of the AES encryption process.

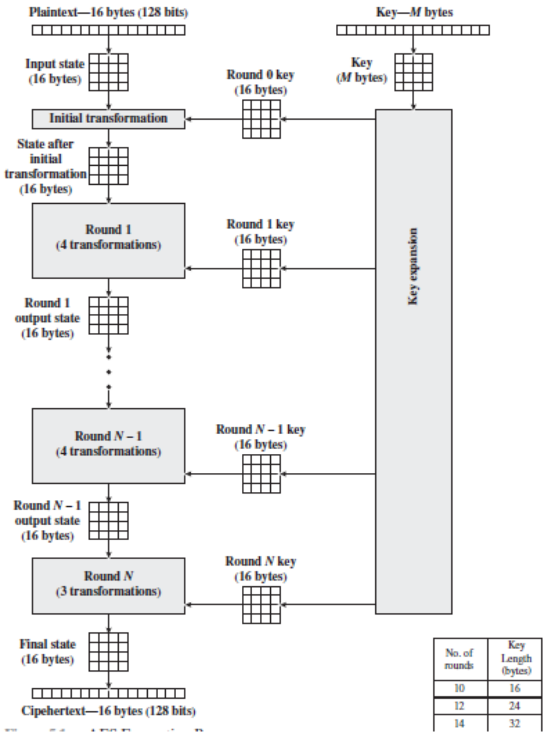

Plaintext—16 bytes (128 bits)
Key—M bytes
Input state (16 bytes)
Round 0 key (16 bytes)
Key (M bytes)
Initial transformation
State after initial transformation (16 bytes)
Round 1 (4 transformations)
Round 1 key (16 bytes)
Key expansion
Round 1 output state (16 bytes)
Round N – 1 (4 transformations)
Round N – 1 key (16 bytes)
Round N – 1 output state (16 bytes)
Round N (3 transformations)
Round N key (16 bytes)
Final state (16 bytes)
Cipehertext—16 bytes (128 bits)
No. of rounds
Key Length (bytes)
10
16
12
24
14
32

Figure 2: AES Encryption Process

III-RELATED WORK:

There are various research studies that compare between the performance of the common encryption algorithms. This section discusses the results of some of these studies:

Rajdeep Bhanot and Rahul Hans [12] have analyzed ten data encryption algorithms DES, Triple DES, RSA, AES, ECC, BLOWFISH, TWOFISH, THREEFISH, RC5 and IDEA. Among them DES, Triple DES, AES, RC5, BLOWFISH, TWOFISH, THREEFISH and IDEA are symmetric key cryptographic algorithms. RSA and ECC are asymmetric key cryptographic algorithms. Their works based on different parameters and compared them to choose the best data encryption algorithm. They have found that each algorithm has its own benefits according to the different parameters.

Ranjeet Masram, et al. [11] provides analysis and comparison of some symmetric key cryptographic ciphers (RC4, AES, Blowfish, RC2, DES, Skipjack, and Triple DES) on the basis of encryption time with the variation of various file features like different data types, data size, data density and key size. Their experiment concluded that encryption time does not depend on data type and encryption it only depends on the number of bytes present in the file. It also showed that encryption time and data size is proportional to each other.

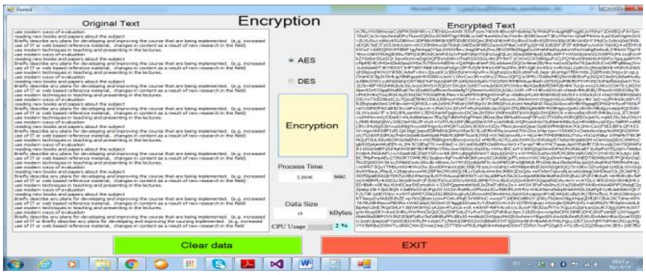
Najib A. Kofahil, et al.[6] presents a comparison between three algorithms DES, Triple DES and Blowfish based on processing time. Their results showed that the Blowfish algorithm was the fastest algorithm followed by the DES algorithm then the T-DES algorithm. The T-DES algorithm was slow in its performance due to the added complexity and security it has over the DES algorithm.

Shraddha Soni, et al. [14] presents an analysis and comparison of various parameters of DES and AES encryption scheme based on the text. Their experimental results concluded that AES algorithm consumes the least encryption and decryption time as compared to DES algorithm.

Sombir Singh, et al. [17] present a comparison between the DES private key based Algorithm and RSA public key based algorithm. The main feature that specifies and differentiate one algorithm from another is the ability to the speed of encryption and decryption of the input plain text. They have found that the encryption and decryption execution time consumed by DES algorithm the least as compared to RSA algorithm. The encryption and decryption speed of DES algorithm is fastest as compared to RSA.

IV-EXPERIMENTAL DESIGN:

The experiment is performed on two platforms a laptop core I5 , 2.5 GH. CPU with operating system windows 7 and an Apple mac book Intel core I5 with mac operating system. Three performance metrics are collected: encryption time, CPU usage and encryption throughput for the two encryption algorithms AES and DES. The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the encryption time [5]. The CPU usage is the percentage of the time that a CPU is committed only to the particular process of calculations. It reflects the load of the CPU. The more CPU usage is used in the encryption process, the higher is the load of the CPU. The experiment is performed to measure the effect of the changing data size and the platform for each cryptography algorithm. Figure 3 shows the interface of the simulation program written in visual basic .net 2013.



use modern ways of evaluation
reading new books and papers about the subject
Briefly describe any plans for developing and improving the course that are being implemented. (e.g. increased use of IT or web based reference material, changes in content as a result of new research in the field)
use modern techniques in teaching and presenting in the lectures.
use modern ways of evaluation
reading new books and papers about the subject
Briefly describe any plans for developing and improving the course that are being implemented. (e.g. increased use of IT or web based reference material, changes in content as a result of new research in the field)
use modern techniques in teaching and presenting in the lectures.
use modern ways of evaluation
reading new books and papers about the subject
Briefly describe any plans for developing and improving the course that are being implemented. (e.g. increased use of IT or web based reference material, changes in content as a result of new research in the field)
use modern techniques in teaching and presenting in the lectures.
use modern ways of evaluation
reading new books and papers about the subject
Briefly describe any plans for developing and improving the course that are being implemented. (e.g. increased use of IT or web based reference material, changes in content as a result of new research in the field)
use modern techniques in teaching and presenting in the lectures.
use modern ways of evaluation
reading new books and papers about the subject
Briefly describe any plans for developing and improving the course that are being implemented. (e.g. increased use of IT or web based reference material, changes in content as a result of new research in the field)
use modern techniques in teaching and presenting in the lectures.
use modern ways of evaluation
reading new books and papers about the subject
Briefly describe any plans for developing and improving the course that are being implemented. (e.g. increased use of IT or web based reference material, changes in content as a result of new research in the field)
use modern techniques in teaching and presenting in the lectures.
use modern ways of evaluation
reading new books and papers about the subject
Briefly describe any plans for developing and improving the course that are being implemented. (e.g. increased use of IT or web based reference material, changes in content as a result of new research in the field)
use modern techniques in teaching and presenting in the lectures.
use modern ways of evaluation
reading new books and papers about the subject
Briefly describe any plans for developing and improving the course that are being implemented. (e.g. increased use of IT or web based reference material, changes in content as a result of new research in the field)
use modern techniques in teaching and presenting in the lectures.
use modern ways of evaluation
Briefly describe any plans for developing and improving the course that are being implemented. (e.g. increased use of IT or Briefly describe any plans for developing and improving the coursing implemented. (e.g. increased use of IT or web based reference material, changes in content as a result of new research in the field

[illegible]

Process Time: 3.6946 sec
Data Size: 15 kBytes
CPU Usage: 2 %

Figure 3: interface of the simulation program

V- SIMULATION RESULTS

Table 1 represents the different sizes of the text files and corresponding encryption execution time taken by DES and AES algorithms in seconds for the windows operating system. The results reveal that the encryption time taken by AES is very short as compared to DES. Figure 4 shows the encryption time taken by DES and DEA for different size text files for the windows operating system.

Table1: encryption time in seconds for deferent data size in windows

Input size(KB)	AES	AES
15	3.8	5.07
30	7.5	17.09
45	8.5	1.96
60	8.8	22.91
75	9.33	29.99
90	10.7	38.15
Average time	8.105	22.195
KB/sec	27.76	10.13

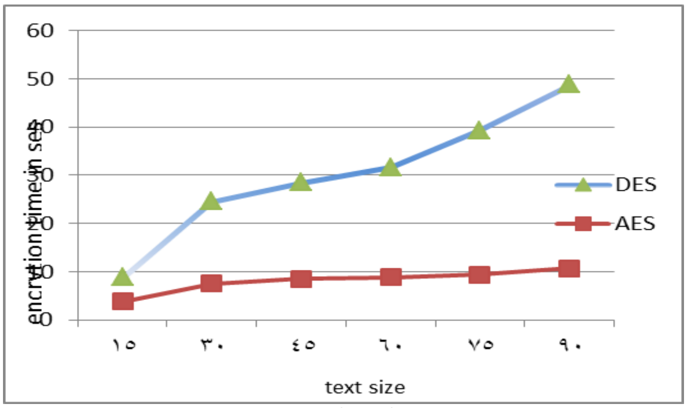


Figure 4: encryption time for deferent data size in windows OS

Table 2 represents the different sizes of the text files and corresponding encryption execution time taken by DES and AES algorithms in seconds for the MAC operating system. From the table we conclude that the encryption time taken by AES is very short as compared to DES. Figure 5 shows the encryption time taken by AES and DES for different size text files for the MAC OS.

Table2: encryption time in sec for deferent data size For the MAC operating system

Input size(KB)	AES	DES
15	3.08	5.01
30	5.7	15.09
45	8.6	17.44
60	8.99	25.88
75	9.29	30.44
90	10.01	37.13
Average time	7.11	21.83
KB/sec	31.65	10.31

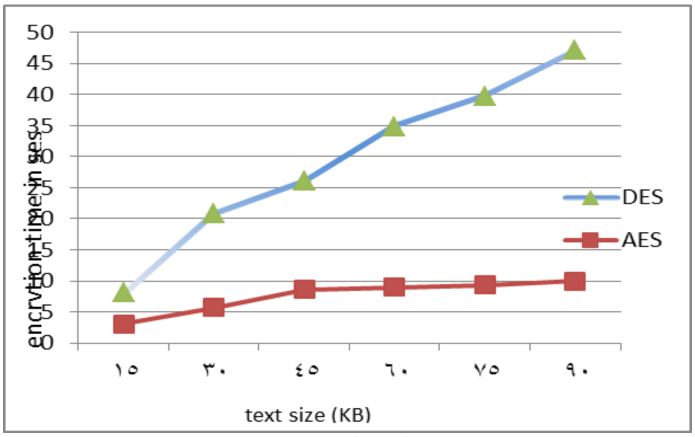


Figure 5: encryption time for deferent data size in MAC OS

Table 3 shows the encryption throughput of the AES and DES for the two platforms. The throughput also explained that the encryption speed of AES is high as compared to DES algorithm for the two platforms. Figure 6 shows the encryption throughput of AES and DES for the two platform.

TABLE3: ENCRYPTION THROUGHPUT OF AES AND DES FOR THE WINDOWS AND MAC

encryption algorithms	encryption throughput for windows	encryption throughput for MAC
AES	27.76	31.65
DES	10.13	10.31

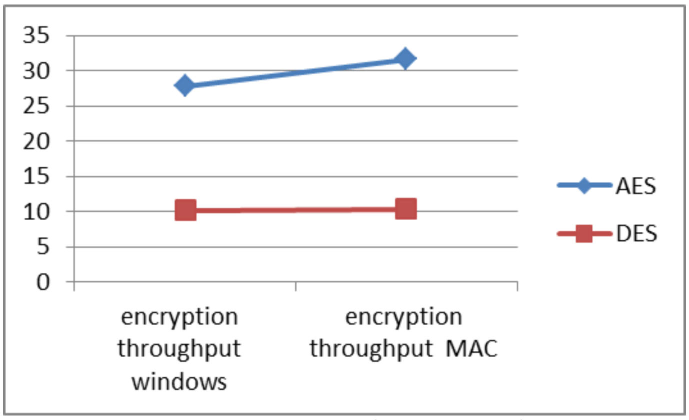


Figure 6: encryption throughput of AES and DES for windows and MAC

Table 4 shows the CPU usage of the AES and DES for the two platforms. The usage of the CPU for DES is less than AES for the two platforms. Figure 7 shows the CPU usage for AES and DES for the two platform.

Table 4: CPU usage in window and mac

encryption algorithms	CPU usage in windows	CPU usage in in MAC
AES	4.2%	2%
DES	2%	1.9%

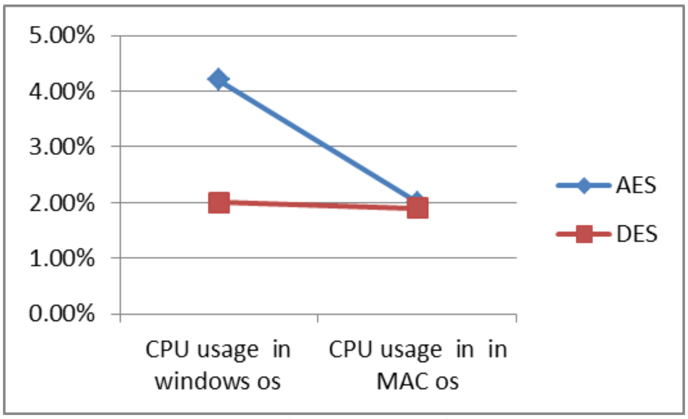


Figure 7: CPU usage for AES and DES for windows and MAC

VI-CONCLUSION

Encryption algorithm plays a very important role in communication security. Our research evaluates the performance of the two encryption algorithms AES and DES. The performance measure of encryption algorithms is conducted in terms of processing time, CPU usage and encryption throughput on Windows and Mac platform for a different text size. The simulation results conclude, that, AES is faster than DES in the execution time for the two platforms. AES has high throughput than DES. DES consumes less CPU usage than AES for two platforms. Our further research will focus on comparing and analyzing the existing other cryptographic algorithms. It will include experiments on image data it will focus on improving encryption time.

REFERENCES

[1] A. Nadeem MYJ (2005)."A performance comparison of data encryption algorithms", First International Conference on Information and Communication Technologies, pp 84- 89.

[2] Atul Kahte.Cryptography and Network Security.Tata Mcgraw Hill, 2007.

[3] Avi Kak, " Lecture Notes on Computer and Network Security" , May 1, 2015 12:14 Noon c 2015 Avinash Kak, Purdue University.

[4] Charels Connell, An Analysis of New DES: A Modified Version of DES, Locust Street Burlington, USA, Boston MA 02215 USA.

[5] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud, " Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009 ISSN: 1943-7765.

[6] Kofahi, N.A, Turki Al-Somani, Khalid Al-Zamil, “Performance evaluation of three Encryption/Decryption Algorithms”, IEEE 46th Midwest Symposium on Circuits and Systems, Vol 2, Issue 1, 30-30 Dec. 2003, pp. 790-793.

[7] M. H. Ibrahim, “A method for obtaining deniable public-key encryption,” International Journal of Network Security, vol. 8, no. 1, pp. 1-9, 2009.

[8] M. H. Ibrahim, “Receiver-deniable public-key encryption,” International Journal of Network Security, vol. 8, no. 2, pp. 159-165, 2009.

[9] M. S. Hwang and C. Y. Liu, “Authenticated encryption schemes: current status and key issues,” International Journal of Network Security, vol. 1, no. 2, pp. 61-73, 2005.

[10] Narender Tyagi, Anita Ganpati "Comparative Analysis of Symmetric Key Encryption Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 8, August 2014 ISSN: 2277 128X.

[11] Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona ANALYSIS AND COMPARISON OF SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS BASED ON VARIOUS FILE FEATURES", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, July 2014.

[12] Rajdeep Bhanot , Rahul Hans, "A Review and Comparative Analysis of Various Encryption Algorithms ", International Journal of Security and Its Applications Vol. 9, No. 4 (2015), pp. 289-306.

[13] S. Masadeh W.Salameh(2007). "End to end keyless self-encrypting/decrypting streaming cipher", Information Technology & National Security Conference 2007.

[14] Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma, "Analysis and Comparison between AES and DES Cryptographic Algorithm Shraddha", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012.

[15] Singhal, Nidhi and Raina, J P S (2011)."Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, ISSN: 2231-280, July to Aug Issue 2011, pp. 177-181. International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.3, May 2015 38

[16] Singh, S Preet and Maini, Raman (2011)."Comparison of Data Encryption Algorithms", International Journal of Computer Science and Communication, vol. 2, No. 1, pp. 125-127.

[17] Sombir Singh, Sunil K Maakar, Dr. Sudesh Kumar," A Performance Analysis of DES and RSA Cryptography", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 3, May – June 2013 ISSN 2278-6856.

[18] William Stallings, "CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE", FIFTH EDITION, Copyright © 2011, 2006 Pearson Education, Inc., publishing as Prentice Hall.