Journal of Harbin Engineering University
ISSN: 1006-7043
Vol. 44 No. 7
July 2023

Comparative Study of Various Parameters of Des and AES Encryption Schemes

K P Saurabh[1]

[1]Research Scholar, Department of Computer Science and Engineering, Dr. A. P. J. Abdul Kalam University, Indore, Madhya Pradesh

Dr. Kailash Patidar[2]

[2]Supervisor, Department of Computer Science and Engineering, Dr. A. P. J. Abdul Kalam University, Indore, Madhya Pradesh

ABSTRACT

The amount of information transmitted via the Internet and other forms of media has increased dramatically. It is important to prevent unauthorized parties from gaining access to this Data since it may include sensitive information. The primary method of protecting this information is through the use of encryption methods. There is a wide range in efficiency among the available encryption techniques. There are still problems with the use of cryptographic algorithms in our modern environment, despite the widespread adoption of such methods. Some are great at encrypting data like photos and text files, while others are more adept at communicating across networks. In light of this, encryption has emerged as a viable solution for ensuring security in the modern world. The various suggested picture encryption systems, each with its own set of advantages and disadvantages, only add to the complexity of the problem. In this study, we compare and contrast some aspects of the DES and AES encryption algorithms.

Keywords: Cryptography, Block Cipher, Decryption, Security, Deciphering

I. INTRODUCTION

Pigeons were used to deliver messages in the past. Since then, civilization has progressed greatly, giving rise to numerous new communities, nations, and empires. This development stoked thoughts of conflict and power struggles. Politics and power prompted an increase in the necessity for clandestine communication among the populace, which in turn sparked the development of cryptography. It all began with refined methods of encoding, and by the end of World War II, cryptography had become entirely mathematical. Currently, two distinct varieties of cryptography are in widespread use. The first, known as secret-key cryptography, has been around since the early 1900s; the second, known as public-key cryptography, has only been in use since the late 1970s.

The method of deciphering ciphertext is akin to deciphering a coded message, and the process of deciphering ciphertext is similar to deciphering a secret message. Two distinct methods of encryption and decryption are in use today. Two factor authentication with symmetric and asymmetric keys.Sender and receiver share the same key in symmetric key cryptography, while with asymmetric key cryptography, they utilize distinct keys. The RSA family of algorithms is an example of asymmetric key cryptography, whiles the DES, AES, 3DES, IDEA, Blowfish method, etc., are all examples of symmetric key encryption.

Cryptography is the practice and study of making data secure from prying eyes by transforming it into an indecipherable format before storing or transmitting it. Encryption is the primary tool used in data cryptography, and it is used to render data such as text, images, audio, and video unrecognizable or incomprehensible during transmission or storage. The primary purpose of cryptography is to protect information from prying eyes.

Decryption is the process of restoring original, unencrypted data.

II. CRYPTOGRAPHY WITH BLOCK CIPHER

A block cipher is a type of symmetric key cipher used in cryptography.To create encrypted text, a block cipher applies a cryptographic key and algorithm to a block of data (for instance, 64 contiguous bits) all at once, rather than to each bit individually.

A block cipher is a type of cryptographic hashing algorithm that encrypts information so that only those with the key may decrypt it. A second input, the secret key, regulates the precision of the transformation. A 128-bit block of cipher text and the secret key are used in the corresponding decryption process, which returns the original 128-bit block of plaintext. A stream cipher, in contrast to a block cipher, encrypts a single number at a time, and its transformation changes as it goes.

Data Encryption Standard (DES, a method of encrypting information) is a block cipher design that has had a significant impact on the development of modern cryptography. The Data Encryption Standard (DES) block cipher, a pioneering encryption algorithm developed in the mid-1970s, was sanctioned by the National Institute of Standards and Technology (NIST). Classified design components, a low key length of the symmetric-key block cipher architecture, and NSA cooperation all contributed to initial controversy, fueling rumors of a backdoor. Many modern programs now avoid using DES because of security concerns. In January 1999, distributed.net and the Electronic Frontier Foundation worked together to publicly crack a DES key in 22 hours and 15 minutes, mostly because the key size was too short at 56 bits. Some theoretical flaws in the cipher have also been demonstrated by analytical results;however they are impossible to mount in practice. Triple DES is a variant of the algorithm that is thought to be theoretically safe despite existing vulnerabilities. The encryption has been replaced in recent years by the more secure Advanced Encryption Standard (AES).

A. Data Encryption Standard (DES)

The Data Encryption Standard (DES) symmetric algorithm was the de facto standard for protecting sensitive information. DES encrypts data 64 bits at a time since it is a 64 bit block cipher. This is in contrast to stream ciphers, which encrypt data in discrete chunks of time, often one bit at a time. The Feistel block cipher is the basis for DES. In the early 1970s, IBM cryptography researcher Horst Feistel created this block cipher. Each cycle includes exclusive OR operations, non-linear substitutions (Sboxes), and bit shuffling. The plaintext and the secret key are both required for DES to perform its encryption function. The nature of this cipher is determined by how the plaintext is accepted and the structure of the keys used for encryption and decryption. Since the same key is used for both encryption and decryption, and since DES only processes data in 64-bit blocks at a time, we may classify it as a symmetric, 64-bit block cipher. Figure 1 shows the overarching design of the DES encryption system.

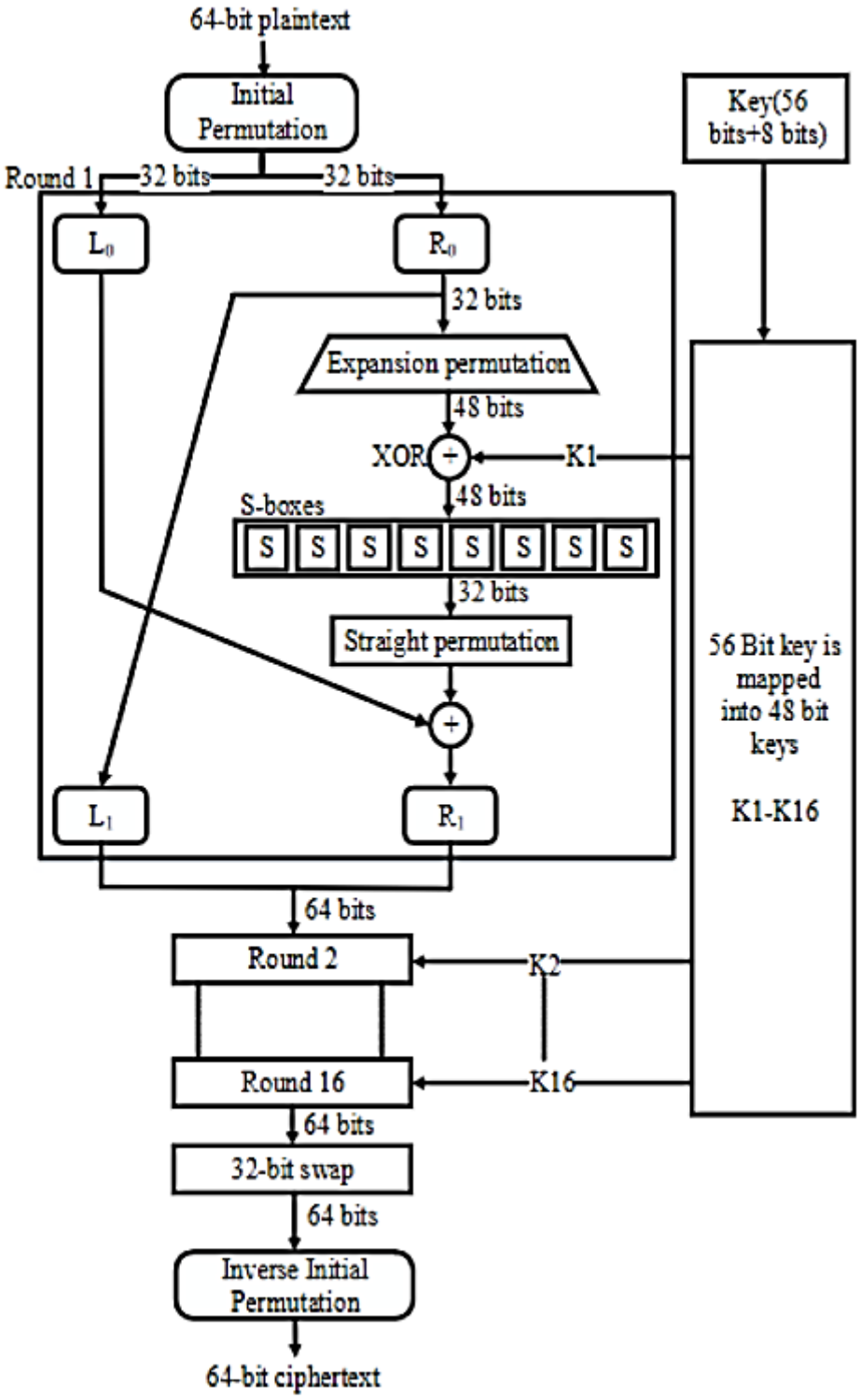

Figure 1: DES Encryption algorithm

B. Advanced Encryption Standard(AES):

The 128-bit blocks used by AES make it a block cipher. AES supports keys of 128, 192, and 256 bits in length. For 128-bit keys, 10 iterations of processing are required for encryption, whereas 192-bit keys require 12 iterations, and 256-bit keys require 14. One byte is swapped out for another, rows are permuted, columns are mixed, and the round key is added at the end of each processing cycle. These four operations, encryption and decryption, are performed in opposite orders. In contrast to DES, the encryption and decryption algorithms here are

very different from one another. Encryption and decryption both employ the same basic techniques, but as was previously indicated, the sequence in which they are performed is different. The basic architecture of AES encryption is seen in Figure 2.

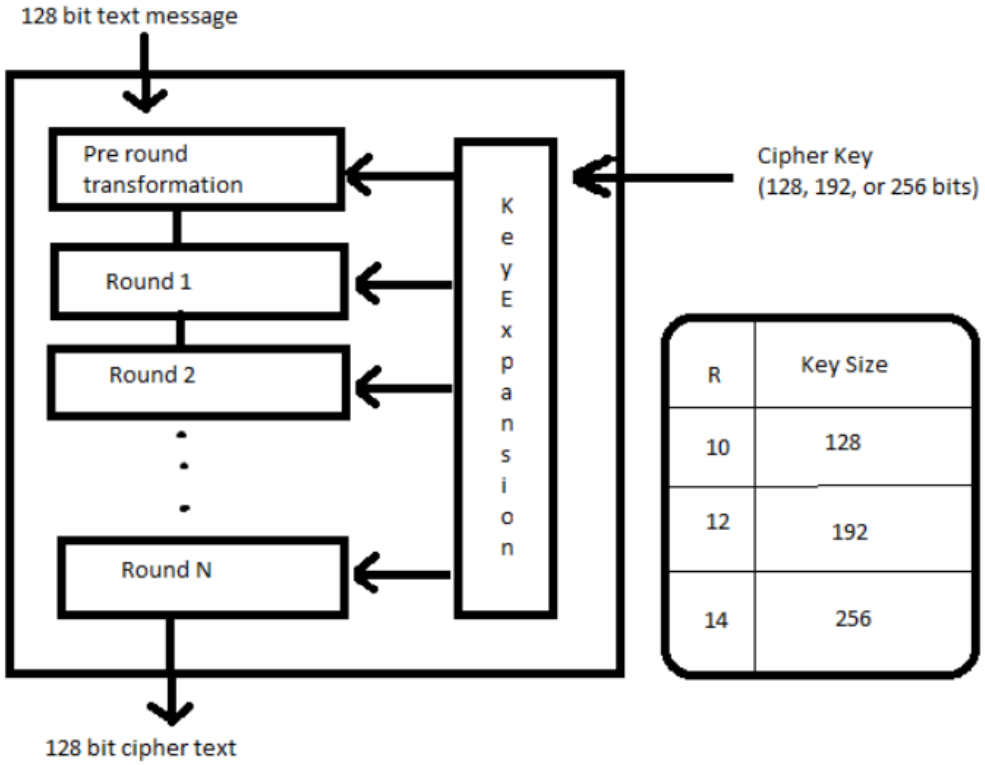

Figure 2: Advanced Encryption algorithm

III. COMPARISON OF AES AND DES

AES (Advanced Encryption Standard) is a more secure encryption algorithm than DES (Data Encryption Standard), to put it simply.

Table 1: Comparison table of AES and DES

S. No.	Factors	AES	DES
1.	Developed	2000	1977
2.	Key Size	128 , 192 , 256 bits	56 bits
3.	Block Size	128 bits	64 bits
4.	Ciphering and Deciphering key	Same	Same
5.	Algorithm	Symmetric	Symmetric
6.	Encryption	Faster	Moderate
7.	Decryption	Faster	Moderate
8.	Power Consumption	Low	Low

9.	Security	Excellent Secure	Not Secure Enough
10.	Deposit of Keys	Needed	Needed
11.	Inherent Vulnerabilities	Brute Force Attack	Brute Force, Linear, differential cryptanalysis attack
12.	Key Used	Same key for encryption and decryption	Same key for encryption and decryption
13.	Rounds	10/12/14	16
14.	Simulation Speed	Faster	Faster
15.	Trojan Horse	Not Proved	No
16.	Hardware and Software Implementation	Faster	Better in hardware than Software
17.	Ciphering and Deciphering Algorithm	Different	Different

IV. RESULTS OF COMPARISON BETWEEN AES AND DES BY USING ONLINE ENCRYPTION TOOL

According To ECB Mode

Table 2: Comparison between AES and DES in ECB block cipher mode

S. No.	File Size (kb)	DES Computation Time (in sec)	AES Computation Time (in sec)
1.	4.44	3.29	4.06
2.	13.6	3.90	4.57
3.	23.6	4.09	5.58
4.	39.5	5.16	6.52
5.	40.8	5.82	6.00
6.	46.9	5.48	6.20
7.	49.7	4.91	5.65
8.	51.9	6.05	6.85
9.	90.6	5.00	5.68
10.	93.6	6.27	7.86

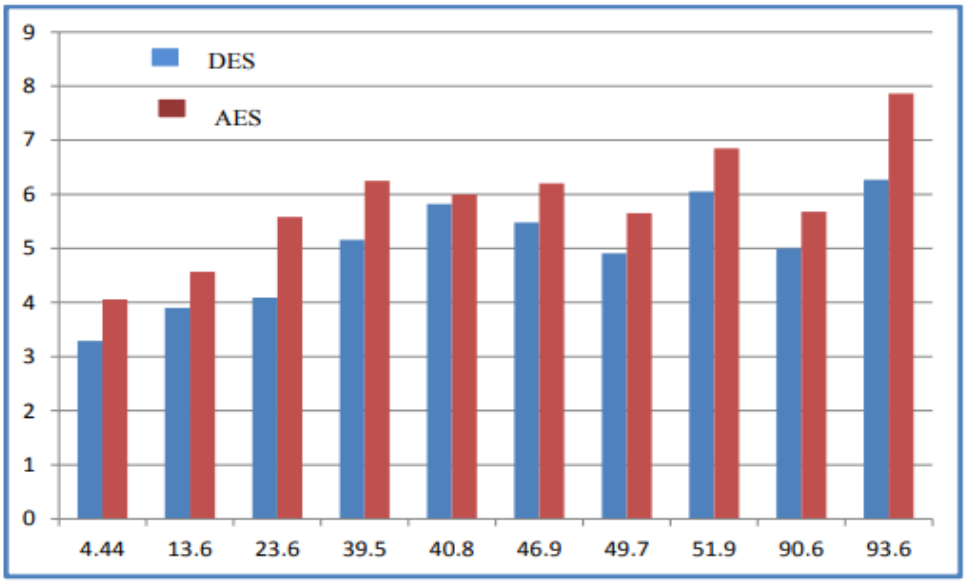

Figure 3: Comparison graph between AES and DES in ECB mode

According to CBC modeL

Table 3: Comparison between AES and DES in CBC block cipher mode

S.No.	File Size (kb)	DES Computation Time (in sec)	AES Computation Time(in sec)
1.	4.44	2.31	3.17
2.	13.6	3.70	4.00
3.	23.6	3.23	4.82
4.	39.5	4.84	5.13
5.	40.8	5.04	5.59
6.	46.9	4.42	5.50
7.	49.7	3.63	4.82
8.	51.9	4.55	5.25
9.	90.6	6.11	6.71
10.	93.6	5.06	5.59

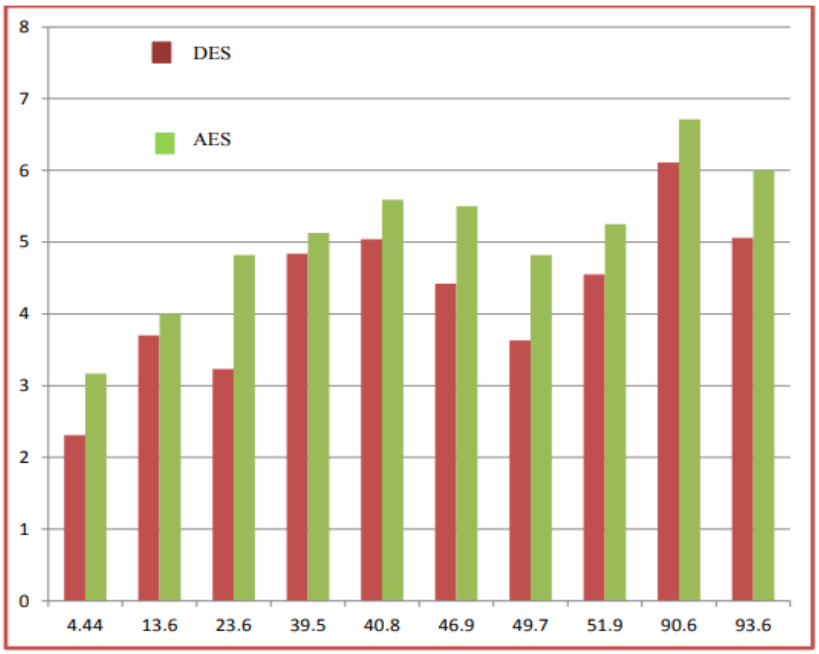

Figure4: Comparison graph between AES and DES in CBC mode

- For both AES and DES we took same file size to compare their computation time of encryption in both of modes ECB and CBC.

- Here we took readings for 10 file size, size is already given in both the table.

- The computation time for both algorithm is different so we major computation time for both algorithms in sec. By the computation time we can compare both algorithms that which one is better and which algorithm is more precise then other.

- Computation time helps me to prepare comparison graph between AES and DES algorithm.

- The computation time is varies with the size of file.

- Computation time is directly proportional to the file size. Maximum the file size maximum the computation time.

- In both the mode ECB and CBC the computation time for both algorithms is different.

- In ECB mode the encryption is done in the electronic code book. In which every block of the file is encrypted individually. At the last we get output which is combination of all the cipher text .

- In CBC mode the encryption is done in cipher block chaining pattern. In which plain text is Ex-or with initialization vector (IV) and then going for encryption.

- For the next block the output of previous block is Ex-or with current plain text, and going for encryption.

V. CONCLUSION

The security provided by an encryption technique is crucial in the realm of communication.This study compares and contrasts the security provided by the AES and DES cryptographic algorithms and argues that the latter should be employed whenever possible within automated teller machines (ATMs). Experimental results and analysis of the input text files led to the conclusion that the AES

method required less time for both encryption and decryption than the DES approach. DES can be employed in less-sensitive scenarios, whereas AES is reserved for the most sensitive ones. Compared to DES, AES is more secure since it utilizes a substitution and permutation approach to encrypt, and because it supports keys with lengths of 128, 192, and 256. It offers a higher and higher level of protection.

REFERENCES: -

1. Chittibabu, Priya. (2019). A Comparative Analysis Of DES, AES and RSA Crypt Algorithms For Network Security in Cloud Computing. 6. 574-82. 10.1729/Journal.19997.

2. RajdeepBhanot , 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.

3. S.Kumari and J. Chawla, Comparative Analysis on Different Parameters of Encryption Algorithms for Information Security, International Journal of Innovations & Advancement in Computer Science (IJIACS), Volume 4, Special Issue, pp. 123-129, 2015.

4. S. Gurpreet and Supriya,A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information SecurityInternational Journal of Computer Applications, Volume6, Issue 19, pp. 33-38, 2013.

5. Pasmavathi B. and Ranjitha S.A Survey Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique: International Journal of Science and Research (IJSR) Volume 2, Issue 4, pp. 170-174,2013.

6. K.Aman, J. Sudesh and M.Sunil, Comparative Analysis between DES and RSA Algorithm's: International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7,pp. 386-391,2012.

7. K.Ajah, M.Singh and P. Bansel, Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network. International Journal of Engineering and Technology, Volume 2, Issue 1, pp.87-92, 2012.

8. 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.

9. H.O.Alanazi, B.B.Zaidan, A.A.Zaidan, H.A.Jalab, M.Shabbir and Y.Al-Nabhani,New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal of Computing, Volume 2, Issue 3, pp.152-157, 2010.