https://doi.org/10.46335/IJIES.2024.9.6.16 **e-ISSN: 2456-3463**
Vol. 9, No. 6, 2024, PP. 73-76

International Journal of Innovations in Engineering and Science, www.ijies.net

Comparative Evaluation of DES and AES Algorithms in Network Security

Shruti Bhande . Aayushi Salbarde , Tejas Budhbaware

Student, Department of CSE (Cyber-Security), St. Vincent Pallotti College of Engineering & Technology, Nagpur, Maharashtra, India- 441108

shrutibhande14@gamil.com

***Received on**: 5 May,2024* ***Revised on**: 29 June,2024* ***Published on**: 01 July ,2024*

Abstract: *In the contemporary digital geography, securing data during its transmission across networks is consummate. This exploration paper aims to conduct an in- depth analysis of the Data Encryption Standard(DES) and the Advanced Encryption Standard(AES) algorithms, exploring their separate places in bolstering network security. These encryption algorithms serve as critical factors in icing the confidentiality and integrity of data exchanges over networks. This paper undertakes a thorough disquisition of the underpinning principles, methodologies, and attributes of DES and AES, aiming to assess their efficacity in terms of security and effectiveness. By comparing and differing the two algorithms, this study trials to determine which algorithm offers superior performance in enhancing network security.*

Keywords: *DES Algorithm, AES Algorithm, Network Security, Encryption, Decryption, Comparative Evaluation*

1. INTRODUCTION:

Network security plays a vital part in securing druggies' data while they browse websites on waiters via the internet, without revealing the position of their bias. This study aims to explore the generalities underpinning the DES and AES algorithms, fastening on encryption and decryption, and determine which algorithm offers superior security and speed.

Both DES and AES algorithms are pivotal for cracking and decoding data transmitted over networks, icing sequestration and protection against unauthorized access. Popular ways like RSA and Blowfish also contribute to this bid.

1.1. DES Algorithm Overview :

DES, or Data Encryption Standard, operates as a block cipher, employing the same key for both encryption and decryption. It processes dispatches in 64- bit blocks, conforming of 16 rounds in a Feistel round structure.

1.2. AES Algorithm Overview :

The AES algorithm, standing for Advanced Encryption Standard, employs symmetric block encryption, where the same key is employed for both encryption and decryption processes. AES operates on 128- bit data, with the number of rounds determining its security and complexity. The table below illustrates the relationship between the number of rounds and the corresponding crucial sizes:

No. of Rounds	Key Size
10	128 bits
12	192 bits
14	256 bits

This table provides information on the different rounds used in AES encryption, with the number of rounds decreeing the position of security and the associated crucial size.

2. METHODOLOGY:

2.1 Steps for DES Algorithm :

- original Permutation: Involves rearranging the bits of a 64- bit data block, where specific bits shift positions.

- Feistel Rounds: Execute 16 rounds of encryption.
- Swapping/ Left-Right exchange: Exchange the positions of left and right halves of the data.
- Final Permutation/ Inverse original Permutation: Reverts the original permutation to gain the final translated affair. In the DES algorithm, the process begins with the original permutation round, where the 64- bit plaintext undergoes a scrupulous rearrangement of its bit.

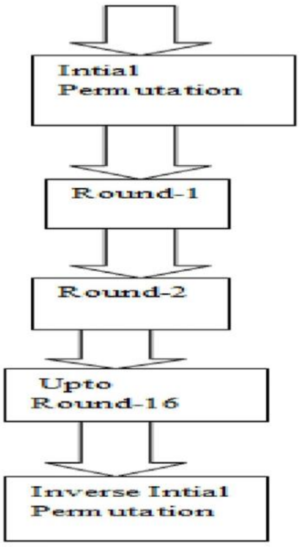

Fig. 2.1.1. Steps of DES algorithm.

This step is pivotal as it sets the sta for posterior cryptographic operations. Durin the original permutation, specific bit positions are altered according to a predefined pattern, icing an effective scrabbling of the plaintext. Following the original permutation, the plaintext proceeds through a series of 16 Feistel rounds, a abecedarian element of the DES encryption process. Each Feistel round operates on a portion of the plaintext, known as a" block," and involves multiple intricate operations, including permutation, negotiation, and crucial mixing. Importantly, a unique 48- bit crucial is employed for each round, enhancing the security and complexity of the encryption process.

Throughout the Feistel rounds, the plaintext undergoes a complex metamorphosis, guided by the named keys and the underpinning cryptographic functions. These rounds serve to completely obscure the original plaintext, making it extremely challenging for unauthorized parties to decrypt the translated data.

Upon completing the Feistel rounds, the translated plaintext is subordinated to inverse permutation, a critical step in the DES algorithm. Inverse permutation effectively reverses the original rearrangement, restoring the translated data to its original 64- bit format. This final permutation ensures comity and thickness in the encryption process, easing flawless decryption at the entering end.

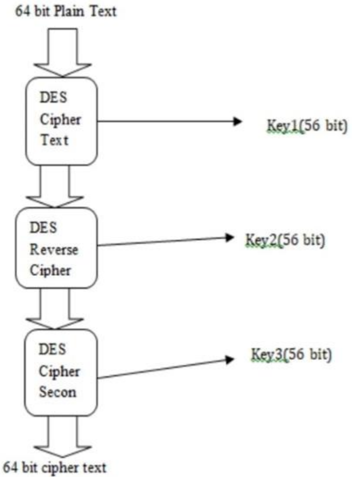

Fig. 2.1.2. Division Operation in DES

Eventually, the capstone of these intricate way yields the ciphertext, a largely secure and ungraspable representation of the original plaintext. Through its scrupulous design and rigorous cryptographic mechanisms, the DES algorithm provides robust protection for sensitive data transmitted over networks. The 32- bit data undergoes expansion, expanding it to 48 bits. latterly, an XOR operation is performed between the expanded data and a 48- bit crucial, performing in a 48- bit affair. This affair is also reused through negotiation boxes(S- boxes), where the 48- bit value is converted into a 32- bit value.

During the crucial generation process, the original 64- bit crucial undergoes a permutation known as" permuted choice- 1(PC- 1), performing in a 56- bit crucial. This 56- bit crucial is also divided into two equal corridor, denoted as Co and Do. Multiples of 8 bits are discarded, yielding 8 corridor of 7 bits each. These bits suffer left shifts in each round of the encryption process.

In specific rounds(i.e., rounds 1, 2, 9, and 18), the bits are rotated by one position, while in other rounds, the two halves are rotated by two positions. After shifting, the performing labors(C1 and D1) serve as inputs for another permutation process known as" permuted choice- 2"(PC- 2), where the 56- bit crucial is reduced to 48 bits by discarding multiples of 8 bits. This process yields the first key for round 1, with C1 representing the first 28 bits and D1 representing the coming 28 bits.

2.2 Steps for AES Algorithm :

The AES algorithm begins with a 128- bit plaintext as input. The original step involves apre-round metamorphosis, during which a 128- bit crucial, denoted as k0, is employed. The number of cipher rounds is contingent upon the ciphertext. Upon completion of the final round, a 128- bit ciphertext is produced as affair.

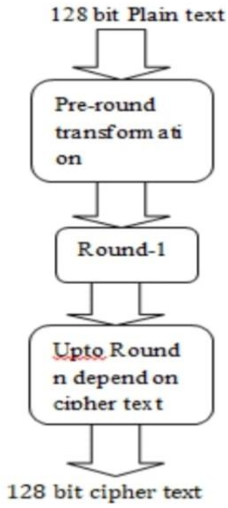
128 bit Plain text
Pre-round transform ati on
Round-1
Upto Round n depend on cipher tex t
128 bit cipher text

Fig . 2.2.1. Steps of AES algorithm

During the encryption process of AES, the 128-bit plaintext undergoes addition with the round key. The "Add Round Key" operation comprises several functions, including:

1. Sub-bytes: This operation involves utilizing predefined S-boxes, which contain tables for substituting bytes. The resulting output is represented in a 4x4 matrix format.

2. Shift Rows: This operation involves shifting the rows of the matrix to achieve diffusion and confusion.

3. Mix Columns: This operation performs a linear transformation on the columns of the matrix, enhancing the cryptographic strength of the algorithm.

4. Add Other Round Key: This step involves adding the round key generated for the current round.

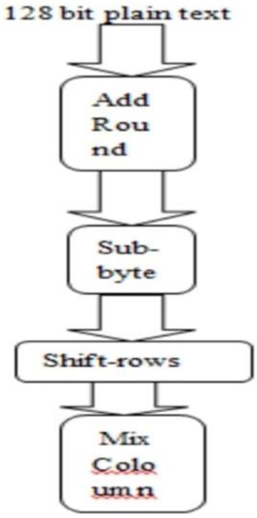

Fig.2.2.2. Process of AES algorithm

Together, these operations contribute to the robust encryption process of AES, ensuring the security and confidentiality of the transmitted data.

3.CONCLUSION:

The AES algorithm offers a robust encryption mechanism, utilizing a 128-bit plaintext and a series of operations including pre-round transformation, "Add Round Key," and various functions like Sub-bytes, Shift Rows, and Mix Columns. These operations ensure the generation of a secure 128-bit ciphertext, enhancing data confidentiality in communication.

In the methodology section, various methods, tools, and techniques were employed to achieve conclusive results. The objectives focused on acquiring new knowledge, assessing thesis necessity, updating tools, and stimulating human understanding, guiding the research process towards successful completion.

Data collection proved to be a challenging yet crucial task, requiring meticulous gathering and arrangement of information from multiple sources. Utilizing websites such as www.cisco.com and www.economictimes.com, the research synthesized relevant data, ensuring comprehensive coverage of the topic.

Key concepts such as encryption and decryption were explored, highlighting the process of converting plain text messages into cipher text for secure transmission. The encryption process ensures that only authorized recipients can decipher the encrypted data, enhancing communication security in various contexts.

4.DISCUSSIONS

Advantages:

AES	DES
1 Security more	1 Security less
2 Time complexity is more	2 Time complexity is less
3complex implementation	3 Simple Implementation

Limitations:

AES	DES
1 Key Length Dependence	1 Small key Size
2 Implementation Security	2 Security Vulnerabilities

Applications:

AES	DES
1 Data Encryption	1 Education and Research
2 Government and Military	2 Low-Security Applications
3 Cloud Computing	3 Legacy Systems

REFERENCES

[1] *Shripal Rawal, Advanced Encryption Standard (AES) and It's Working, International Research Journal*

[2] *of Engineering and Technology (IRJET), Volume: 03 Issue: 08, 2016.*

[3] *[2] Douglas Selent, ADVANCED ENCRYPTION STANDARD, RIVIER ACADEMIC JOURNAL, V6, NUMBER 2,*

[4] *2010.*

[5] *[3] Dr. Prerna Mahajan, Abhishek Sachdeva, A Study of Encryption Algorithms AES, DES and RSA for*

[6] *Security, Global Journal of Computer Science and Technology Network, Web & Security, Volume 13*

[7] *,Issue 15, 2013.*

[8] *[4] Kefa Rabah, Theory and implementation of data encryption standard: A Review, Research Gate, 2005*

[9] *[5] Fahmi Ruziq, Poltak Sihombing, Sawaluddin, Combination Analysis of Data Encryption Standard (DES)*

[10] *Algorithm and LUC Algorithm on File Security, International Journal of Research and Review, Vol.7,*

[11] *Issue: 2, 2020.*

[12] *[6] Nirmaljeet Kaur, Sukhman Sodhi, Data Encryption Standard Algorithm (DES) for Secure Data*

[13] *Transmission, International Conference on Advances in Emerging Technology, 2016.*

[14] *Abhishek Yadav, Ms. Richa Sharma, SECURE AND IMPROVED APPROACH FOR 3-DES ALGORITHM*

[15] *AGAINST CRYPTOGRAPHIC ATTACKS, International Science Press, 2016.*

[16] *Meixi Chen, Accounting Data Encryption Processing Based on Data Encryption Standard Algorithm, Hindawi, Volume 2021, 2021.*

[17] *https://youtu.be/UUoBOKq1IxQ.*

[18] *https://youtu.be/YVT4fcW7sI8.*

[19] *https://youtu.be/eMHcQByhR-g.*

[20] *https://youtu.be/vj7HJ56mdiw.*