International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-12 Issue-6, May 2023

Improved Data Encryption Standard Algorithm using Zigzag Scan for Secured Data Transmission

S. Hemasri, S. Kiran, A. Ranichitra, A. Rajesh Kanna

Abstract: ***The cryptosystem is a combination of cryptographic algorithms used to provide security services for the information. One of them is the Data Encryption Standard, also known as DES, which is a symmetric-key block cypher released by the National Bureau of Standards (NBS). DES is a block cypher that performs encryption of each 64-bit block. Encryption of the data using an algorithm that translates the original data into an unreadable format, making it difficult for an intruder to attack. The DES is more secure than other cryptosystems because the time required for cryptanalysis has been minimised. Due to advancements in hardware techniques, the traditional DES may be vulnerable to various kinds of attacks through different cryptanalysis methods. This paper presents a new design of DES called the Improved DES, which demonstrates that the Improved DES is more secure than the DES against differential cryptanalysis. It divides each substitution box into four sub-blocks of 16 bits and then applies the zig-zag function to each of these sub-blocks. It improves the standard encryption levels by columnar transposition.***

Keywords: Cryptography, DES, Zigzag Scan, Key Generation.

I. INTRODUCTION

Nowadays, data has become the biggest resource for every organisation, whether it is confidential or non-confidential. It is a significant challenge for the organisation to provide security for confidential data, i.e., data that is not shared with others. Different kinds of attacks on major organisations aim to steal data. Therefore, providing security is the primary concern.

A. Cryptography

Cryptography is all about the techniques supporting private and secure communications. It attempts to preserve the integrity of data and curb snoops from reading it. It is the study of techniques and procedures used to secure information by making it unreadable to unintended recipients. Here are some cases where cryptography played a significant role in protecting your communication:

Manuscript received on 04 April 2023 | Revised Manuscript received on 25 April 2023 | Manuscript Accepted on 15 May 2023 | Manuscript published on 30 May 2023.

*Correspondence Author(s)
S. Hemasri*, Ph.D (Pursuing), Department of Computer Science, Madurai Kamraj University, Madurai (Tamil Nadu), India. E-mail: hema0129@gmail.com, ORCID ID: https://orcid.org/0009-0001-6103-0276
Dr. S. Kiran, Associate Professor, Department of Computer Science and Engineering, Yogi Vemana University, Ganganapalle (A.P.), India. ORCID ID: https://orcid.org/0000-0002-0725-3356
Dr. A. Ranichitra, Assistant Professor, Department of Computer Science, S.Ramasamy Naidu Memorial College, Sattur (Tamil Nadu), India. ORCID: https://orcid.org/0000-0001-6071-0635
Dr. A. Rajesh Kanna, Assistant Professor, Department of Computer Science, S.Ramasamy Naidu Memorial College, Sattur (Tamil Nadu), India. ORCID: https://orcid.org/0000-0001-5161-4334

- Logged in to your account by providing your credentials.
- Bought something online through your credit card.
- Sent a message to your friend through instant messaging platforms.

B. Public Key Cryptography

Public key cryptography, also known as asymmetric cryptography, works on a set of keys. The sender uses the receiver's public key to encrypt the data and the receiver's private key to decrypt it.

RSA (Rivest, Shamir, Adelman) and DSA (Digital Signature Algorithm) are two different types of public-key cryptography algorithms. By using PKC, confidentiality can be provided. To perform encryption, the sender must use the receiver's public key, and to decrypt, the receiver uses their unique private key, ensuring that no other person can decrypt the data.

C. Private Key Cryptography

Private key encryption uses the same key for both encryption and decryption. The encryption and decryption processes may lead to key management issues. The main drawback of secret key cryptography is protecting the key when everyone is using the private key.

For example, if a user wants to communicate with different people, they must use different private keys. For a group of N people, it will utilise keys equal to N*(N-1)/2.

D. Methods of Cryptography

- Symmetric Cryptography
- Asymmetric Cryptography
- Hashing

a. Symmetric Cryptography

In symmetric cryptography, both the sender and receiver use a common secret key to share encrypted data. That is, symmetric encryption utilises a key to encrypt the plaintext into ciphertext and transfer it to the receiver, where the receiver also applies the same key to decrypt the ciphertext into plaintext.

In block algorithms, the length of bits is encrypted in blocks, whereas in stream algorithms, the data is encrypted in the form of streams. These are the two types of symmetric cryptography algorithms. Some examples of symmetric encryption algorithms are AES, DES, and IDEA. A etc.,

b. Asymmetric Cryptography

Public key cryptography, also known as asymmetric cryptography, works on a pair of keys – a public key and a private key- to protect data from unauthorised access. The data should be encrypted with the public key, but the ciphertext can be decrypted only with the intended recipient's private key.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

To establish a secure connection between two parties, this asymmetric encryption process is also used. It is also used to establish encrypted links between websites and browsers in SSL (Secure Socket Layer) and TLS (Transport Layer Security). Examples of Asymmetric cryptography include ECC (Elliptic Curve Cryptosystem) and DSS (Digital Signature Standard).

c. Hashing

An algorithm that considers an arbitrary amount of input data and generates an encrypted text of fixed size is called a hash function. Hashing is a cryptographic mathematical operation that transforms data into a string of text. Hashing is easy to execute but immensely difficult to reverse. Some of the hashing algorithms include MD5 (Message Digest 5), SHA1 (Secure Hashing Algorithm 1), and SHA256.

E. Decryption Process

The decryption process is the reverse of the encryption process, which converts the received ciphertext into plaintext.

II. LITERATURE SURVEY

- Sombir Singh Et Al [1] proposes a secure communication system which uses a private key cryptography-Data encryption standard (DES). Before the implementation of the DES algorithm, a transposition technique was added to enhance the algorithm's security. Security has been improved, which is particularly evident in the field of communication using the proposed method. When implementing the transposition technique, the attacker must first break the main DES algorithm and then the transposition technique itself.
- Nirmaljeet Kaur and Sukhman Sodhi [2] identifies substitution(confusion) and transposition(diffusion) based on DES is implemented. Some online applications, such as banking systems, are considered insecure for performing encryption using the DES algorithm. In this paper, we present several analytical results that highlight theoretical weaknesses in the cypher. Therefore, to maximize the standard DES algorithm, new level of security is added to it.
- Na Su Et Al [3] proposed paper optimizes the AES algorithm and combines the characteristics of IoT computing resources and storage resources to construct the data encryption standard DESI in the Internet of Things. This paper introduces the data encryption standard DESI for the Internet of Things, based on the AES algorithm, and demonstrates that DESI has higher efficiency than the AES algorithm. Incorporated with the security analysis of DESI, it can be shown that DESI effectively combines efficiency and security, making it a valuable tool for providing encryption protection in the IoT environment.
- Wang sheng and Zhou Jian [4] proposes higher requirements for the security protection technology of information communication. The 3DES algorithm is derived from three rounds of encryption based on the DES algorithm, which utilises shift, XOR, S-box, and other operations. The conclusion is that the information communication data encryption technology proposed in the paper is compared and tested with traditional encryption technology in terms of encryption strength, data processing efficiency, and encryption and decryption time.
- Khalid Ali Hussein Et Al [5] proposed method was a parallel environment has been utilized to construct a new encryption system, based on involving the so-called 'zig-zag' ordering that is used in JPEG data compression. A new three-dimensional chaotic system is developed to overcome the limitations of regular encryption methods.
- Pratibha Chaudhary Et Al [6] identifies that the proposed work is implemented on grayscale images applied on MATLAB version 2016a. The experimental results exhibit that the proposed work provides a good compression ratio. Ultimately, a joint image compression and encryption work is proposed for grayscale images with various dimensions, such as 256x256, 512x512, and 1024x1024, and different sizes.
- Li, S., Zhao, L., & Yang, N. [7] offers a secure triple layer image steganography technique works on zigzag pattern for embedding secret data. This paper employs a triple-layer message security scheme, where the initial two layers are based on cryptographic functions and the third layer is based on steganographic functions. The encrypted bits are enabled within the LSBs of each, with the R, G, and B colour channels applying a zigzag pattern to identify the order in which the encrypted bits are organised.
- Ahmed A. Abd El-Latif Et Al [8] proposes a conventional method for cryptographic techniques depend on mathematical computation-based construction. Quantum walks (QWs) are a universal quantum computational model that inherently possess cryptographic features, which can be leveraged to build efficient cryptographic mechanisms. This paper utilises the features of quantum walks to generate a new S-box method, which plays a prominent role in block cypher techniques for 5G-IoT technologies.
- Shanshan Li Et Al [9] identify an algorithm that works on a chaotic system, which constitutes the two-dimensional Sine Logistic modulation map (2D-SLMM) and the two-dimensional Hénon-Sine map (2D-HSM). The encryption method consists of a zigzag scan, a scramble, a pixel grey value transformation, and dynamic diffusion. The pixel grey value transformation uses a password feedback method. The proposed work is lossless for medical image encryption and decryption. The problems of low-dimensional chaotic maps, such as narrow intervals and specific parameters, are also avoided, in addition to the issues with spectral texture and contour of medical images.
- Harshali D. Zodpe et al. [10] proposed a method that presents a low-cost Field Programmable Gate Arrays (FPGAs) and builds special-purpose hardware for computationally intensive applications, which has become feasible. This paper presents the design for the Hardware implementation of the Data Encryption Standard (DES) based on an FPGA, which applies an exhaustive key search. An

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

iterative and loop-unrolled DES architecture is implemented in this paper.

- Mohit Agarwal [11] proposes a Format Preserving Encryption method achieved with the help of exclusive OR operation, Advance encryption standard (AES), and a translation method for 16-digit numeric data. To minimise database modifications by securing the length and format of input data, the format-preserving encryption method is used. The defects that occur in the proposed method, such as prefix schemes, length-preserving encryption mechanisms, and cycle walking, are overcome by utilising this method.
- Ali Mohammed Ali Argabi and Md Imran Alam [12] identifies an integrated concept DES and AES Algorithms and generates a new algorithm like AEDS. It has been tested with various inputs, including files and strings (AES, DES, and AES), on three different Machines. AEDS Algorithm shows the best results over the two Algorithms because it defeats the drawbacks of those algorithms. Brute force attack is minimised compared to the other two algorithms.

III. DATA ENCRYPTION STANDARD

A. Introduction

The Data Encryption Standard is used to preserve digital data. The encryption process translates plain text into ciphertext. The decryption process converts the ciphertext into the original plaintext.

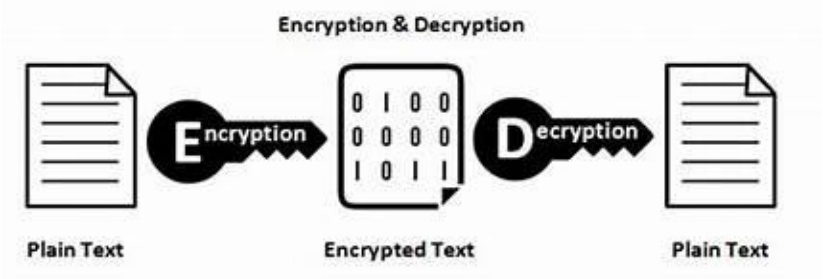


Figure 1: Overall representation of Encryption and Decryption

DES accepts input of 64 bits, and the output is also of a similar size. A 64-bit secret key is considered a second input. It uses a block cypher algorithm, dividing the message into blocks of bits. These blocks of bits passed through substitution, transposition, and other mathematical functions [1].

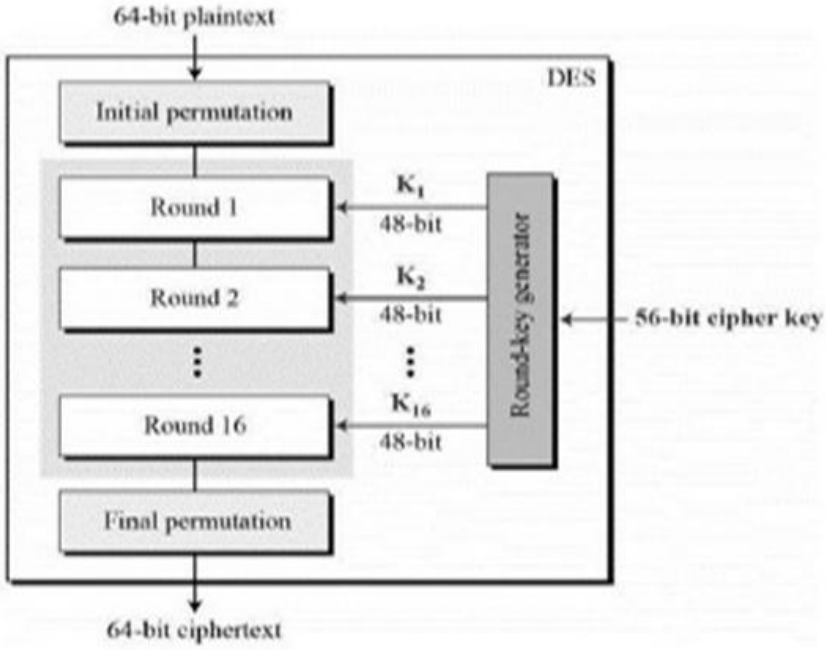


Figure 2: Representation of DES

B. Data Encryption Standard Algorithm

The standard algorithm used by the DES to perform the encryption and decryption process is as follows,

DES Algorithm Steps

DES uses a 64-bit plaintext and transforms it into a 64-bit ciphertext. The algorithm process uses the following steps [2]:

1. Initially, a 64-bit plaintext will be accepted and transferred to the initial permutation round.
2. The initial permutation rearranges the bits into two portions, referred to as the left and right portions.
3. During the encryption process, both the left and right portions undergo 16 rounds of encryption.

4. Finally, the two portions are merged, yielding a final permutation.
5. Finally, a 64-bit ciphertext is generated using the above steps.

C. Initial and Final Permutation

The initial and final permutations are keyless straight permutations, which are reverse to each other [3]. The figure below shows some of the inputs and their equivalent outputs.

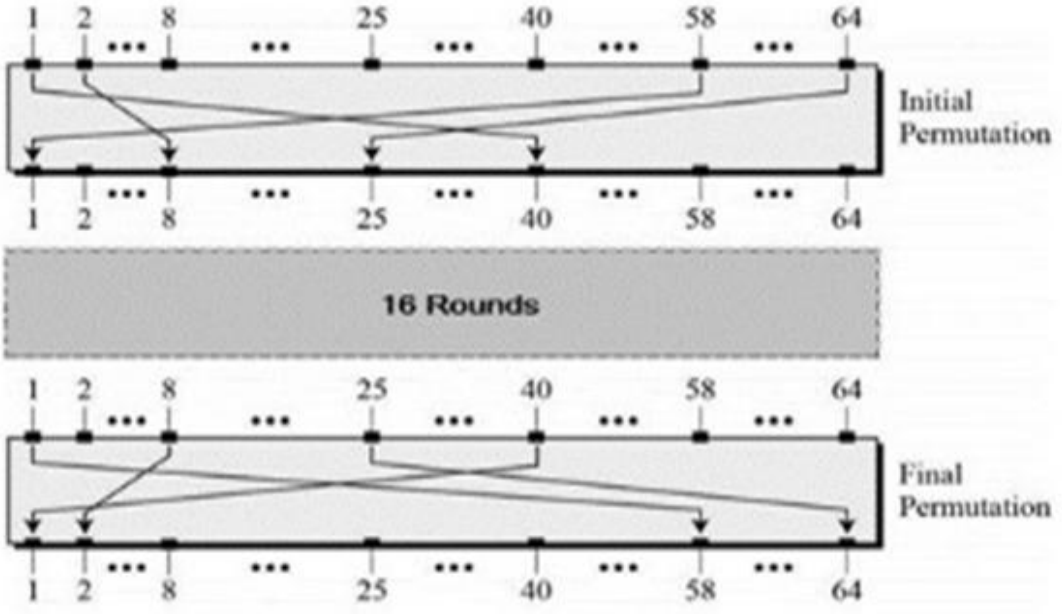


Figure 3: Initial and Final Permutation

D. Round Function

It uses the rightmost 32 bits of a 48-bit key to generate a 32-bit output. During this round, the input is passed through the initial permutation, and then the correct half data (r0) is rounded using the secret key. An XOR operation is performed on the left half of the data (l0), and then the data is transferred to the next round (r1). Similarly, all the round functions up to round 16 are executed, and then the reverse initial permutation is performed. The output bits are then transferred.

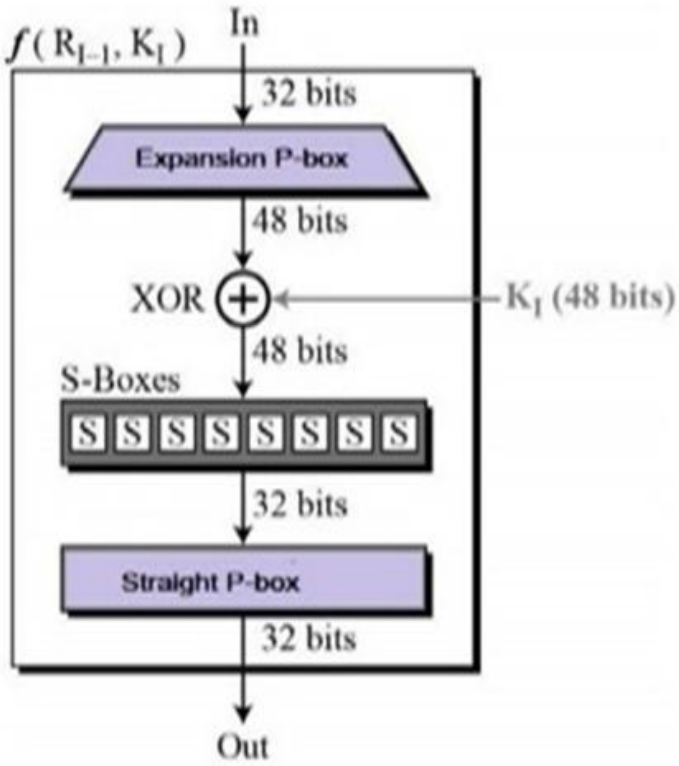


Figure 4: Round Function

- *Expansion Permutation Box* – Due to the use of a 32-bit input and a 48-bit round key, the right portion of the data is expanded to 48 bits. Permutation logic is shown in the figure below

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

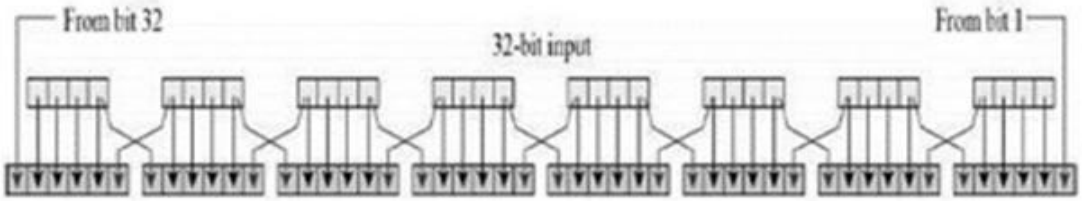


Figure 5: S-Box

The figure below represents a permutation logic as a table

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

Figure 6: Expansion Permutation Box

- *XOR (Whitener)* – To follow the expansion permutation, DES works on the XOR operation on the expanded right portion and the round function.
- *Substitution Boxes* − The S-boxes are used to perform confusion. DES utilizes eight S-boxes, each with a 6-bit input and a 4-bit output, as depicted below

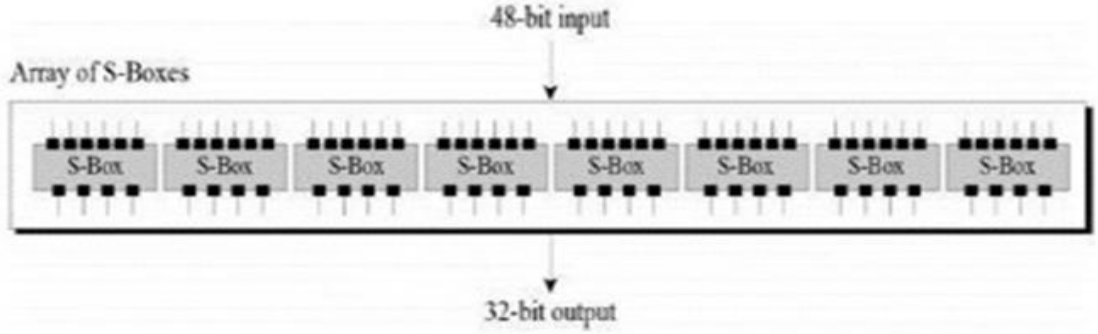


Figure 7: Substitution Box

The S-box rule is shown below

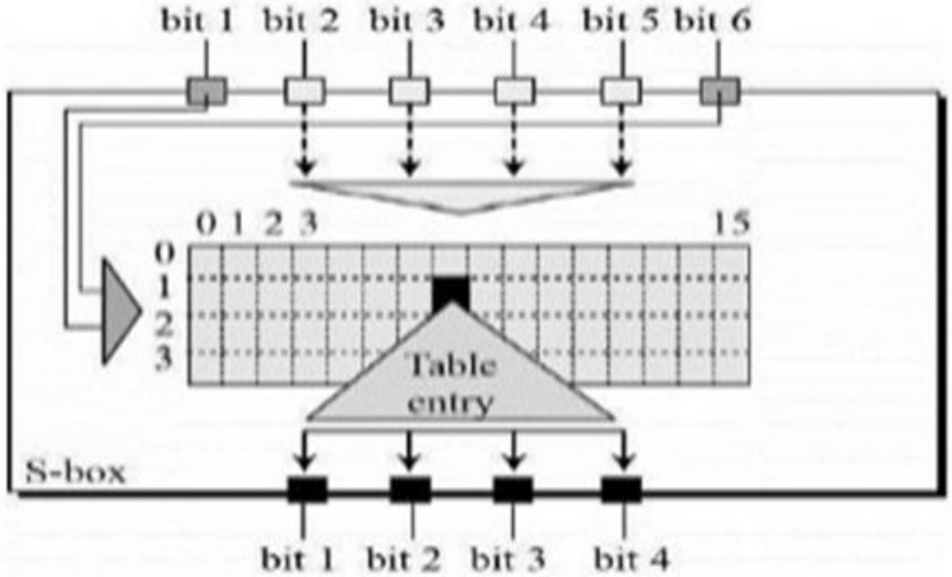


Figure 8: S-box with table

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The sum of eight S-box tables is accepted, and the output is then merged into a 32-bit section.
Straight Permutation – The below figure depicts the S-box output of a 32-bit value passed through the straight permutation.

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

E. Key Generation

A sixteen 48-bit key among 56-bit cypher keys is produced using the round-key generator [4]. The process of key generation is shown in the picture below: –

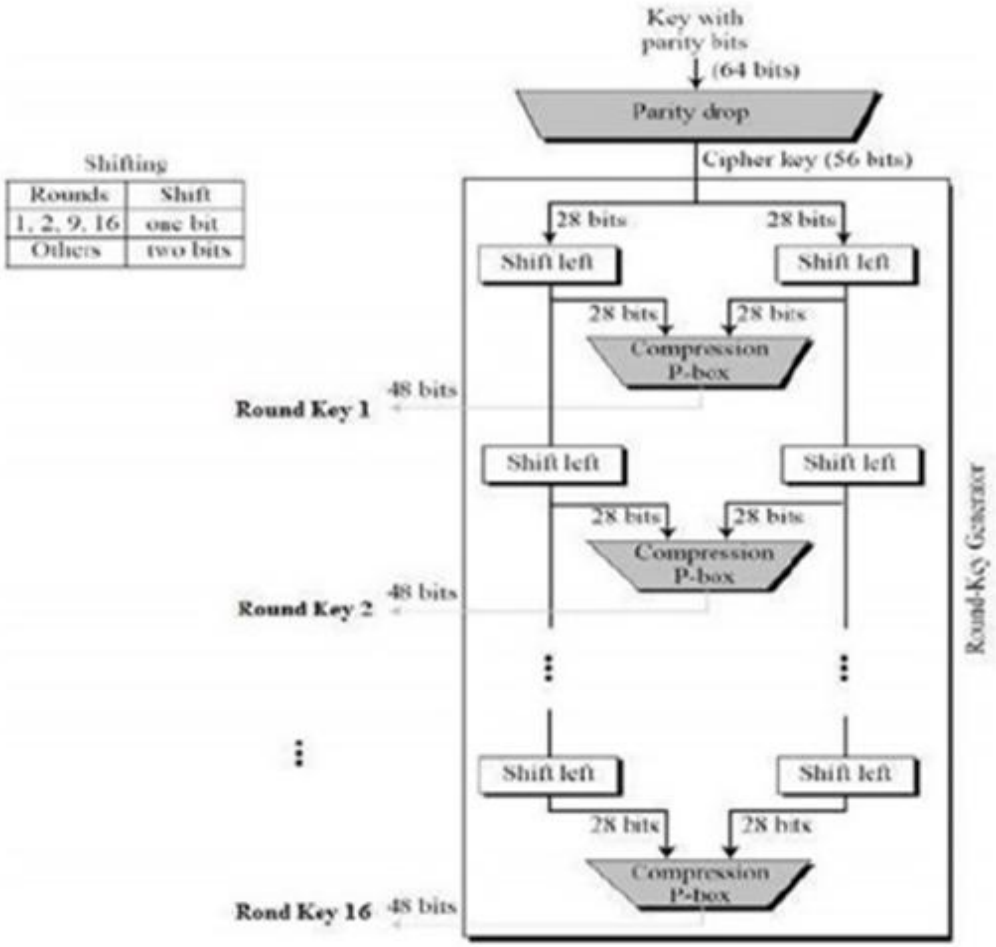


Figure 9: Round Key Generator

F. DES Analysis

The DES analysis can be conducted based on two properties: the Avalanche Effect and Completeness.

IV. IMPROVED DATA ENCRYPTION STANDARD USING ZIG ZAG SCAN

A. Introduction

Numerous hackers have cracked the Data Encryption Standard in recent years, making it vulnerable to compromise by introducing improved DES, which includes functions that are difficult to decrypt unless the key for the plaintext is known. Improved DES ensures that the features in DES cannot be compromised and can be maintained with high security.

B. Zig-Zag pattern

The Zig-Zag pattern (ZZ) is a typical scanning pattern used in image compression, which is performed on the result of the quantisation process, where the pixel values in a 2-D square matrix are reordered into a 1-D matrix. Subsequently, a lossless encoding procedure called RLE is applied to the result of the Zigzag

scan. During scanning, we visit each cell exactly once in some order and create a 1-D matrix. The zigzag pattern scans the 2D square matrix in a horizontal, diagonal, vertical, and diagonal fashion [5].

Starting from the upper left to the lower right.

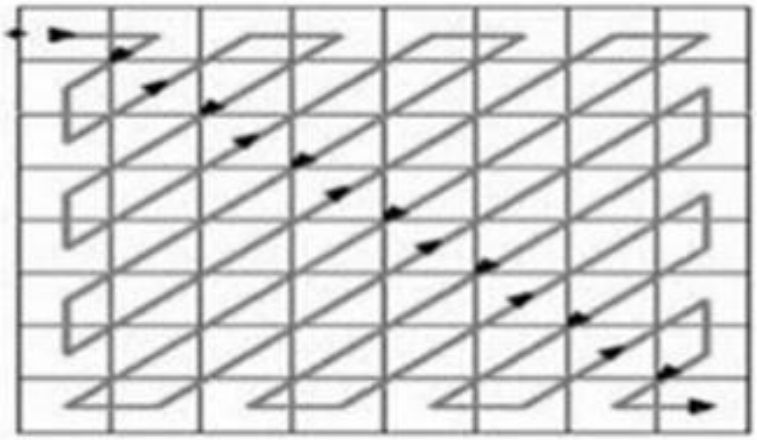


Figure 10: Zigzag Pattern

The algorithm for ZZ is presented below.

Step 0: Initialize row =1 and column =1

Step 1: Move right once by incrementing the column by 1

Step 2: Move to the bottom left by incrementing the row by one and decrementing the column

Example of zig-zag scan:

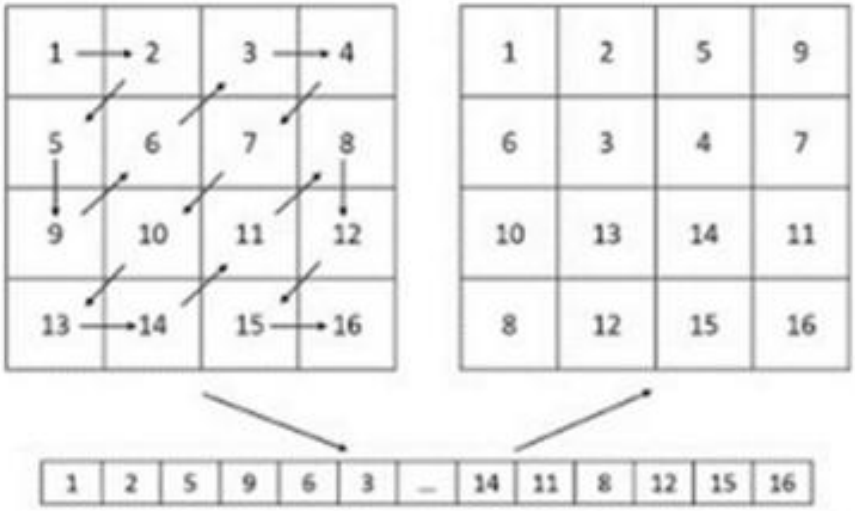


Figure 11: Zigzag Scan

In the given figure, one of the methods of zig-zag scan is shown in the first given

S=1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16

For S, we have applied a zig-zag scan, and then S will be converted to

S=1,2,5,9,6,3,4,7,10,13,14,11,8,12,15,16

C. Columnar transposition method

The Columnar Transposition Cypher is an encryption method that exchanges the columns of a table. Columnar transposition requires plain text written in rows, and then the cypher text is obtained by reading the columns. It rearranges the order of plain text bits—no replacement/substitution.

D. Improved DES Algorithm

The process starts by accepting 64-bit plain text and passing it to the initial permutation.

1. The initial permutation rearranges the bits into two portions, referred to as the left-hand portion and the right-hand portion.
2. Both the left and right portions go through 16 rounds of the encryption process.
3. In the Round function, a zig-zag scan is performed on the SBOX.
4. Then, Columnar Transposition is performed on the result after the zigzag scan of the SBOX.
5. Then, the XOR operation is performed in the round function
6. Ultimately, the left portion and right portion are rejoined, and a final permutation is executed on the recently merged block.
7. A 64-bit ciphertext is produced after accomplishing the above steps.

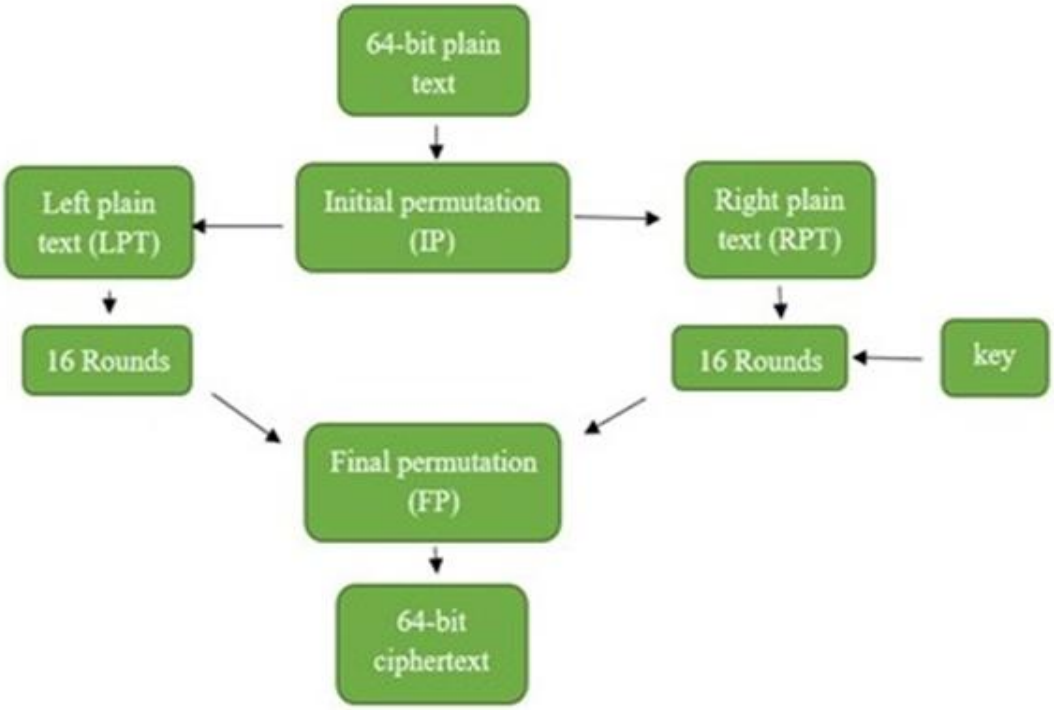


Figure 12: Improved DES

In the above figure, there are 16 rounds, which introduce a function called zigzag scan on the S-box. After this, the process will perform columnar transposition on the SBOX and then continue for 16 rounds.

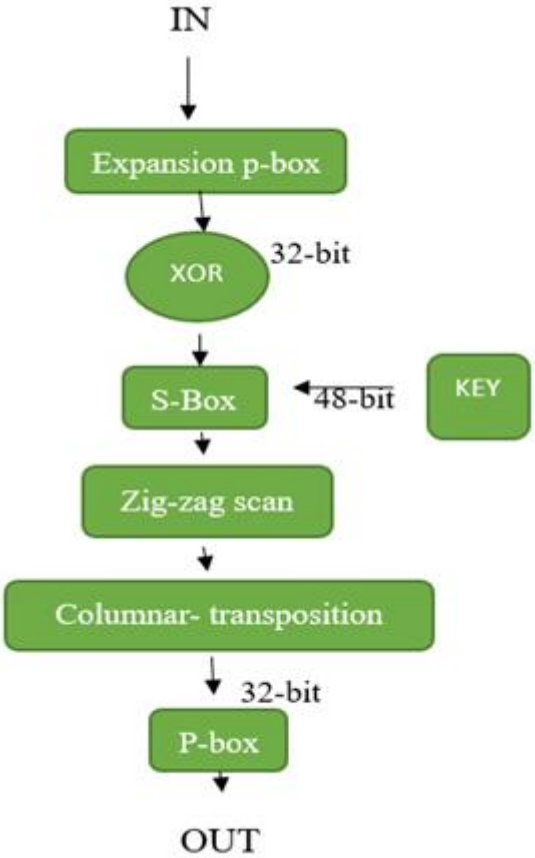


Figure 13: Modified Round function

E. Modified Round Function

From the flowchart, it can be observed that the functions zigzag and columnar transposition are used, and the output of these functions, 32 bits, is given to the p-box, where they are XORed with the left plain text, and then the output is produced for the next round.

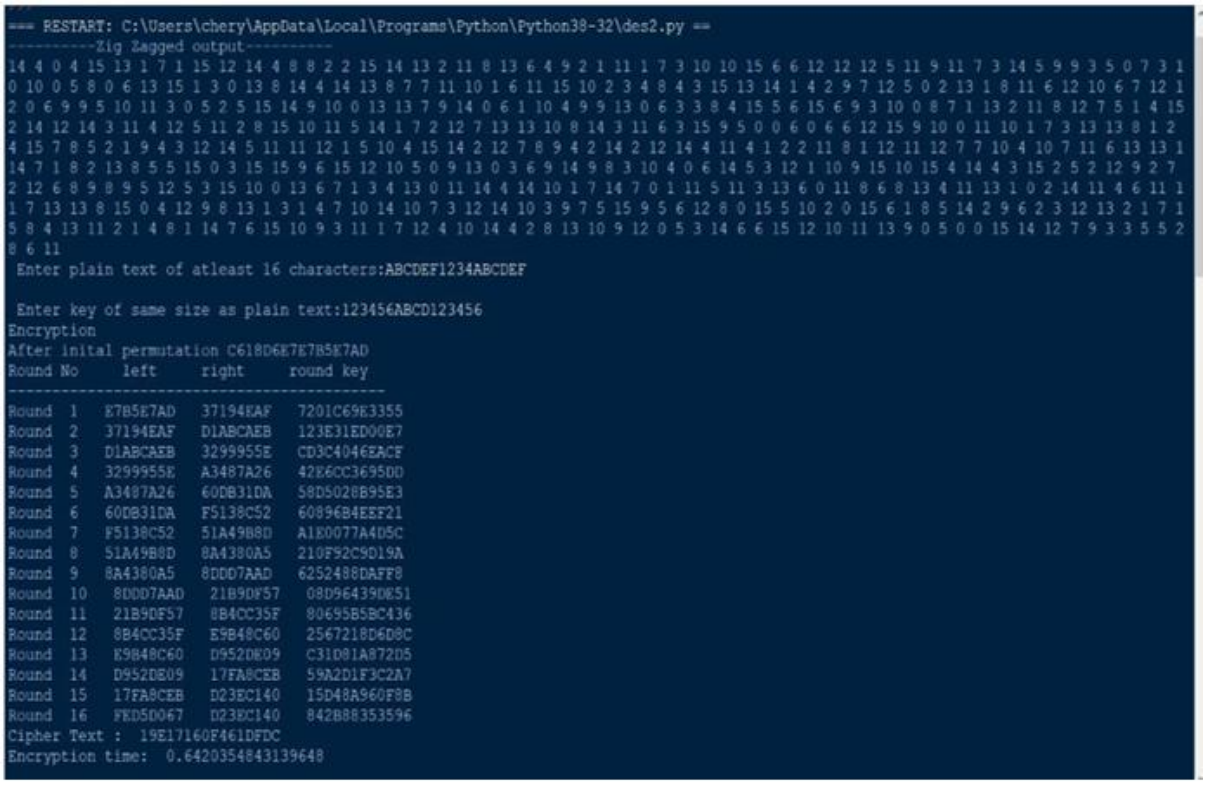
V. RESULTS

Improved DES utilises the Zig-Zag Scan for enhanced results, while maintaining features such as completeness, Avalanche Effect, Encryption Time, and decryption time in seconds. Features of Improved DES include the avalanche effect and Completeness.

Encryption time:0.6420354843139648
Decryption time:0.8394386768341064
Examples for Improved DES

Encryption for case 1

Table 1. Encryption for case 1

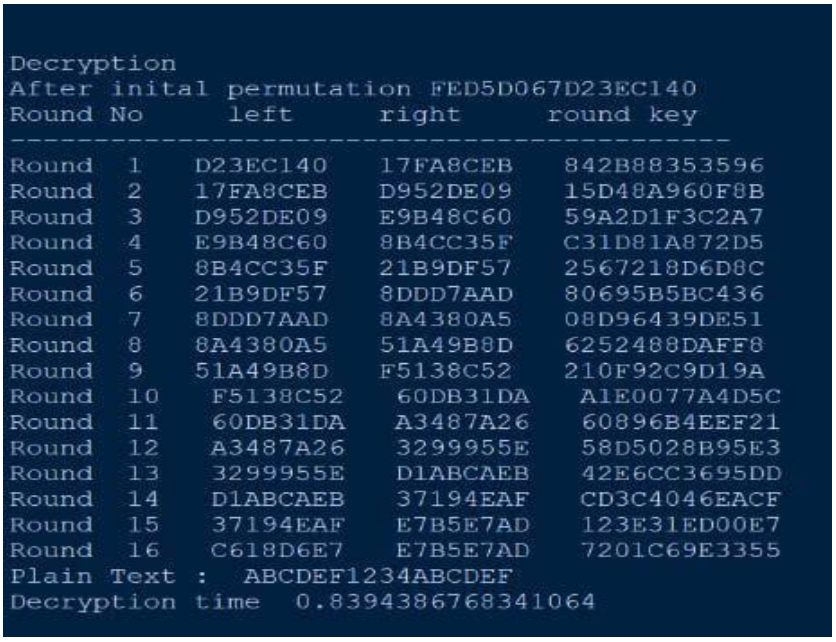


```
=== RESTART: C:\Users\chery\AppData\Local\Programs\Python\Python38-32\des2.py ==
----------Zig Zagged output----------
14 4 0 4 15 13 1 7 1 15 12 14 4 8 8 2 2 15 14 13 2 11 8 13 6 4 9 2 1 11 1 7 3 10 10 15 6 6 12 12 12 5 11 9 11 7 3 14 5 9 9 3 5 0 7 3 1
0 10 0 5 8 0 6 13 15 1 3 0 13 8 14 4 14 13 8 7 7 11 10 1 6 11 15 10 2 3 4 8 4 3 15 13 14 1 4 2 9 7 12 5 0 2 13 1 8 11 6 12 10 6 7 12 1
2 0 6 9 9 5 10 11 3 0 5 2 5 15 14 9 10 0 13 13 7 9 14 0 6 1 10 4 9 9 13 0 6 3 3 8 4 15 5 6 15 6 9 3 10 0 8 7 1 13 2 11 8 12 7 5 1 4 15
2 14 12 14 3 11 4 12 5 11 2 8 15 10 11 5 14 1 7 2 12 7 13 13 10 8 14 3 11 6 3 15 9 5 0 0 6 0 6 6 12 15 9 10 0 11 10 1 7 3 13 13 8 1 2
4 15 7 8 5 2 1 9 4 3 12 14 5 11 11 12 1 5 10 4 15 14 2 12 7 8 9 4 2 14 2 12 14 4 11 4 1 2 2 11 8 1 12 11 12 7 7 10 4 10 7 11 6 13 13 1
14 7 1 8 2 13 8 5 5 15 0 3 15 15 9 6 15 12 10 5 0 9 13 0 3 6 9 14 9 8 3 10 4 0 6 14 5 3 12 1 10 9 15 10 15 4 14 4 3 15 2 5 2 12 9 2 7
2 12 6 8 9 8 9 5 12 5 3 15 10 0 13 6 7 1 3 4 13 0 11 14 4 14 10 1 7 14 7 0 1 11 5 11 3 13 6 0 11 8 6 8 13 4 11 13 1 0 2 14 11 4 6 11 1
1 7 13 13 8 15 0 4 12 9 8 13 1 3 1 4 7 10 14 10 7 3 12 14 10 3 9 7 5 15 9 5 6 12 8 0 15 5 10 2 0 15 6 1 8 5 14 2 9 6 2 3 12 13 2 1 7 1
5 8 4 13 11 2 1 4 8 1 14 7 6 15 10 9 3 11 1 7 12 4 10 14 4 2 8 13 10 9 12 0 5 3 14 6 6 15 12 10 11 13 9 0 5 0 0 15 14 12 7 9 3 3 5 5 2
8 6 11
 Enter plain text of atleast 16 characters:ABCDEF1234ABCDEF

 Enter key of same size as plain text:123456ABCD123456
Encryption
After inital permutation C618D6E7E7B5E7AD
Round No      left      right      round key
-------------------------------------
Round  1   E7B5E7AD   37194EAF   7201C69E3355
Round  2   37194EAF   D1ABCAEB   123E31ED00E7
Round  3   D1ABCAEB   3299955E   CD3C4046EACF
Round  4   3299955E   A3487A26   42E6CC3695DD
Round  5   A3487A26   60DB31DA   58D5028B95E3
Round  6   60DB31DA   F5138C52   60896B4EEF21
Round  7   F5138C52   51A49B8D   A1E0077A4D5C
Round  8   51A49B8D   8A4380A5   210F92C9D19A
Round  9   8A4380A5   8DDD7AAD   6252488DAFF8
Round  10   8DDD7AAD   21B9DF57   08D96439DE51
Round  11   21B9DF57   8B4CC35F   80695B5BC436
Round  12   8B4CC35F   E9B48C60   2567218D6D8C
Round  13   E9B48C60   D952DE09   C31D81A872D5
Round  14   D952DE09   17FA8CEB   59A2D1F3C2A7
Round  15   17FA8CEB   D23EC140   15D48A960F8B
Round  16   FED5D067   D23EC140   842B88353596
Cipher Text :  19E17160F461DFDC
Encryption time:  0.6420354843139648
```

Decryption for case 1

Table 2. Decryption for case 1



```
Decryption
After inital permutation FED5D067D23EC140
Round No      left      right      round key
-------------------------------------
Round  1   D23EC140   17FA8CEB   842B88353596
Round  2   17FA8CEB   D952DE09   15D48A960F8B
Round  3   D952DE09   E9B48C60   59A2D1F3C2A7
Round  4   E9B48C60   8B4CC35F   C31D81A872D5
Round  5   8B4CC35F   21B9DF57   2567218D6D8C
Round  6   21B9DF57   8DDD7AAD   80695B5BC436
Round  7   8DDD7AAD   8A4380A5   08D96439DE51
Round  8   8A4380A5   51A49B8D   6252488DAFF8
Round  9   51A49B8D   F5138C52   210F92C9D19A
Round  10   F5138C52   60DB31DA   A1E0077A4D5C
Round  11   60DB31DA   A3487A26   60896B4EEF21
Round  12   A3487A26   3299955E   58D5028B95E3
Round  13   3299955E   D1ABCAEB   42E6CC3695DD
Round  14   D1ABCAEB   37194EAF   CD3C4046EACF
Round  15   37194EAF   E7B5E7AD   123E31ED00E7
Round  16   C618D6E7   E7B5E7AD   7201C69E3355
Plain Text :  ABCDEF1234ABCDEF
Decryption time  0.8394386768341064
```


Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Encryption for case2

Table 3: Encryption for case2

```
 Enter plain text of atleast 16 characters:ABCDEF1234ABCDED

 Enter key of same size as plain text:123456ABCD123456
Encryption
After inital permutation C618D6E7E7B5E72D
Round No      left      right      round key
--------------------------------------------
Round  1   E7B5E72D   37296EAE   7201C69E3355
Round  2   37296EAE   50E85AC9   123E31ED00E7
Round  3   50E85AC9   A99142A9   CD3C4046EACF
Round  4   A99142A9   83654694   42E6CC3695DD
Round  5   83654694   E6924E02   58D5028B95E3
Round  6   E6924E02   05A5C6A3   60896B4EEF21
Round  7   05A5C6A3   578228C6   A1E0077A4D5C
Round  8   578228C6   AA8E168B   210F92C9D19A
Round  9   AA8E168B   7AB24539   6252488DAFF8
Round  10   7AB24539   1CE74F85   08D96439DE51
Round  11   1CE74F85   5C5AAE9F   80695B5BC436
Round  12   5C5AAE9F   2EF00EEA   2567218D6D8C
Round  13   2EF00EEA   DF26C105   C31D81A872D5
Round  14   DF26C105   40D35AD4   59A2D1F3C2A7
Round  15   40D35AD4   4DE33D9A   15D48A960F8B
Round  16   2F24D387   4DE33D9A   842B88353596
Cipher Text :  ED67D9CA0E78A427
Encryption time:  0.9885833263397217
```

Decryption for case2

Table 4: Decryption for case 2

```
Decryption
After inital permutation 2F24D3874DE33D9A
Round No      left      right      round key
--------------------------------------------
Round  1   4DE33D9A   40D35AD4   842B88353596
Round  2   40D35AD4   DF26C105   15D48A960F8B
Round  3   DF26C105   2EF00EEA   59A2D1F3C2A7
Round  4   2EF00EEA   5C5AAE9F   C31D81A872D5
Round  5   5C5AAE9F   1CE74F85   2567218D6D8C
Round  6   1CE74F85   7AB24539   80695B5BC436
Round  7   7AB24539   AA8E168B   08D96439DE51
Round  8   AA8E168B   578228C6   6252488DAFF8
Round  9   578228C6   05A5C6A3   210F92C9D19A
Round  10   05A5C6A3   E6924E02   A1E0077A4D5C
Round  11   E6924E02   83654694   60896B4EEF21
Round  12   83654694   A99142A9   58D5028B95E3
Round  13   A99142A9   50E85AC9   42E6CC3695DD
Round  14   50E85AC9   37296EAE   CD3C4046EACF
Round  15   37296EAE   E7B5E72D   123E31ED00E7
Round  16   C618D6E7   E7B5E72D   7201C69E3355
Plain Text :  ABCDEF1234ABCDED
Decryption time  0.9185218811035156
```

Avalanche Effect generated for two cases:

Table 5: Avalanche Effect

```
 Avalanche Effect can be observed as:
CASE - 1
 Plain text: ABCDEF1234ABCDEF
 Cipher text: 19E17160F461DFDC
CASE - 2
 Plain text: ABCDEF1234ABCDED
 Cipher text: ED67D9CA0E78A427
>>>
```

The results demonstrate the performance of the zigzag scanning approach, which enhances the encryption time of the input file with greater completeness and a more pronounced avalanche effect.

VI. CONCLUSION

Nowadays, all data transfers, business transactions, and various kinds of applications are carried out through the internet. Providing security and maintaining confidentiality will play a crucial role in ensuring the success of this initiative. Therefore, in this paper, the improved DES algorithm is employed to provide enhanced protection compared to the traditional DES. The improved DES is designed with modifications to the S-box and also utilises a zig-zag scan method, making it stronger than the DES through the use of columnar transposition.

DECLARATION

Funding/Grants/ Financial Support	No, I did not receive.
Conflicts of Interest/Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participation	No, the article does not require ethical approval or consent to participate, as it presents evidence that is not subject to interpretation.
Availability of Data and Material/Data Access Statement	Not relevant.
Authors Contribution	S. Hemasri; methodology, S. Hemasri, S.Kiran, and Rajeshkanna Coding, A.Ranichitra; validation, S. Kiran, A.Rajeshkanna, and A. Ranichitra; investigation, S. Kiran and A.Rajeshkanna; resources, S.Hemasri; writing—original draft preparation, S.Hemasri, and S. Kiran; writing—review and editing, S.Hemasri, S. Kiran and A.Ranichitra. All authors have read and agreed to the published version of the manuscript.

REFERENCES

1. Sombir Singh, Sunil K. Maakar, Dr. Sudesh Kumar, “Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques”, Vol, Issue 6, June 2013, ISSN: 2277 128X.
2. Kaur, N., & Sodhi, S. (2016, October). The Data Encryption Standard (DES) algorithm is used for secure data transmission and encryption. In International Conference on Advances in Emerging Technology (ICAET) (pp. 31-37).
3. Na Su Yi Zhang, Mingue Lithe,” Research on Data Encryption Standard Based on AES Algorithm in Internet of Things Environment”,2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference [ITNEC]2019.
4. Wang Sheng Zhou Jian, “Research on Data Encryption of Network Communication Based on Big Data “,2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering.
5. Khalid Ali Hussein, Sadiq A.M. Mehdi, Salam Ayad Hussein, “Image encryption based on parallel algorithm via zigzag manner with a new chaotic system”, Journal of Southwest Jiantong University, vol.54, No.4, Aug 2019, ISSN no.0258-2724. [CrossRef]
6. Pratibha Chaudary, Ritu Gupta, Abhilash Singh, Pramathesh Majumder, Ayushi Pandey,” Joint Image Compression Using a novel column-wise scanning and optimisation algorithm”, International Conference on Computational Intelligence and Data Science (2019), Procedia computer science 169(2020)244-253. [CrossRef]
7. Li, S., Zhao, L., & Yang, N. (2021). Medical image encryption based on 2d zigzag confusion and dynamic diffusion. Security and Communication Networks, 2021. [CrossRef]
8. Elkandoz, M. T., Alexan, W., & Hussein, H. H. (2019, April). Double-layer image security scheme with aggregated mathematical sequences. In 2019 International Conference on Advanced Communication Technologies and Networking (CommNet) (pp. 1-7). IEEE. [CrossRef]
9. Ahmed A. Abd El-Latif, Bassem Abd-El-Atty, Wojcicch Mazurczak, “Data Encryption Based on Quantum Walks for 5G Internet of Things Scenario”, IEEE Transactions on Network and Service Management, Vol . 17, No. 1, mar 2020. [CrossRef]
10. Shanshan Li, Li Zhao and Na Yang, “Medical Image Encryption Based on 2D ZigZag Confusion and Dynamic Diffusion”, Hindwai Security and Communication Networks, Vol . 20, article ID:6624809.
11. Harshali D. Zodpe, Prakash Wani, Rakesh R. Mehta: Design and Implementation of an algorithm for DES Cryptanalysis, Hybrid Intelligent Systems, 2012 12th International Conference.
12. Mohit Agarwal,” Ensuring Data Security in Databases using Format Preserving Encryption”, 978-1-5386-1719-9/18$31.00 2018 IEEE.

AUTHORS PROFILE

Singareddy Hemasri received the B.Tech. and M.Tech degrees in computer science and engineering from JNTUA Anantapur, India, in 2011 and 2013, respectively. She is currently pursuing a Ph.D. degree in the Department of Computer Science at Madurai Kamraj University, Madurai. Her current research interests include wireless sensor networks and Cryptography.

Dr. S. Kiran is an Associate Professor in the Department of Computer Science and Engineering at Yogivemana University, Proddatur. He acquired an M.Tech Degree from Nagarjuna University, Guntur. He completed his Ph.D. in Computer Science from S.K. University. He has been continuously imparting his knowledge to several students in research activities. He published many articles in National and International journals. His research areas include image processing, Cryptography and Network Security, Software Engineering, and Data mining and data warehousing.

Dr. A. Ranichitra received the MCA degree from P.S.G.R. Krishnammai College for Women, Coimbatore, in 1999, the M.Phil. degree from Mother Teresa Women’s University, Kadaikanal, India, in 2004, and the Ph.D. degree from Manonmaniam Sundaranar University, Tirunelveli, India, in 2016. She is currently an Assistant Professor in the Department of Computer Science at S.Ramasamy Naidu Memorial College, Sattur. She has contributed several publications to reputed international journals and conferences. Her research interests include VANET, Machine Learning, Image Processing, and Data Mining.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Dr. A. Rajesh Kanna received the M.Sc. degree from Alagappa University, Karaikudi, in 1998, and the M.Phil. Manonmaniam Sundaranar University, Tirunelveli, India, in 2004, and the Ph.D. degree from the S.Ramasamy Naidu Memorial College, Sattur, Madurai, India, in 2021. He is currently an Assistant Professor in the Department of Computer Science at S.Ramasamy Naidu Memorial College, Sattur. He has contributed to several publications in reputable international journals and conferences. His research interests include data mining and computer networks.