Alqalam Journal of Medical and Applied Sciences. 2025;8(3):1864-1871
https://doi.org/10.54361/ajmas.258385

Original article

SOA Algorithm for Secure Data Encryption and Decryption: A New Random Key-Based Encryption Method

Samyrah Abu Irzayzah[1]*, Osamah Aljalali[2], Aml Altirban[2], Rem Arebi[2]

[1]*Department of Mathematics, Faculty of Arts and Sciences, University of Elmergib, Libya*
[2]*Department of Mathematics, Faculty of Science, University of Tripoli, Libya*
Corresponding Email. *smabuirzayzah@elmergib.edu.ly*

Abstract
In this paper, we present the SOA algorithm, a novel approach to secure data encryption and decryption. The SOA algorithm is based on matrix-based operations and uses a unique method to divide text into blocks represented by 2×1 matrices. Each block is encrypted using a randomly generated block key and a corresponding key matrix, ensuring that each block has a unique encryption. The encryption process combines block keys, key matrices, and fixed matrices to convert plaintext blocks into encrypted data. The decryption process uses the same block keys and includes a special matrix generated from the block key, fixed matrix, and identity matrix, allowing for accurate recovery of the original text. The SOA algorithm is characterized by its use of random keys for each block, with the addition of fixed matrices, ensuring a high level of security and resistance to attacks. This approach, based on random keys and complexity of key computations, provides a flexible, efficient, and mathematically powerful framework for modern data encryption and decryption, making it a promising way to secure sensitive information in various applications.
Keywords. SOA Algorithm, Random Keys, Fixed Matrices, Encryption, Decryption.

Introduction

In the modern era of technology, where data is constantly being transmitted and stored, ensuring the security of information has become one of the most critical challenges. Encryption is one of the most powerful tools we have to keep sensitive data safe. Most encryption methods rely on mathematical techniques to make data unreadable to anyone without the correct key. There are many research papers in cryptography, for example [1-7]. The data or information to be encrypted is called the plaintext. The plaintext data is then encrypted using various encryption techniques, mathematical calculations, and an encryption key, and decryption is the process of repeating the encryption so that previously encrypted information can be viewed or accessed. This involves converting unreadable data (ciphertext) into readable text (plaintext). So, while encryption is the process of making data unreadable, decryption is the process of converting encrypted information into its original and understandable form.

The method of encrypting and decrypting information depends on a specific type of encryption key. There are several encryption and decryption algorithms used for security and privacy protection. It is among the most common algorithms: AES: The AES algorithm is one of the best algorithms used in data encryption, and it is used in many applications such as integrated encryption systems, email, and online data storage services [8,9]. RSA: It is one of the most prominent algorithms used in general encryption, and is widely used to protect electronic communications [10]. DES: The DES algorithm is a traditional encryption algorithm known for its security, but it is considered simple compared to the security standards used nowadays [11]. Blowfish: A good encryption algorithm that can be used easily, and has a security level similar to the popular AES encryption algorithm [12].

In this paper, we present a novel approach to text encryption and decryption algorithms (SOA algorithm). The basis of our algorithm is to divide the text into small blocks, specifically 2×1 matrices. Each block is treated as a separate unit of encryption, allowing us to random key for every block. To further enhance security, we also create a key matrix for each block, which depends on the length of the block and the block number. In addition to these block-specific keys and matrices, two fixed square matrices are used throughout the encryption process, adding an extra layer of complexity and robustness to the system.

The encryption process involves transforming each using its unique block key, the corresponding key matrix, and the fixed square matrices. This results in encrypted blocks that are highly secure and difficult to decipher without the correct keys. By using a different key for each block, our method ensures that even if a single block is compromised, the security of the remaining blocks is not affected.

Decryption, the reverse of encryption, is an equally important aspect of any cryptographic system. In our algorithm, the decryption process uses the same block key generated during encryption. To retrieve the plaintext, we employ a specially constructed matrix formed by multiplying the key matrix by a fixed square matrix and adding it to the identity matrix. This ensures an accurate and efficient recovery of the plaintext from the encrypted blocks.

Our approach combines the use of randomness, block-based encryption, and matrix operations to provide a secure and flexible encryption method. By encrypting each block individually and introducing randomness into the key generation process, we achieve a high degree of security. The use of mathematical operations

Received*: 23-06-2025 -* ***Accepted****: 21-07-2025 -* ***Published****: 28-07-2025*

on matrices provides a strong framework for encryption and decryption while keeping the algorithm conceptually straightforward. This research aims to demonstrate the effectiveness of matrix-based cryptography and its potential for securing data in various applications. Our algorithm is particularly useful for scenarios where customized and adaptable encryption methods are required. It offers a novel perspective on designing an encryption system, paving the way for further exploration and innovation in the field of cryptography.

The proposed encryption algorithm

In this paper, we present a new encryption and decryption algorithm. We put the message we want to encrypt in a matrix E of size $2 \times m$ adding $0 = n + 26$ for the space between two words and the end of the message, we divide the message matrix E of size $2 \times m$ into block matrices named $E_j, (j = 1, 2, \dots, \mathrm{m})$ of size 2×1. The main idea of the method is the encryption of each message matrix with different keys. Now, we will define choosing n.The number of block matrices $E_j, (j = 1, 2, \dots, \mathrm{m})$ is denoted by m. According to mWe choose the number n as follows [13],

$$n = \begin{cases} m & , \quad m \leq 3 \\ \left[\left|\frac{m}{2}\right|\right] & , \quad m > 3 \end{cases}.$$

Now, we explain the encryption method. Suppose that the matrices E_j, K_j, C_j , A, B , S, I, $(j = 1, 2, \dots, m)$ are of the forms:

$$E_j = \begin{pmatrix} e_1^j \\ e_2^j \end{pmatrix}, \quad K_j = \begin{pmatrix} g_1^j \\ g_2^j \end{pmatrix}, \quad A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}, \quad C_j = \begin{pmatrix} c_1^j \\ c_2^j \end{pmatrix}$$

$$S = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (j = 1, 2, \dots, m).$$

Now, we define the alphabet table according to mod 29 (This table can be expanded to the used characters in the message text).

Table 1. Character Table

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
n	$n+1$	$n+2$	$n+3$	$n+4$	$n+5$	$n+6$	$n+7$	$n+8$	$n+9$
K	L	M	N	O	P	Q	R	S	T
$n+10$	$n+11$	$n+12$	$n+13$	$n+14$	$n+15$	$n+16$	$n+17$	$n+18$	$n+19$
U	V	W	X	Y	Z	0	,	!	
$n+20$	$n+21$	$n+22$	$n+23$	$n+24$	$n+25$	$n+26$	$n+27$	$n+28$	

Now, we explain a new encryption and decryption algorithm.

Encryption Algorithm.

Step 1. Divided message matrix E into blocks $E_j = \begin{pmatrix} e_1^j \\ e_2^j \end{pmatrix}, j = 1, 2, \dots, m.$

Step 2. Choose n.

Step 3. Determine the elements $e_1^j, e_2^j,\ j = 1, 2, \dots, m.$

Step 4. Determine the encryption keys $x_j,\ j = 1, 2, \dots, m.$

Step 5. Compute $K_j = \begin{pmatrix} k_1^j \\ k_2^j \end{pmatrix} = \begin{pmatrix} e_1^j \\ 2e_1^j + e_2^j \end{pmatrix}, j = 1, 2, \dots, m.$

Step 6. Compute the cipher text,

$$C_j = \left(-x_j A \pm B\right) K_j,$$

where

$$A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}, \quad C_j = \begin{pmatrix} c_1^j \\ c_2^j \end{pmatrix}, \quad j = 1, 2, \dots, m.$$

Step 7. Construct the matrix $C = \begin{pmatrix} c_1^j \\ c_2^j \end{pmatrix}_{j \in \{1,2,\dots,m\}}$.

Step 8. End of algorithm.

Decryption Algorithm.

Received*: 23-06-2025 -* ***Accepted****: 21-07-2025 -* ***Published****: 28-07-2025*

https://doi.org/10.54361/ajmas.258385

Step 1. Divided the cipher message matrix C into blocks $\begin{pmatrix} c_1^j \\ c_2^j \end{pmatrix}, j = 1, 2, \dots, m.$

Step 2. Compute the decryption text,

$$E_j = (-x_j S \pm I) C_j,$$

where

$$E_j = \begin{pmatrix} u_1^j \\ v_2^j \end{pmatrix}, \qquad S = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}, \qquad C_j = \begin{pmatrix} c_1^j \\ c_2^j \end{pmatrix}, \qquad j = 1, 2, \dots, m.$$

Step 3. Construct the matrix $E = \begin{pmatrix} e_1^j \\ e_2^j \end{pmatrix}_{j \in \{1,2,\dots,m\}}$.

Step 4. End of algorithm.

Example of the Encryption and Decryption Process

To help explain how our algorithm works, we will show step-by-step examples of the encryption and decryption processes.

Example 3.1. encrypted the message text:
"I REALLY CANNOT BELIEVE WE DID THAT!"
the messages matrix E is:

$$E = \begin{pmatrix} I & R & A & L & \gamma & A & N & T & B & L & E & E & W & \gamma & I & \gamma & H & T \\ \gamma & E & L & Y & C & N & O & \gamma & E & I & V & \gamma & E & D & D & T & A & ! \end{pmatrix}$$

Encryption Algorithm.

Step 1. To encrypt the message text, we divide the message matrix into blocks

$$E_j = \begin{pmatrix} e_1^j \\ e_2^j \end{pmatrix}, j = 1, 2, \dots, 18.$$

Hence,

$$E_1 = \begin{pmatrix} I \\ \gamma \end{pmatrix}, \quad E_2 = \begin{pmatrix} R \\ E \end{pmatrix}, \quad E_3 = \begin{pmatrix} A \\ L \end{pmatrix},$$
$$E_4 = \begin{pmatrix} L \\ Y \end{pmatrix}, \quad E_5 = \begin{pmatrix} \gamma \\ C \end{pmatrix}, \quad E_6 = \begin{pmatrix} A \\ N \end{pmatrix},$$
$$E_7 = \begin{pmatrix} N \\ O \end{pmatrix}, \quad E_8 = \begin{pmatrix} T \\ \gamma \end{pmatrix}, \quad E_9 = \begin{pmatrix} B \\ E \end{pmatrix},$$
$$E_{10} = \begin{pmatrix} L \\ I \end{pmatrix}, \quad E_{11} = \begin{pmatrix} E \\ V \end{pmatrix}, \quad E_{12} = \begin{pmatrix} E \\ \gamma \end{pmatrix},$$
$$E_{13} = \begin{pmatrix} W \\ E \end{pmatrix}, \quad E_{14} = \begin{pmatrix} \gamma \\ D \end{pmatrix}, \quad E_{15} = \begin{pmatrix} I \\ D \end{pmatrix},$$
$$E_{16} = \begin{pmatrix} \gamma \\ T \end{pmatrix}, \quad E_{17} = \begin{pmatrix} H \\ A \end{pmatrix}, \quad E_{18} = \begin{pmatrix} T \\ ! \end{pmatrix}.$$

Step 2. To choose n, we compute a, Since the number of blocks E_j, $j = 1, 2, \dots, 18$ is $18 > 3$, so we choose $n = 9$, thus the "character table" for the message is as follows:

Table 2. Shift Cipher Encoding Table

I	**γ**	**R**	**E**	**A**	**L**	**L**	**Y**	**γ**
17	6	26	13	9	20	20	4	6
C	A	N	N	O	T	γ	B	E
11	9	22	22	23	28	6	10	13
L	I	E	V	E	γ	W	E	γ
20	17	13	1	13	6	2	13	6
D	I	D	γ	T	H	A	T	!
12	17	12	6	28	16	9	28	7

Step 3. The elements of the blocks $E_j, j = 1, 2, \dots, 18$ as follows

Table 3. Block Matrix Elements Table

e_1^1	**17**	e_1^{10}	**20**	e_2^1	**6**	e_2^{10}	**17**
e_1^2	26	e_1^{11}	13	e_2^2	13	e_2^{11}	1
e_1^3	9	e_1^{12}	13	e_2^3	20	e_2^{12}	6
e_1^4	20	e_1^{13}	2	e_2^4	4	e_2^{13}	13

Received*: 23-06-2025 -* ***Accepted****: 21-07-2025 -* ***Published****: 28-07-2025*

https://doi.org/10.54361/ajmas.258385

e_1^5	6	e_1^{14}	6	e_2^5	11	e_2^{14}	12
e_1^6	9	e_1^{15}	17	e_2^6	22	e_2^{15}	12
e_1^7	22	e_1^{16}	6	e_2^7	23	e_2^{16}	28
e_1^8	28	e_1^{17}	16	e_2^8	6	e_2^{17}	9
e_1^9	10	e_1^{18}	28	e_1^9	13	e_2^{18}	7

Step 4. We determine the encryption keys $x_j,\ j = 1, 2, \dots, 18$.

Table 4. Encryption Keys Table

j	x_j	j	x_j
1	3	10	-2
2	-1	11	1951
3	6	12	2023
4	10	13	-4
5	2	14	8
6	-13	15	12
7	40	16	5
8	2020	17	-6
9	-5	18	33

Step 5. Compute $K_j = \begin{pmatrix} k_1^j \\ k_2^j \end{pmatrix} = \begin{pmatrix} e_1^j \\ 2e_1^j + e_2^j \end{pmatrix}, j = 1, 2, \dots, 18.$

Table 5. Secret Keys Table

k_1^1	**17**	k_1^{10}	**20**	k_2^1	**40**	k_2^{10}	**57**
k_1^2	26	k_1^{11}	13	k_2^2	65	k_2^{11}	27
k_1^3	9	k_1^{12}	13	k_2^3	38	k_2^{12}	32
k_1^4	20	k_1^{13}	2	k_2^4	44	k_2^{13}	17
k_1^5	6	k_1^{14}	6	k_2^5	23	k_2^{14}	24
k_1^6	9	k_1^{15}	17	k_2^6	40	k_2^{15}	46
k_1^7	22	k_1^{16}	6	k_2^7	67	k_2^{16}	40
k_1^8	28	k_1^{17}	16	k_2^8	62	k_2^{17}	41
k_1^9	10	k_1^{18}	28	k_2^9	33	k_2^{18}	63

Step 6. Compute the cipher text,

$$C_j = \left(-x_j A \pm B\right)K_j,$$

where

$$A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}, \quad C_j = \begin{pmatrix} c_1^j \\ c_2^j \end{pmatrix}, \quad j = 1, 2, \dots, 18.$$

$$C_1 = \left(\begin{pmatrix} -3 & 3 \\ 3 & -3 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 17 \\ 40 \end{pmatrix} = \begin{pmatrix} 52 \\ -75 \end{pmatrix},$$

$$C_2 = \left(\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 26 \\ 65 \end{pmatrix} = \begin{pmatrix} -65 \\ 26 \end{pmatrix},$$

$$C_3 = \left(\begin{pmatrix} -6 & 6 \\ 6 & -6 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 9 \\ 38 \end{pmatrix} = \begin{pmatrix} 165 \\ -194 \end{pmatrix},$$

$$C_4 = \left(\begin{pmatrix} -10 & 10 \\ 10 & -10 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 20 \\ 44 \end{pmatrix} = \begin{pmatrix} 220 \\ -244 \end{pmatrix},$$

$$C_5 = \left(\begin{pmatrix} -2 & 2 \\ 2 & -2 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 6 \\ 23 \end{pmatrix} = \begin{pmatrix} 28 \\ -45 \end{pmatrix},$$

$$C_6 = \left(\begin{pmatrix} 13 & -13 \\ -13 & 13 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 9 \\ 40 \end{pmatrix} = \begin{pmatrix} -412 \\ 381 \end{pmatrix},$$

$$C_7 = \left(\begin{pmatrix} -40 & 40 \\ 40 & -40 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 22 \\ 67 \end{pmatrix} = \begin{pmatrix} 1778 \\ -1823 \end{pmatrix},$$

$$C_8 = \left(\begin{pmatrix} -2020 & 2020 \\ 2020 & -2020 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 28 \\ 62 \end{pmatrix} = \begin{pmatrix} 68652 \\ -68686 \end{pmatrix},$$

Received*: 23-06-2025 -* ***Accepted****: 21-07-2025 -* ***Published****: 28-07-2025*

https://doi.org/10.54361/ajmas.258385

$$C_9 = \left(\begin{pmatrix} 5 & -5 \\ -5 & 5 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 10 \\ 33 \end{pmatrix} = \begin{pmatrix} -125 \\ 102 \end{pmatrix},$$
$$C_{10} = \left(\begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 20 \\ 57 \end{pmatrix} = \begin{pmatrix} -94 \\ 57 \end{pmatrix},$$
$$C_{11} = \left(\begin{pmatrix} -1951 & 1951 \\ 1951 & -1951 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 13 \\ 27 \end{pmatrix} = \begin{pmatrix} 27301 \\ -27315 \end{pmatrix},$$
$$C_{12} = \left(\begin{pmatrix} -2023 & 2023 \\ 2023 & -2023 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 13 \\ 32 \end{pmatrix} = \begin{pmatrix} 38424 \\ -38443 \end{pmatrix},$$
$$C_{13} = \left(\begin{pmatrix} 4 & -4 \\ -4 & 4 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 2 \\ 17 \end{pmatrix} = \begin{pmatrix} -62 \\ 47 \end{pmatrix},$$
$$C_{14} = \left(\begin{pmatrix} -8 & 8 \\ 8 & -8 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 6 \\ 24 \end{pmatrix} = \begin{pmatrix} 138 \\ -156 \end{pmatrix},$$
$$C_{15} = \left(\begin{pmatrix} -12 & 12 \\ 12 & -12 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 17 \\ 46 \end{pmatrix} = \begin{pmatrix} 331 \\ -360 \end{pmatrix},$$
$$C_{16} = \left(\begin{pmatrix} -5 & 5 \\ 5 & -5 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 6 \\ 40 \end{pmatrix} = \begin{pmatrix} 164 \\ -198 \end{pmatrix},$$
$$C_{17} = \left(\begin{pmatrix} 6 & -6 \\ -6 & 6 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 16 \\ 41 \end{pmatrix} = \begin{pmatrix} -166 \\ 141 \end{pmatrix},$$
$$C_{18} = \left(\begin{pmatrix} -33 & 33 \\ 33 & -33 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 28 \\ 63 \end{pmatrix} = \begin{pmatrix} 1127 \\ -1162 \end{pmatrix}.$$

Decryption Algorithm.

Step 1. Compute the decryption text,

$$E_j = (-x_j S \pm I)C_j,$$

where

$$E_j = \begin{pmatrix} u_1^j \\ v_2^j \end{pmatrix}, \qquad S = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}, \qquad C_j = \begin{pmatrix} c_1^j \\ c_2^j \end{pmatrix}, \qquad j = 1, 2, \ldots, 18.$$

$$E_1 = \left(\begin{pmatrix} -3 & -3 \\ 3 & 3 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 52 \\ -75 \end{pmatrix} = \begin{pmatrix} 17 \\ 6 \end{pmatrix},$$
$$E_2 = \left(\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} -65 \\ 26 \end{pmatrix} = \begin{pmatrix} 26 \\ 13 \end{pmatrix},$$
$$E_3 = \left(\begin{pmatrix} -6 & -6 \\ 6 & 6 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 165 \\ -194 \end{pmatrix} = \begin{pmatrix} 9 \\ 20 \end{pmatrix},$$
$$E_4 = \left(\begin{pmatrix} -10 & -10 \\ 10 & 10 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 220 \\ -224 \end{pmatrix} = \begin{pmatrix} 20 \\ 4 \end{pmatrix},$$
$$E_5 = \left(\begin{pmatrix} -2 & -2 \\ 2 & 2 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 28 \\ -45 \end{pmatrix} = \begin{pmatrix} 6 \\ 11 \end{pmatrix},$$
$$E_6 = \left(\begin{pmatrix} 13 & 13 \\ -13 & -13 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} -412 \\ 381 \end{pmatrix} = \begin{pmatrix} 9 \\ 22 \end{pmatrix},$$
$$E_7 = \left(\begin{pmatrix} -40 & -40 \\ 40 & 40 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 1778 \\ -1823 \end{pmatrix} = \begin{pmatrix} 22 \\ 23 \end{pmatrix},$$
$$E_8 = \left(\begin{pmatrix} -2020 & -2020 \\ 2020 & 2020 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 68652 \\ -68686 \end{pmatrix} = \begin{pmatrix} 28 \\ 6 \end{pmatrix},$$
$$E_9 = \left(\begin{pmatrix} 5 & 5 \\ -5 & -5 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} -125 \\ 102 \end{pmatrix} = \begin{pmatrix} 10 \\ 13 \end{pmatrix},$$
$$E_{10} = \left(\begin{pmatrix} 2 & 2 \\ -2 & -2 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} -94 \\ 57 \end{pmatrix} = \begin{pmatrix} 20 \\ 17 \end{pmatrix},$$
$$E_{11} = \left(\begin{pmatrix} -1951 & -1951 \\ 1951 & 1951 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 27301 \\ -27315 \end{pmatrix} = \begin{pmatrix} 13 \\ 1 \end{pmatrix},$$
$$E_{12} = \left(\begin{pmatrix} -2023 & -2023 \\ 2023 & 2023 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 38424 \\ -38443 \end{pmatrix} = \begin{pmatrix} 13 \\ 6 \end{pmatrix},$$
$$E_{13} = \left(\begin{pmatrix} 4 & 4 \\ -4 & -4 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} -62 \\ 47 \end{pmatrix} = \begin{pmatrix} 2 \\ 13 \end{pmatrix},$$

Received: *23-06-2025* - ***Accepted***: *21-07-2025* - ***Published***: *28-07-2025*

https://doi.org/10.54361/ajmas.258385

$$E_{14} = \left(\begin{pmatrix} -8 & -8 \\ 8 & 8 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 138 \\ -156 \end{pmatrix} = \begin{pmatrix} 6 \\ 12 \end{pmatrix},$$
$$E_{15} = \left(\begin{pmatrix} -12 & -12 \\ 12 & 12 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 331 \\ -360 \end{pmatrix} = \begin{pmatrix} 17 \\ 12 \end{pmatrix},$$
$$E_{16} = \left(\begin{pmatrix} -5 & -5 \\ 5 & 5 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 164 \\ -198 \end{pmatrix} = \begin{pmatrix} 6 \\ 28 \end{pmatrix},$$
$$E_{17} = \left(\begin{pmatrix} 6 & 6 \\ -6 & -6 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} -166 \\ 144 \end{pmatrix} = \begin{pmatrix} 16 \\ 9 \end{pmatrix},$$
$$E_{18} = \left(\begin{pmatrix} -33 & -33 \\ 33 & 33 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 1127 \\ -1162 \end{pmatrix} = \begin{pmatrix} 28 \\ 7 \end{pmatrix}.$$

Step 2. Construct the matrix $E = \begin{pmatrix} e_1^j \\ e_2^j \end{pmatrix}_{j\in\{1,2,\dots,18\}}$,

thus

$$E = \begin{pmatrix} I & R & A & L & \gamma & A & N & T & B & L & E & E & W & \gamma & I & \gamma & H & T \\ \gamma & E & L & Y & C & N & O & \gamma & E & I & V & \gamma & E & D & D & T & A & ! \end{pmatrix}$$

from table (2).

Example 3.2. encrypted the message text:
"CIPHER"
the messages matrix E is:

$$E = \begin{pmatrix} C & P & E \\ I & H & R \end{pmatrix}$$

Encryption Algorithm.
Step 1. To encrypt the message text, we divide the message matrix into blocks

$$E_j = \begin{pmatrix} e_1^j \\ e_2^j \end{pmatrix}, j = 1, 2, 3.$$

Hence,

$$E_1 = \begin{pmatrix} C \\ I \end{pmatrix}, \quad E_2 = \begin{pmatrix} P \\ H \end{pmatrix}, \quad E_3 = \begin{pmatrix} E \\ R \end{pmatrix},$$

Step 2. To choose n, we compute a, Since the number of blocks A_j, $j = 1, 2, 3$ is $3 \leq 3$, so we choose $n = 3$, thus, the "character table" for the message as follows:

Table 2.1. Shift Cipher Encoding Table

C	***I***	***P***
5	11	18
H	*E*	*R*
10	7	20

Step 3. The elements of the blocks $E_j, j = 1, 2, 3$ as follows:

Table 2.2. Block Matrix Elements Table

e_1^1	**5**
e_2^1	11
e_1^2	18
e_2^2	10
e_1^3	7
e_2^3	20

Step 4. We determine the encryption keys x_j, $j = 1, 2, 3$.

Table 2.3. Encryption Keys Table

j	x_j
1	5
2	3
3	−125

Step 5. Compute $K_j = \begin{pmatrix} k_1^j \\ k_2^j \end{pmatrix} = \begin{pmatrix} u_1^j \\ 2u_1^j + v_2^j \end{pmatrix}, j = 1, 2, 3.$

Received*: 23-06-2025 -* ***Accepted****: 21-07-2025 -* ***Published****: 28-07-2025*

Table 2.4. Secret Keys Table

k_1^1	5
k_2^1	21
k_1^2	18
k_2^2	46
k_1^3	7
k_2^3	34

Step 6. Compute the cipher text,

$$C_j = (-x_j A \pm B)K_j,$$

where

$$A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}, \quad C_j = \begin{pmatrix} c_1^j \\ c_2^j \end{pmatrix}, \quad j = 1, 2, 3.$$

$$C_1 = \left(\begin{pmatrix} -5 & 5 \\ 5 & -5 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 5 \\ 21 \end{pmatrix} = \begin{pmatrix} 85 \\ -69 \end{pmatrix},$$

$$C_2 = \left(\begin{pmatrix} -3 & 3 \\ 3 & -3 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 18 \\ 46 \end{pmatrix} = \begin{pmatrix} 102 \\ -74 \end{pmatrix},$$

$$C_3 = \left(\begin{pmatrix} 125 & -125 \\ -125 & 125 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\right)\begin{pmatrix} 7 \\ 34 \end{pmatrix} = \begin{pmatrix} 3395 \\ -3368 \end{pmatrix}.$$

Decryption Algorithm.

Step 1. Compute the decryption text,

$$E_j = (-x_j S \pm I)C_j,$$

where

$$E_j = \begin{pmatrix} e_1^j \\ e_2^j \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}, \quad C_j = \begin{pmatrix} c_1^j \\ c_2^j \end{pmatrix}, \quad j = 1, 2, 3.$$

$$E_1 = \left(\begin{pmatrix} -5 & -5 \\ 5 & 5 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 85 \\ -69 \end{pmatrix} = \begin{pmatrix} 5 \\ 11 \end{pmatrix},$$

$$E_2 = \left(\begin{pmatrix} -3 & -3 \\ 3 & 3 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 102 \\ -74 \end{pmatrix} = \begin{pmatrix} 18 \\ 10 \end{pmatrix},$$

$$E_3 = \left(\begin{pmatrix} 125 & 125 \\ -125 & -125 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 3395 \\ -3368 \end{pmatrix} = \begin{pmatrix} 7 \\ 20 \end{pmatrix}.$$

Step 2. Construct the matrix $E = \begin{pmatrix} e_1^j \\ e_2^j \end{pmatrix}_{j\in\{1,2,3\}}$

thus

$E = \begin{pmatrix} C & P & E \\ I & H & R \end{pmatrix}$.

from table (6).

Discussion

In this study, we proposed a new encryption and decryption algorithm based on matrices, which improves security by dividing the text into small blocks and generating random keys for each block. By working on 2×1 matrix blocks and giving each block its own unique key and key matrix, the method keeps each part of the message separate. This means that if one block is broken, the others remain safe, which is an important advantage over many traditional block ciphers.

Compared to earlier research in matrix-based encryption and block ciphers, our approach offers both innovation and practical benefits. While previous methods often use fixed keys or matrices for all blocks, our method adds more security by combining random block keys with fixed matrices. This layered design helps protect against common attacks like brute-force and statistical analysis.

The decryption uses the same keys and matrices, applying simple but reliable matrix operations to recover the original message correctly. This process keeps the algorithm efficient and trustworthy.

From a theoretical point of view, our work shows that combining randomness with matrix transformations can create flexible encryption systems. In practice, this method can be useful for applications that need adaptable security, such as Internet of Things (IoT) devices, personalized data protection, or lightweight

Received*: 23-06-2025 -* ***Accepted****: 21-07-2025 -* ***Published****: 28-07-2025*

encryption where resources are limited.
One important result is the flexibility of this matrix-based system. Since each block is handled almost independently, it is possible to use parallel processing to speed up encryption and decryption for large amounts of data. Also, this approach could be combined with machine learning techniques to generate better keys depending on the data.
For future work, it would be interesting to test larger matrix blocks, mix this method with other encryption systems like elliptic curve cryptography, or use machine learning to improve key randomness. Also, further security testing is needed to check how well the algorithm resists known attacks.
In summary, the proposed algorithm provides a promising and adaptable way to secure data. Its use of separate keys for each block and the matrix-based operations lays a good foundation for new developments in modern cryptography.

Conclusion

In this research, we introduced a new encryption and decryption algorithm (SOA algorithm) that enhances security by using a unique random key for each block of text and combining it with computational methods, key matrices from the blocks, and fixed square matrices. This approach ensures that each block is encrypted differently, making it harder for attackers to break the encryption. The results show that our algorithm is effective in securing text data while maintaining a structured process for encryption and decryption. This makes it a strong candidate for applications requiring high security and reliability. Future work can explore optimizing the algorithm for larger datasets and testing it against more advanced cryptographic attacks to further validate its strength.

Conflict of interest. Nil

References

1. Hellman M. New directions in cryptography. IEEE Trans Inf Theory. 1976;22(6):644–54.
2. Kretschmer W, Qian L, Sinha M, Tal A. Quantum cryptography in algorithmica. In: Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC 2023). New York (NY): Association for Computing Machinery; 2023. p.1589–602. doi:10.1145/3564246.3585225.
3. Ibrahim DR, Teh JS, Abdullah R. An overview of visual cryptography techniques. Multimed Tools Appl. 2021;80:31927–52. doi:10.1007/s11042-021-11229-9.
4. Diffie W, Hellman ME. New directions in cryptography. In: Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman. 1st ed. New York (NY): Association for Computing Machinery; 2022. p.365–90. doi:10.1145/3549993.3550007.
5. Silva C, Cunha VA, Barraca JP, et al. Analysis of the cryptographic algorithms in IoT communications. Inf Syst Front. 2024;26:1243–60. doi:10.1007/s10796-023-10383-9.
6. Rivest RL, Shamir A, Adleman LM. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978;21:120–6.
7. Singh G. A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. Int J Comput Appl. 2013;67(19).
8. Abdullah AM. Advanced encryption standard (AES) algorithm to encrypt and decrypt data. Cryptogr Netw Secur. 2017;16(1):11.
9. Sanchez-Avila C, Sanchez-Reillol R. The Rijndael block cipher (AES proposal): A comparison with DES. In: Proceedings of IEEE 35th Annual International Carnahan Conference on Security Technology. Piscataway (NJ): IEEE; 2001. p.229–34.
10. Zhou X, Tang X. Research and implementation of RSA algorithm for encryption and decryption. In: Proceedings of 2011 6th International Forum on Strategic Technology. Piscataway (NJ): IEEE; 2011. p.1118–21. doi:10.1109/IFOST.2011.6021216.
11. Han SJ, Oh HS, Park J. The improved data encryption standard (DES) algorithm. In: Proceedings of ISSSTA'95 International Symposium on Spread Spectrum Techniques and Applications. Vol. 3. Piscataway (NJ): IEEE; 1996. p.1310–4.
12. Schneier B. Description of a new variable-length key, 64-bit block cipher (Blowfish). In: International Workshop on Fast Software Encryption. Berlin: Springer; 1993. p.191–204.
13. Abo Irzayzah S, Al Bolati T. Coding and decoding algorithms using Jacobsthal and Jacobsthal-Lucas numbers. Alqala J. 2023;20:19–28.

Received*: 23-06-2025 -* ***Accepted****: 21-07-2025 -* ***Published****: 28-07-2025*