Alqalam Journal of Medical and Applied Sciences. 2026;9(3):628-640
https://doi.org/10.54361/ajmas.269314

Original article

MSA: A Multi-Key Block Encryption Algorithm with 3×3 Random Matrix Keys for Enhanced Data Security

Abdullah Abdulsamad, **Mohanad Seyam**, **Samyrah Abu Irzayzah***

Department of Mathematics, Faculty of Arts and Sciences, University of Elmergib, Libya
Corresponding Email. smabuirzayzah@elmergib.edu.ly

Abstract
This paper presents a novel block encryption and decryption algorithm, referred to as the MSA algorithm, which is fundamentally based on block-based cryptographic principles. In the proposed scheme, the plaintext is first arranged into a matrix of size $3 \times i$ and then partitioned into a set of 3×3 matrix blocks. The MSA algorithm performs block encryption by encrypting each block independently using two distinct encryption keys that are automatically generated for each block. A unique pair of keys is assigned to every block, where the keys are square matrices with the same dimensions as the blocks and are generated through an indirect mathematical mechanism. Each element within a block is encrypted individually through a combined and highly complex mathematical process that simultaneously relies on both keys. This block-wise, element-level encryption significantly increases the algorithm's complexity and enhances its resistance to cryptanalytic attacks. After encrypting all blocks, the ciphertext blocks are reassembled into an encrypted matrix that preserves the original dimensions of the plaintext matrix prior to block partitioning. During the decryption phase, the encrypted matrix is again divided into blocks. However, the decryption keys are mathematically generated from the original encryption keys and differ from them in both size and structure, as they are represented by 2×2 matrices. These keys are produced through a controlled, randomized permutation of the encryption key elements. Each encrypted element is then decrypted individually using the corresponding decryption keys, ensuring accurate recovery of the original plaintext. The proposed MSA algorithm adopts an advanced block-based encryption methodology aimed at enhancing information security, providing effective protection for sensitive data, and reducing the risk of unauthorized access, thereby offering improved security and efficiency compared to many conventional block encryption schemes.
Keywords. MSA Algorithm, Cipher Keys, Block Matrices, Encryption, Decryption.

Introduction

Modern encryption is a fundamental cornerstone of information security in the digital age. It is based on the development of advanced mathematical algorithms designed to protect data from unauthorized access. The importance of encryption has grown significantly with the increasing reliance on communication networks, smart systems, and digital platforms. Consequently, encryption plays a crucial role in strengthening trust in electronic systems and countering the rapidly growing cyber threats, making it an essential component in building secure and reliable information systems. Over the years, numerous encryption and decryption algorithms have been proposed in the field of cryptography. Many studies have focused on the use of matrices as powerful mathematical tools for constructing encryption and decryption keys. Several matrix-based encryption schemes have been introduced in the literature (see, for example, [1–4]. Kalika Prasad and Hrishesh Mahato investigated the use of generalized Fibonacci matrices as encryption keys within the Affine–Hill algorithm, where the plaintext is encrypted by multiplying it with a mathematically generated matrix, while the decryption process relies on the inverse of that matrix [5]. In addition, a number of studies have explored block encryption techniques, which are based on dividing the plaintext into blocks and processing each block independently [6,7,8]. Despite these efforts, there remains a need for block encryption schemes that employ more advanced mathematical structures to further enhance security and increase resistance to cryptanalytic attacks. Motivated by this observation, the method proposed in this paper is based on a block encryption mechanism, but implemented in a different manner that relies on higher mathematical complexity. The proposed approach aims to improve the level of security and significantly increase the difficulty of cryptanalysis. Moreover, building upon previous studies, this paper presents an extended development of the idea introduced by Samyrah M. Abu Irzayzah et al. [9], by proposing a more advanced conception of a matrix-based block encryption mechanism. Unlike the previous algorithm, which represents the plaintext within a $2 \times m$ matrix, the proposed MSA algorithm employs a different structural representation by embedding the plaintext into a $3 \times i$ matrix. This modification contributes to accelerating the encryption process and improving the overall computational efficiency. The proposed method further relies on generating two distinct encryption keys for each encryption block, where the text matrix is divided into blocks of size 3×3, and each block possesses independent keys. This approach significantly increases the level of randomness and mathematical complexity, thereby enhancing the security features of the system. Moreover, each element within a block is encrypted independently using a composite mathematical mechanism, which further limits the possibility of recovering the original plaintext without access to the correct keys. In the decryption phase, key matrices are mathematically derived from the original encryption

***Received**: 05-01-2026 - **Accepted**: 04-03-2026 - **Published**: 11-03-2026*

keys; however, this derivation is not performed in a direct manner. Instead, it is based on rearranging and shuffling the elements of the encryption keys according to a specific procedure, resulting in the generation of new key matrices that are structurally different from the original ones. This emphasis on key generation increases the mathematical complexity of the system and makes it difficult to establish a direct relationship between encryption and decryption keys, thereby enhancing the algorithm's resistance to cryptanalysis and potential attacks. Accordingly, the proposed MSA algorithm demonstrates greater robustness and accuracy in encryption compared to several existing algorithms, while providing a higher level of protection for sensitive data. Furthermore, the proposed system adopts a novel character encoding scheme that differs fundamentally from traditional encodings used in previous studies [10,11,12]. This encoding is based on a dynamic selection mechanism related to the number of blocks involved in the encryption process, assigning each character a variable numerical value computed within the internal structure of the algorithm itself. Such an approach increases randomness and strengthens the overall security of the encryption scheme. The construction and utilization of this encoding mechanism will be explained in detail in the subsequent sections.

The proposed encryption algorithm

In this paper, we describe novel algorithms for encryption and decryption. To encrypt the message, we put the message in a matrix T of size $3 \times i$ adding $\theta = \left[\left|\frac{j^2}{2}\right|\right] - 9$ for the space between two words and the end of the message, we divide the message matrix T of size $3 \times i$ into block matrices named $G_n, (n = 1, 2, \dots, p)$ of size 3×3. This method is the encryption of each message block matrix of size 3×3 with two different keys on each block from block matrices. For readability and simplicity, let the matrices $G_n, M_n, A_n, S_n, n = 1, 2, \dots, p$ are of the forms:

$$G_n = \begin{bmatrix} g_1^n & g_2^n & g_3^n \\ g_4^n & g_5^n & g_6^n \\ g_7^n & g_8^n & g_9^n \end{bmatrix}, M_n = \begin{bmatrix} m_1^n & m_2^n & m_3^n \\ m_4^n & m_5^n & m_6^n \\ m_7^n & m_8^n & m_9^n \end{bmatrix}, A_n = \begin{bmatrix} a_1^n & a_2^n & a_3^n \\ a_4^n & a_5^n & a_6^n \\ a_7^n & a_8^n & a_9^n \end{bmatrix}, S_n = \begin{bmatrix} s_1^n & s_2^n & s_3^n \\ s_4^n & s_5^n & s_6^n \\ s_7^n & s_8^n & s_9^n \end{bmatrix}, n = 1, 2, \dots, p,$$

such that the matrices M_n, A_n are different keys, and with the condition that the determinants of all matrices M_n are relatively prime to the chosen modulus, i.e. $(det(M_n), q) = 1$ [13].

Now, we define the following alphabet table according to $mod\ q$ such that $q = 35$ (This table can be expanded to the used characters in the message text).

Table 1. character table

A	$\left[\left\|\frac{j^2}{2}\right\|\right] - 35$	***H***	$\left[\left\|\frac{j^2}{2}\right\|\right] - 28$	***O***	$\left[\left\|\frac{j^2}{2}\right\|\right] - 21$	***V***	$\left[\left\|\frac{j^2}{2}\right\|\right] - 14$	)	$\left[\left\|\frac{j^2}{2}\right\|\right] - 7$
B	$\left[\left\|\frac{j^2}{2}\right\|\right] - 34$	*I*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 27$	*P*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 20$	*W*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 13$	:	$\left[\left\|\frac{j^2}{2}\right\|\right] - 6$
C	$\left[\left\|\frac{j^2}{2}\right\|\right] - 33$	*J*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 26$	*Q*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 19$	*X*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 12$	,	$\left[\left\|\frac{j^2}{2}\right\|\right] - 5$
D	$\left[\left\|\frac{j^2}{2}\right\|\right] - 32$	*K*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 25$	*R*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 18$	*Y*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 11$	–	$\left[\left\|\frac{j^2}{2}\right\|\right] - 4$
E	$\left[\left\|\frac{j^2}{2}\right\|\right] - 31$	*L*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 24$	*S*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 17$	*Z*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 10$	1	$\left[\left\|\frac{j^2}{2}\right\|\right] - 3$
F	$\left[\left\|\frac{j^2}{2}\right\|\right] - 30$	*M*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 23$	*T*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 16$	θ	$\left[\left\|\frac{j^2}{2}\right\|\right] - 9$	2	$\left[\left\|\frac{j^2}{2}\right\|\right] - 2$
G	$\left[\left\|\frac{j^2}{2}\right\|\right] - 29$	*N*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 22$	*U*	$\left[\left\|\frac{j^2}{2}\right\|\right] - 15$	(	$\left[\left\|\frac{j^2}{2}\right\|\right] - 8$	3	$\left[\left\|\frac{j^2}{2}\right\|\right] - 1$

Now, we explain a new encryption and decryption algorithm.

Encryption Algorithm.

1. Put the message in the message matrix T of size $3 \times i$, $n = 1, 2, \dots, p$.
2. Divided the matrix T into blocks $G_n, n = 1, 2, \dots, p$ as follows:

$$G_n = \begin{bmatrix} g_1^n & g_2^n & g_3^n \\ g_4^n & g_5^n & g_6^n \\ g_7^n & g_8^n & g_9^n \end{bmatrix}$$

3. Find k " the number of the block matrices $G_n, n = 1, 2, \dots, p$".
4. Find j as follows:

Received: 05-01-2026 - **Accepted**: 04-03-2026 - **Published**: 11-03-2026

$$j = \begin{cases} k, & k \le 3 \\ k-2, & k > 3 \end{cases}.$$

5. Compute the elements $g_h^n, (1 \le h \le 9)$ of the block matrices $G_n, n = 1, 2, \dots, p$.
6. Determine the encryption keys $M_n = \begin{bmatrix} m_1^n & m_2^n & m_3^n \\ m_4^n & m_5^n & m_6^n \\ m_7^n & m_8^n & m_9^n \end{bmatrix}, A_n = \begin{bmatrix} a_1^n & a_2^n & a_3^n \\ a_4^n & a_5^n & a_6^n \\ a_7^n & a_8^n & a_9^n \end{bmatrix}$,

$n = 1, 2, \dots, p$, such that $(det(M_n), q) = 1$.

7. Compute the elements $e_r^n, (1 \le r \le 9),\ n = 1, 2, \dots, p$,

$$a_r^n + g_h^n \to e_r^n(modq), \qquad r = h = t, t = 1,5\,,9, n = 1, 2, \dots, p$$
$$a_r^n + g_h^n \to e_r^n(modq), \qquad r = 2, h = 4,$$
$$a_r^n + g_h^n \to e_r^n(modq), \qquad r = 3, h = 7,$$
$$a_r^n + g_h^n \to e_r^n(modq), \qquad r = 4, h = 2,$$
$$a_r^n + g_h^n \to e_r^n(modq), \qquad r = 6, h = 8,$$
$$a_r^n + g_h^n \to e_r^n(modq), \qquad r = 7, h = 3,$$
$$a_r^n + g_h^n \to e_r^n(modq), \qquad r = 8, h = 6.$$

8. Compute the elements $s_r^n, (1 \le r \le 9)$, of the cipher text,

$$e_1^n m_1^n + e_4^n m_2^n + e_7^n m_3^n \to s_1^n(modq),$$
$$e_1^n m_4^n + e_4^n m_5^n + e_7^n m_6^n \to s_2^n(modq),$$
$$e_1^n m_7^n + e_4^n m_8^n + e_7^n m_9^n \to s_3^n(modq),$$
$$e_2^n m_1^n + e_5^n m_2^n + e_8^n m_3^n \to s_4^n(modq),$$
$$e_2^n m_4^n + e_5^n m_5^n + e_8^n m_6^n \to s_5^n(modq),$$
$$e_2^n m_7^n + e_5^n m_8^n + e_8^n m_9^n \to s_6^n(modq),$$
$$e_3^n m_1^n + e_6^n m_2^n + e_9^n m_3^n \to s_7^n(modq),$$
$$e_3^n m_4^n + e_6^n m_5^n + e_9^n m_6^n \to s_8^n(modq),$$
$$e_3^n m_7^n + e_6^n m_8^n + e_9^n m_9^n \to s_9^n(modq).$$

9. Construct the encrypted block matrices $S_n, n = 1, 2, \dots, p$ corresponding to the block matrices $G_n, n = 1, 2, \dots, p$ as follow,

$$S_n = \begin{bmatrix} s_1^n & s_2^n & s_3^n \\ s_4^n & s_5^n & s_6^n \\ s_7^n & s_8^n & s_9^n \end{bmatrix}.$$

10. Construct the matrix $S = \begin{bmatrix} s_1^1 & s_2^1 & s_3^1 & s_1^2 & s_2^2 & s_3^2 & \cdots & s_1^p & s_2^p & s_3^p \\ s_4^1 & s_5^1 & s_6^1 & s_4^2 & s_5^2 & s_6^2 & \cdots & s_4^p & s_5^p & s_6^p \\ s_7^1 & s_8^1 & s_9^1 & s_7^2 & s_8^2 & s_9^2 & \cdots & s_7^p & s_8^p & s_9^p \end{bmatrix}$.
11. End of algorithm.

Decryption Algorithm.

1. Divided the cipher message matrix S into blocks $S_n = \begin{bmatrix} s_1^n & s_2^n & s_3^n \\ s_4^n & s_5^n & s_6^n \\ s_7^n & s_8^n & s_9^n \end{bmatrix}, n = 1, 2, \dots, p$.
2. Compute the decryption keys,

$$B_1^n = \begin{bmatrix} -m_5^n & m_8^n \\ m_6^n & -m_9^n \end{bmatrix},\ B_2^n = \begin{bmatrix} -m_6^n & -m_9^n \\ -m_4^n & -m_7^n \end{bmatrix},\ B_3^n = \begin{bmatrix} -m_4^n & -m_7^n \\ -m_5^n & -m_8^n \end{bmatrix},$$

$$C_1^n = \begin{bmatrix} -m_2^n & -m_8^n \\ -m_3^n & -m_9^n \end{bmatrix},\ C_2^n = \begin{bmatrix} -m_3^n & m_9^n \\ m_1^n & -m_7^n \end{bmatrix},\ C_3^n = \begin{bmatrix} m_8^n & -m_2^n \\ -m_7^n & m_1^n \end{bmatrix},$$

$$D_1^n = \begin{bmatrix} m_3^n & -m_6^n \\ -m_2^n & m_5^n \end{bmatrix},\quad D_2^n = \begin{bmatrix} m_1^n & m_4^n \\ m_3^n & m_6^n \end{bmatrix},\quad D_3^n = \begin{bmatrix} -m_4^n & m_1^n \\ m_5^n & -m_2^n \end{bmatrix}, n = 1, 2, \dots., p.$$

3. Compute the elements,

$$c_1^n \to \det(B_1^n)\,, d_1^n \to \det(C_1^n)\,, l_1^n \to \det(D_1^n),$$
$$c_2^n \to \det(B_2^n)\,, d_2^n \to \det(C_2^n)\,, l_2^n \to \det(D_2^n),$$
$$c_2^n \to \det(B_3^n)\,, d_3^n \to \det(C_3^n)\,, l_3^n \to \det(D_3^n)$$

4. Compute the elements,

$$\frac{1}{\det(M_n)}[s_1^n C_1^n - s_2^n d_1^n - s_3^n l_1^n] \to p_1^n,$$
$$\frac{1}{\det(M_n)}[s_4^n C_1^n - s_5^n d_1^n - s_6^n l_1^n] \to p_2^n,$$
$$\frac{1}{\det(M_n)}[s_7^n C_1^n - s_8^n d_1^n - s_9^n l_1^n] \to p_3^n,$$

***Received**: 05-01-2026 - **Accepted**: 04-03-2026 - **Published**: 11-03-2026*

$$\frac{1}{\det(M_n)}[s_1^n C_2^n - s_2^n d_2^n - s_3^n l_2^n] \to p_4^n,$$
$$\frac{1}{\det(M_n)}[s_4^n C_2^n - s_5^n d_2^n - s_6^n l_2^n] \to p_5^n,$$
$$\frac{1}{\det(M_n)}[s_7^n C_2^n - s_8^n d_2^n - s_9^n l_2^n] \to p_6^n,$$
$$\frac{1}{\det(M_n)}[s_7^n C_2^n - s_8^n d_2^n - s_9^n l_2^n] \to p_6^n,$$
$$\frac{1}{\det(M_n)}[s_1^n C_3^n - s_2^n d_3^n - s_3^n l_3^n] \to p_7^n,$$
$$\frac{1}{\det(M_n)}[s_4^n C_3^n - s_5^n d_3^n - s_6^n l_3^n] \to p_8^n,$$
$$\frac{1}{\det(M_n)}[s_7^n C_3^n - s_8^n d_3^n - s_8^n l_3^n] \to p_9^n,$$

5. Compute the elements, $g_h^n, (1 \le h \le 9)$, $n = 1, 2, \dots, p$, of the decryption text, as follows:

$$p_r^n - a_r^n \to g_h^n(modq), \quad r = h = t = 1, 5, 9,$$
$$p_r^n - a_r^n \to g_h^n(modq), \quad r = 4, h = 2,$$
$$p_r^n - a_r^n \to g_h^n(modq), \quad r = 7, h = 3,$$
$$p_r^n - a_r^n \to g_h^n(modq), \quad r = 2, h = 4,$$
$$p_r^n - a_r^n \to g_h^n(modq), \quad r = 8, h = 6,$$
$$p_r^n - a_r^n \to g_h^n(modq), \quad r = 3, h = 7,$$
$$p_r^n - a_r^n \to g_h^n(modq), \quad r = 6, h = 8,$$

6. Construct the matrix $T = \begin{bmatrix} g_1^1 & g_2^1 & g_3^1 & g_1^2 & g_2^2 & g_3^2 & \cdots & g_1^p & g_2^p & g_3^p \\ g_4^1 & g_5^1 & g_6^1 & g_4^2 & g_5^2 & g_6^2 & \cdots & g_4^p & g_5^p & g_6^p \\ g_7^1 & g_8^1 & g_9^1 & g_7^2 & g_8^2 & g_9^2 & \cdots & g_7^p & g_8^p & g_9^p \end{bmatrix}$.
7. 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:

"NEXT-GENERATION CRYPTOGRAPHERS: ABDULLAH (1), MOHANAD (2), SAMYRAH (3)."

Encryption Algorithm.

Step 1. To encrypt the message, we put the message in the message matrix T as follows:

$$T = \begin{bmatrix} N & E & X & T & - & G & E & N & E & R & A & T & I & O & N & \theta & C & R & Y & P & T & O & G & R \\ A & P & H & E & R & S & : & \theta & A & B & D & U & L & L & A & H & (& 1 &) & , & \theta & M & O & H \\ A & N & A & D & \theta & (& 2 &) & , & \theta & S & A & M & Y & R & A & H & \theta & (& 3 &) & \theta & \theta & \theta \end{bmatrix}.$$

Step 2. Divide the matrix T of size 3×24 into blocks $G_n, n = 1, 2, \dots, 8$ of size 3×3, as follows,

$$G_1 = \begin{bmatrix} N & E & X \\ A & P & H \\ A & N & A \end{bmatrix}, G_2 = \begin{bmatrix} T & - & G \\ E & R & S \\ D & \theta & (\end{bmatrix}, G_3 = \begin{bmatrix} E & N & E \\ : & \theta & A \\ 2 &) & , \end{bmatrix}, G_4 = \begin{bmatrix} R & A & T \\ B & D & U \\ \theta & S & A \end{bmatrix},$$

$$G_5 = \begin{bmatrix} I & O & N \\ L & L & A \\ M & Y & R \end{bmatrix}, G_6 = \begin{bmatrix} \theta & C & R \\ H & (& 1 \\ A & H & \theta \end{bmatrix}, G_7 = \begin{bmatrix} Y & P & T \\ ) & , & \theta \\ (& 3 &) \end{bmatrix}, G_8 = \begin{bmatrix} O & G & R \\ M & O & H \\ \theta & \theta & \theta \end{bmatrix}.$$

Step 3. From Step (2), since the number of the block matrices $G_n, n = 1, 2, \dots, 8$, is 8, so $k = 8$.

Step 4. To find j, from Step (3), we have $n = 8 > 3$, then $j = 6$. So the following "character table" for the message matrix T:

Table 2. Shift Cipher Encoding Table

N	E	X	A	P	H	A	N	A
31	22	6	18	33	25	18	31	18
T	$-$	G	E	R	S	D	θ	(
2	14	27	22	0	1	21	9	10
E	N	E	:	θ	A	2	)	,
22	31	22	12	9	18	16	11	13

***Received**: 05-01-2026 - **Accepted**: 04-03-2026 - **Published**: 11-03-2026*

R	*A*	*T*	*B*	*D*	*U*	*θ*	*S*	*A*
0	18	2	19	21	3	9	1	18
I	*O*	*N*	*L*	*L*	*A*	*M*	*Y*	*R*
26	32	31	29	29	18	30	7	0
θ	*C*	*R*	*H*	(	1	*A*	*H*	*θ*
9	20	0	25	10	15	18	25	9
Y	*P*	*T*	)	,	*θ*	(	3	)
7	33	2	11	13	9	10	17	11
O	*G*	*R*	*M*	*O*	*H*	*θ*	*θ*	*θ*
32	24	0	30	32	25	9	9	9

Step 5. The elements $g_h^n, (1 \le h \le 9)$ of the block matrices $G_n, n = 1, 2, \dots, 8$.

Table 3. Block Matrix Elements Table

g_1^1	g_2^1	g_3^1	g_4^1	g_5^1	g_6^1	g_7^1	g_8^1	g_9^1
31	22	6	18	33	25	18	31	18
g_1^2	g_2^2	g_3^2	g_4^2	g_5^2	g_6^2	g_7^2	g_8^2	g_9^2
2	14	27	22	0	1	21	9	10
g_1^3	g_2^3	g_3^3	g_4^3	g_5^3	g_6^3	g_7^3	g_8^3	g_9^3
22	31	22	12	9	18	16	11	13
g_1^4	g_2^4	g_3^4	g_4^4	g_5^4	g_6^4	g_7^4	g_8^4	g_9^4
0	18	2	19	21	3	9	1	18
g_1^5	g_2^5	g_3^5	g_4^5	g_5^5	g_6^5	g_7^5	g_8^5	g_9^5
26	32	31	29	29	18	30	7	0
g_1^6	g_2^6	g_3^6	g_4^6	g_5^6	g_6^6	g_7^6	g_8^6	g_9^6
9	20	0	25	10	15	18	25	9
g_1^7	g_2^7	g_3^7	g_4^7	g_5^7	g_6^7	g_7^7	g_8^7	g_9^7
7	33	2	11	13	9	10	17	11
g_1^8	g_2^8	g_3^8	g_4^8	g_5^8	g_6^8	g_7^8	g_8^8	g_9^8
32	24	0	30	32	25	9	9	9

Step 6. Now, we determine the encryption keys, $M_n, n = 1, 2, \dots, 8$ such that $(det(M_n),\ 35) = 1$,

$$M_1 = \begin{bmatrix} 1 & 0 & 3 \\ -2 & 1 & 6 \\ 0 & 2 & 1 \end{bmatrix},\ M_2 = \begin{bmatrix} 2 & -2 & 0 \\ 0 & -7 & 3 \\ 4 & 0 & 1 \end{bmatrix},\ M_3 = \begin{bmatrix} -1 & 3 & 5 \\ 0 & 1 & -9 \\ 0 & 2 & -2 \end{bmatrix},\ M_4 = \begin{bmatrix} 0 & 2 & 0 \\ 3 & 6 & -2 \\ -2 & -5 & 1 \end{bmatrix},$$

$$M_5 = \begin{bmatrix} -2 & 4 & 5 \\ 3 & -2 & -3 \\ 0 & 0 & 2 \end{bmatrix},\ M_6 = \begin{bmatrix} 6 & -1 & 2 \\ -5 & -4 & 0 \\ 2 & 7 & 0 \end{bmatrix},\ M_7 = \begin{bmatrix} -3 & 0 & -4 \\ 1 & 3 & 2 \\ 3 & 0 & 1 \end{bmatrix},\ M_8 = \begin{bmatrix} 0 & 3 & 2 \\ 1 & 0 & 2 \\ 3 & 1 & 1 \end{bmatrix},$$

Therefore,

$det(M_1) = -23 \equiv 12(mod35)$, then $(12,35) = 1$, $\frac{1}{\det(M_1)} = \frac{1}{12} = 12^{-1} \equiv 3\ (mod35)$,

$det(M_2) = -38 \equiv 32(mod35)$, hence $(32,35) = 1$, $\frac{1}{\det(M_2)} = \frac{1}{32} = 32^{-1} \equiv 23\ (mod35)$,

$det(M_3) = -16 \equiv 19(mod35)$, then $(19,35) = 1$, $\frac{1}{\det(M_3)} = \frac{1}{19} = 19^{-1} \equiv 24\ (mod35)$,

$det(M_4) = 2 \equiv 2(mod35)$, hence $(2,35) = 1$, $\frac{1}{\det(M_4)} = \frac{1}{2} = 2^{-1} \equiv 18\ (mod35)$,

$det(M_5) = -16 \equiv 19(mod35)$, then $(19,35) = 1$, $\frac{1}{\det(M_5)} = \frac{1}{19} = 19^{-1} \equiv 24\ (mod35)$,

$det(M_6) = -54 \equiv 16(mod35)$, so $(16,35) = 1$, $\frac{1}{\det(M_6)} = \frac{1}{16} = 16^{-1} \equiv 11\ (mod35)$,

$det(M_7) = 27 \equiv 27(mod35)$, then $(27,35) = 1$, $\frac{1}{\det(M_7)} = \frac{1}{27} = 27^{-1} \equiv 13\ (mod35)$,

$det(M_8) = 17 \equiv 17(mod35)$, so $(17,35) = 1$. $\frac{1}{\det(M_8)} = \frac{1}{17} = 17^{-1} \equiv 33\ (mod35)$.

And the encryption keys, $A_n, n = 1, 2, \dots, 8$,

$$A_1 = \begin{bmatrix} 1 & 3 & -1 \\ 4 & -7 & 0 \\ 0 & 2 & -2 \end{bmatrix},\ A_2 = \begin{bmatrix} 3 & -1 & 0 \\ 5 & -6 & 2 \\ 0 & -3 & 0 \end{bmatrix},\ A_3 = \begin{bmatrix} -2 & 8 & 0 \\ 2 & -3 & 1 \\ 0 & 4 & 6 \end{bmatrix},\ A_4 = \begin{bmatrix} -5 & 0 & 3 \\ 7 & 2 & -3 \\ 0 & 5 & 1 \end{bmatrix},$$

$$A_5 = \begin{bmatrix} 2 & -3 & 0 \\ 4 & -8 & 1 \\ 0 & 10 & 2 \end{bmatrix},\ A_6 = \begin{bmatrix} 5 & -3 & 9 \\ 11 & -1 & 0 \\ 3 & 1 & 4 \end{bmatrix},\ A_7 = \begin{bmatrix} 2 & 9 & 7 \\ 0 & 4 & -2 \\ 0 & -3 & 5 \end{bmatrix},\ A_8 = \begin{bmatrix} 8 & -1 & 0 \\ 3 & -5 & -6 \\ 2 & 12 & 4 \end{bmatrix}.$$

***Received**: 05-01-2026 - **Accepted**: 04-03-2026 - **Published**: 11-03-2026*

Step 7. We compute the elements e_1^n, e_5^n, e_9^n, $n = 1, 2, \dots, 8$.

Table 4(a). Indexed Arithmetic Generation Table for key and Block Elements

r=h = t = 1	e_1^1	e_1^2	e_1^3	e_1^4	e_1^5	e_1^6	e_1^7	e_1^8
	32	5	20	30	28	14	9	5
r=h = t = 5	e_5^1	e_5^2	e_5^3	e_5^4	e_5^5	e_5^6	e_5^7	e_5^8
	26	29	6	23	21	9	17	27
r=h = t = 9	e_9^1	e_9^2	e_9^3	e_9^4	e_9^5	e_9^6	e_9^7	e_9^8
	16	10	19	19	2	13	16	13

Now, we compute the elements $e_2^n, e_3^n, e_4^n, e_6^n, e_7^n, e_8^n$, $n = 1, 2, \dots, 8$.

Table 4(b). Indexed Arithmetic Generation Table for key and Block Elements

r=**2**, **h = 4**	e_2^1	e_2^2	e_2^3	e_2^4	e_2^5	e_2^6	e_2^7	e_2^8
	21	21	20	19	26	22	20	29
r=3, h = 7	e_3^1	e_3^2	e_3^3	e_3^4	e_3^5	e_3^6	e_3^7	e_3^8
	17	21	16	12	30	27	17	9
r=4, h = 2	e_4^1	e_4^2	e_4^3	e_4^4	e_4^5	e_4^6	e_4^7	e_4^8
	26	19	33	25	1	31	33	27
r=6, h = 8	e_6^1	e_6^2	e_6^3	e_6^4	e_6^5	e_6^6	e_6^7	e_6^8
	31	11	12	33	8	25	15	3
r=7, h = 3	e_7^1	e_7^2	e_7^3	e_7^4	e_7^5	e_7^6	e_7^7	e_7^8
	6	27	22	2	31	3	2	2
r=8, h = 6	e_8^1	e_8^2	e_8^3	e_8^4	e_8^5	e_8^6	e_8^7	e_8^8
	27	33	22	8	28	16	6	2

Step 8. We compute the elements $s_1^n, s_2^n, s_3^n, s_4^n, s_5^n, s_6^n, s_7^n, s_8^n, s_9^n, n = 1, 2, \dots, 8$.

for $n = 1, 2, \dots, 8$ we comput the elements $s_1^1, s_1^2, s_1^3, s_1^4, s_1^5, s_1^6, s_1^7, s_1^8$,

$s_1^1 = e_1^1 m_1^1 + e_4^1 m_2^1 + e_7^1 m_3^1 = 50 \equiv 15(mod35)$, $s_1^2 = e_1^2 m_1^2 + e_4^2 m_2^2 + e_7^2 m_3^2 = -28 \equiv 7(mod35)$,
$s_1^3 = e_1^3 m_1^3 + e_4^3 m_2^3 + e_7^3 m_3^3 = 189 \equiv 14(mod35)$, $s_1^4 = e_1^4 m_1^4 + e_4^4 m_2^4 + e_7^4 m_3^4 = 50 \equiv 15(mod35)$,
$s_1^5 = e_1^5 m_1^5 + e_4^5 m_2^5 + e_7^5 m_3^5 = 103 \equiv 33(mod35)$, $s_1^6 = e_1^6 m_1^6 + e_4^6 m_2^6 + e_7^6 m_3^6 = 59 \equiv 24(mod35)$,
$s_1^7 = e_1^7 m_1^7 + e_4^7 m_2^7 + e_7^7 m_3^7 = -35 \equiv 0(mod35)$, $s_1^8 = e_1^8 m_1^8 + e_4^8 m_2^8 + e_7^8 m_3^8 = 85 \equiv 15(mod35)$,

for $n = 1, 2, \dots, 8$, we comput the elements $s_2^1, s_2^2, s_2^3, s_2^4, s_2^5, s_2^6, s_2^7, s_2^8$,

$s_2^1 = e_1^1 m_4^1 + e_4^1 m_5^1 + e_7^1 m_6^1 = -2 \equiv 33(mod35)$, $s_2^2 = e_1^2 m_4^2 + e_4^2 m_5^2 + e_7^2 m_6^2 = -52 \equiv 18(mod35)$,
$s_2^3 = e_1^3 m_4^3 + e_4^3 m_5^3 + e_7^3 m_6^3 = -165 \equiv 10(mod35)$, $s_2^4 = e_1^4 m_4^4 + e_4^4 m_5^4 + e_7^4 m_6^4 = 236 \equiv 26(mod35)$,
$s_2^5 = e_1^5 m_4^5 + e_4^5 m_5^5 + e_7^5 m_6^5 = -11 \equiv 24(mod35)$, $s_2^6 = e_1^6 m_4^6 + e_4^6 m_5^6 + e_7^6 m_6^6 = -194 \equiv 16(mod35)$,
$s_2^7 = e_1^7 m_4^7 + e_4^7 m_5^7 + e_7^7 m_6^7 = 112 \equiv 7(mod35)$, $s_2^8 = e_1^8 m_4^8 + e_4^8 m_5^8 + e_7^8 m_6^8 = 9 \equiv 9(mod35)$.

for $n = 1, 2, \dots, 8$, we comput the elements $s_3^1, s_3^2, s_3^3, s_3^4, s_3^5, s_3^6, s_3^7, s_3^8$,

$s_3^1 = e_1^1 m_7^1 + e_4^1 m_8^1 + e_7^1 m_9^1 = 58 \equiv 23(mod35)$, $s_3^2 = e_1^2 m_7^2 + e_4^2 m_8^2 + e_7^2 m_9^2 = 47 \equiv 12(mod35)$,
$s_3^3 = e_1^3 m_7^3 + e_4^3 m_8^3 + e_7^3 m_9^3 = 22 \equiv 22(mod35)$, $s_3^4 = e_1^4 m_7^4 + e_4^4 m_8^4 + e_7^4 m_9^4 = -183 \equiv 27(mod35)$,
$s_3^5 = e_1^5 m_7^5 + e_4^5 m_8^5 + e_7^5 m_9^5 = 62 \equiv 27(mod35)$, $s_3^6 = e_1^6 m_7^6 + e_4^6 m_8^6 + e_7^6 m_9^6 = 245 \equiv 0(mod35)$,
$s_3^7 = e_1^7 m_7^7 + e_4^7 m_8^7 + e_7^7 m_9^7 = 29 \equiv 29(mod35)$, $s_3^8 = e_1^8 m_7^8 + e_4^8 m_8^8 + e_7^8 m_9^8 = 44 \equiv 9(mod35)$.

for $n = 1, 2, \dots, 8$, we comput the elements $s_4^1, s_4^2, s_4^3, s_4^4, s_4^5, s_4^6, s_4^7, s_4^8$,

$s_4^1 = e_2^1 m_1^1 + e_5^1 m_2^1 + e_8^1 m_3^1 = 102 \equiv 32(mod35)$, $s_4^2 = e_2^2 m_1^2 + e_5^2 m_2^2 + e_8^2 m_3^2 = -16 \equiv 19(mod35)$,
$s_4^3 = e_2^3 m_1^3 + e_5^3 m_2^3 + e_8^3 m_3^3 = 108 \equiv 3(mod35)$, $s_4^4 = e_2^4 m_1^4 + e_5^4 m_2^4 + e_8^4 m_3^4 = 46 \equiv 11(mod35)$,
$s_4^5 = e_2^5 m_1^5 + e_5^5 m_2^5 + e_8^5 m_3^5 = 172 \equiv 32(mod35)$, $s_4^6 = e_2^6 m_1^6 + e_5^6 m_2^6 + e_8^6 m_3^6 = 155 \equiv 15(mod35)$,
$s_4^7 = e_2^7 m_1^7 + e_5^7 m_2^7 + e_8^7 m_3^7 = -84 \equiv 21(mod35)$, $s_4^8 = e_2^8 m_1^8 + e_5^8 m_2^8 + e_8^8 m_3^8 = 85 \equiv 15(mod35)$.

for $n = 1, 2, \dots, 8$, we comput the elements $s_5^1, s_5^2, s_5^3, s_5^4, s_5^5, s_5^6, s_5^7, s_5^8$,

$s_5^1 = e_2^1 m_4^1 + e_5^1 m_5^1 + e_8^1 m_6^1 = 146 \equiv 6(mod35)$, $s_5^2 = e_2^2 m_4^2 + e_5^2 m_5^2 + e_8^2 m_6^2 = -104 \equiv 1(mod35)$,
$s_5^3 = e_2^3 m_4^3 + e_5^3 m_5^3 + e_8^3 m_6^3 = -192 \equiv 18(mod35)$, $s_5^4 = e_2^4 m_4^4 + e_5^4 m_5^4 + e_8^4 m_6^4 = 179 \equiv 4(mod35)$,
$s_5^5 = e_2^5 m_4^5 + e_5^5 m_5^5 + e_8^5 m_6^5 = -48 \equiv 22(mod35)$, $s_5^6 = e_2^6 m_4^6 + e_5^6 m_5^6 + e_8^6 m_6^6 = -146 \equiv 29(mod35)$,
$s_5^7 = e_2^7 m_4^7 + e_5^7 m_5^7 + e_8^7 m_6^7 = 83 \equiv 13(mod35)$, $s_5^8 = e_2^8 m_4^8 + e_5^8 m_5^8 + e_8^8 m_6^8 = 33 \equiv 33(mod35)$.

for $n = 1, 2, \dots, 8$, we comput the elements $s_6^1, s_6^2, s_6^3, s_6^4, s_6^5, s_6^6, s_6^7, s_6^8$,

$s_6^1 = e_2^1 m_7^1 + e_5^1 m_8^1 + e_8^1 m_9^1 = 79 \equiv 9(mod35)$, $s_6^2 = e_2^2 m_7^2 + e_5^2 m_8^2 + e_8^2 m_9^2 = 117 \equiv 12(mod35)$,
$s_6^3 = e_2^3 m_7^3 + e_5^3 m_8^3 + e_8^3 m_9^3 = -32 \equiv 3(mod35)$, $s_6^4 = e_2^4 m_7^4 + e_5^4 m_8^4 + e_8^4 m_9^4 = -145 \equiv 30(mod35)$,
$s_6^5 = e_2^5 m_7^5 + e_5^5 m_8^5 + e_8^5 m_9^5 = 56 \equiv 21(mod35)$, $s_6^6 = e_2^6 m_7^6 + e_5^6 m_8^6 + e_8^6 m_9^6 = 107 \equiv 2(mod35)$,
$s_6^7 = e_2^7 m_7^7 + e_5^7 m_8^7 + e_8^7 m_9^7 = 66 \equiv 31(mod35)$, $s_6^8 = e_2^8 m_7^8 + e_5^8 m_8^8 + e_8^8 m_9^8 = 116 \equiv 11(mod35)$.

***Received**: 05-01-2026 - **Accepted**: 04-03-2026 - **Published**: 11-03-2026*

for $n = 1,2,\dots,8$, we comput the elements $s_7^1, s_7^2, s_7^3, s_7^4, s_7^5, s_7^6, s_7^7, s_7^8$,

$$s_7^1 = e_3^1 m_1^1 + e_6^1 m_2^1 + e_9^1 m_3^1 = 65 \equiv 30(mod35), \quad s_7^2 = e_3^2 m_1^2 + e_6^2 m_2^2 + e_9^2 m_3^2 = 20 \equiv 20(mod35),$$
$$s_7^3 = e_3^3 m_1^3 + e_6^3 m_2^3 + e_9^3 m_3^3 = 115 \equiv 10(mod35), \quad s_7^4 = e_3^4 m_1^4 + e_6^4 m_2^4 + e_9^4 m_3^4 = 66 \equiv 31(mod35),$$
$$s_7^5 = e_3^5 m_1^5 + e_6^5 m_2^5 + e_9^5 m_3^5 = -18 \equiv 17(mod35), \quad s_7^6 = e_3^6 m_1^6 + e_6^6 m_2^6 + e_9^6 m_3^6 = 163 \equiv 23(mod35),$$
$$s_7^7 = e_3^7 m_1^7 + e_6^7 m_2^7 + e_9^7 m_3^7 = -115 \equiv 25(mod35), \quad s_7^8 = e_3^8 m_1^8 + e_6^8 m_2^8 + e_9^8 m_3^8 = 35 \equiv 0(mod35).$$

for $n = 1,2,\dots,8$, we comput the elements $s_8^1, s_8^2, s_8^3, s_8^4, s_8^5, s_8^6, s_8^7, s_8^8$,

$$s_8^1 = e_3^1 m_4^1 + e_6^1 m_5^1 + e_9^1 m_6^1 = 93 \equiv 23(mod35), \quad s_8^2 = e_3^2 m_4^2 + e_6^2 m_5^2 + e_9^2 m_6^2 = -47 \equiv 23(mod35),$$
$$s_8^3 = e_3^3 m_4^3 + e_6^3 m_5^3 + e_9^3 m_6^3 = -159 \equiv 16(mod35), \quad s_8^4 = e_3^4 m_4^8 + e_6^4 m_5^4 + e_9^4 m_6^4 = 196 \equiv 21(mod35),$$
$$s_8^5 = e_3^5 m_4^5 + e_6^5 m_5^5 + e_9^5 m_6^5 = 68 \equiv 33(mod35), \quad s_8^6 = e_3^6 m_4^6 + e_6^6 m_5^6 + e_9^6 m_6^6 = -235 \equiv 10(mod35),$$
$$s_8^7 = e_3^7 m_4^7 + e_6^7 m_5^7 + e_9^7 m_6^7 = 94 \equiv 24(mod35), \quad s_8^8 = e_3^8 m_4^8 + e_6^8 m_5^8 + e_9^8 m_6^8 = 35 \equiv 0(mod35),$$

for $n = 1,2,\dots,8$, we comput the elements $s_9^1, s_9^2, s_9^3, s_9^4, s_9^5, s_9^6, s_9^7, s_9^8$,

$$s_9^1 = e_3^1 m_7^1 + e_6^1 m_8^1 + e_9^1 m_9^1 = 78 \equiv 8(mod35), \quad s_9^2 = e_3^2 m_7^2 + e_6^2 m_8^2 + e_9^2 m_9^2 = 94 \equiv 24(mod35),$$
$$s_9^3 = e_3^3 m_7^3 + e_6^3 m_8^3 + e_9^3 m_9^3 = -14 \equiv 21(mod35), \quad s_9^4 = e_3^4 m_7^4 + e_6^4 m_8^4 + e_9^4 m_9^4 = -170 \equiv 5(mod35),$$
$$s_9^5 = e_3^5 m_7^5 + e_6^5 m_8^5 + e_9^5 m_9^5 = 4 \equiv 4(mod35), \quad s_9^6 = e_3^6 m_7^6 + e_6^6 m_8^6 + e_9^6 m_9^6 = 229 \equiv 16(mod35),$$
$$s_9^7 = e_3^7 m_7^7 + e_6^7 m_8^7 + e_9^7 m_9^7 = 67 \equiv 32(mod35), \quad s_9^8 = e_3^8 m_7^8 + e_6^8 m_8^8 + e_9^8 m_9^8 = 43 \equiv 8(mod35).$$

Step 9. Construct the encrypted block matrices $S_n, n = 1,2,\dots,8$ corresponding to the block matrices $G_n, n = 1,2,\dots,8$ as follow,

$$S_1 = \begin{bmatrix} 15 & 33 & 23 \\ 32 & 6 & 9 \\ 30 & 23 & 8 \end{bmatrix}, S_2 = \begin{bmatrix} 7 & 18 & 12 \\ 19 & 1 & 12 \\ 20 & 23 & 24 \end{bmatrix}, S_3 = \begin{bmatrix} 14 & 10 & 22 \\ 3 & 18 & 3 \\ 10 & 16 & 21 \end{bmatrix}, S_4 = \begin{bmatrix} 15 & 26 & 27 \\ 11 & 4 & 30 \\ 31 & 21 & 5 \end{bmatrix},$$
$$S_5 = \begin{bmatrix} 33 & 24 & 27 \\ 32 & 22 & 21 \\ 17 & 33 & 4 \end{bmatrix}, S_6 = \begin{bmatrix} 24 & 16 & 0 \\ 15 & 29 & 2 \\ 23 & 10 & 16 \end{bmatrix}, \quad S_7 = \begin{bmatrix} 0 & 7 & 29 \\ 21 & 13 & 31 \\ 25 & 24 & 32 \end{bmatrix}, S_8 = \begin{bmatrix} 15 & 9 & 9 \\ 18 & 33 & 12 \\ 0 & 0 & 8 \end{bmatrix}.$$

Step 10. Construct the matrix $S = \begin{bmatrix} s_1^1 & s_2^1 & s_3^1 & s_1^2 & s_2^2 & s_3^2 & \cdots & s_1^8 & s_2^8 & s_3^8 \\ s_4^1 & s_5^1 & s_6^1 & s_4^2 & s_5^2 & s_6^2 & \cdots & s_4^8 & s_5^8 & s_6^8 \\ s_7^1 & s_8^1 & s_9^1 & s_7^2 & s_8^2 & s_9^2 & \cdots & s_7^8 & s_8^8 & s_9^8 \end{bmatrix}$,

$$S = \begin{bmatrix} 15 & 33 & 23 & 7 & 18 & 12 & 14 & 10 & 22 & 15 & 26 & 27 & 33 & 24 & 27 & 24 & 16 & 0 & 0 & 7 & 29 & 15 & 9 & 9 \\ 32 & 6 & 9 & 19 & 1 & 12 & 3 & 18 & 3 & 11 & 4 & 30 & 32 & 22 & 21 & 15 & 29 & 2 & 21 & 13 & 31 & 18 & 33 & 12 \\ 30 & 23 & 8 & 20 & 23 & 24 & 10 & 16 & 21 & 31 & 21 & 5 & 17 & 33 & 4 & 23 & 10 & 16 & 25 & 24 & 32 & 0 & 0 & 8 \end{bmatrix}.$$

Step 11. End of algorithm.

Decryption Algorithm.

Step 1. After dividing the cipher message matrix S into blocks $S_n, n = 1,2,\dots,8$, The decryption key matrices are obtained by substituting values into the matrices derived from the encryption key elements. They are formulated as 2×2 matrices whose entries depend on $n = 1,2,\dots,8$.

Now, we compute the decryption key matrices, $B_1^1, B_1^2, B_1^3, B_1^4, B_1^5, B_1^6, B_1^7, B_1^8$ as follows,

$$B_1^1 = \begin{bmatrix} -1 & 2 \\ 6 & -1 \end{bmatrix}, \quad B_1^2 = \begin{bmatrix} 7 & 0 \\ 3 & -1 \end{bmatrix}, \quad B_1^3 = \begin{bmatrix} -1 & 2 \\ -9 & 2 \end{bmatrix}, \quad B_1^4 = \begin{bmatrix} -6 & -5 \\ -2 & -1 \end{bmatrix}$$
$$B_1^5 = \begin{bmatrix} 2 & 0 \\ -3 & -2 \end{bmatrix}, \quad B_1^6 = \begin{bmatrix} 4 & 7 \\ 0 & 0 \end{bmatrix}, \quad B_1^7 = \begin{bmatrix} -3 & 0 \\ 2 & -1 \end{bmatrix}, \quad B_1^8 = \begin{bmatrix} 0 & 1 \\ 2 & -1 \end{bmatrix}.$$

We compute the decryption key matrices, $B_2^1, B_2^2, B_2^3, B_2^4, B_2^5, B_2^6, B_2^7, B_2^8$ as follows,

$$B_2^1 = \begin{bmatrix} -6 & -1 \\ 2 & 0 \end{bmatrix}, \quad B_2^2 = \begin{bmatrix} -3 & -1 \\ 0 & -4 \end{bmatrix}, \quad B_2^3 = \begin{bmatrix} 9 & 2 \\ 0 & 0 \end{bmatrix}, \quad B_2^4 = \begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix}$$
$$B_2^5 = \begin{bmatrix} 3 & -2 \\ -3 & 0 \end{bmatrix}, \quad B_2^6 = \begin{bmatrix} 0 & 0 \\ 5 & -2 \end{bmatrix}, \quad B_2^7 = \begin{bmatrix} -2 & -1 \\ -1 & -3 \end{bmatrix}, \quad B_2^8 = \begin{bmatrix} -2 & -1 \\ -1 & -3 \end{bmatrix}.$$

Now, we compute the decryption key matrices, $B_3^1, B_3^2, B_3^3, B_3^4, B_3^5, B_3^6, B_3^7, B_3^8$ as follows,

$$B_3^1 = \begin{bmatrix} 2 & 0 \\ -1 & -2 \end{bmatrix}, \quad B_3^2 = \begin{bmatrix} 0 & -4 \\ 7 & 0 \end{bmatrix}, \quad B_3^3 = \begin{bmatrix} 0 & 0 \\ -1 & -2 \end{bmatrix}, \quad B_3^4 = \begin{bmatrix} -3 & 2 \\ -6 & 5 \end{bmatrix}$$
$$B_3^5 = \begin{bmatrix} -3 & 0 \\ 2 & 0 \end{bmatrix}, \quad B_3^6 = \begin{bmatrix} 5 & -2 \\ 4 & -7 \end{bmatrix}, \quad B_3^7 = \begin{bmatrix} -1 & -3 \\ -3 & 0 \end{bmatrix}, \quad B_3^8 = \begin{bmatrix} -1 & -3 \\ 0 & -1 \end{bmatrix}.$$

Now, we compute the decryption key matrices, $C_1^1, C_1^2, C_1^3, C_1^4, C_1^5, C_1^6, C_1^7, C_1^8$ as follows,

$$C_1^1 = \begin{bmatrix} 0 & -2 \\ -3 & -1 \end{bmatrix}, \quad C_1^2 = \begin{bmatrix} 2 & 0 \\ 0 & -1 \end{bmatrix}, \quad C_1^3 = \begin{bmatrix} -3 & -2 \\ -5 & 2 \end{bmatrix}, \quad C_1^4 = \begin{bmatrix} -2 & 5 \\ 0 & -1 \end{bmatrix}$$

Received*: 05-01-2026 -* ***Accepted****: 04-03-2026 -* ***Published****: 11-03-2026*

$$C_1^5=\begin{bmatrix}-4 & 0\\ -5 & -2\end{bmatrix},\quad C_1^6=\begin{bmatrix}1 & -7\\ -2 & 0\end{bmatrix},\quad C_1^7=\begin{bmatrix}0 & 0\\ 4 & -1\end{bmatrix},\quad C_1^8=\begin{bmatrix}-3 & -1\\ -2 & -1\end{bmatrix}.$$

Now, we compute the decryption key matrices, $C_2^1, C_2^2, C_2^3, C_2^4, C_2^5, C_2^6, C_2^7, C_2^8$ as follows,

$$C_2^1=\begin{bmatrix}-3 & 1\\ 1 & 0\end{bmatrix},\quad C_2^2=\begin{bmatrix}0 & 1\\ 2 & -4\end{bmatrix},\quad C_2^3=\begin{bmatrix}-5 & -2\\ -1 & 0\end{bmatrix},\quad C_2^4=\begin{bmatrix}0 & 1\\ 0 & 2\end{bmatrix}$$

$$C_2^5=\begin{bmatrix}-5 & 2\\ -2 & 0\end{bmatrix},\quad C_2^6=\begin{bmatrix}-2 & 0\\ 6 & -2\end{bmatrix},\quad C_2^7=\begin{bmatrix}4 & 1\\ -3 & -3\end{bmatrix},\quad C_2^8=\begin{bmatrix}-2 & 1\\ 0 & -3\end{bmatrix}.$$

Now, we compute the decryption key matrices, $C_3^1, C_3^2, C_3^3, C_3^4, C_3^5, C_3^6, C_3^7, C_3^8$ as follows,

$$C_3^1=\begin{bmatrix}2 & 0\\ 0 & 1\end{bmatrix},\quad C_3^2=\begin{bmatrix}0 & 2\\ -4 & 2\end{bmatrix},\quad C_3^3=\begin{bmatrix}2 & -3\\ 0 & -1\end{bmatrix},\quad C_3^4=\begin{bmatrix}-5 & -2\\ 2 & 0\end{bmatrix}$$

$$C_3^5=\begin{bmatrix}0 & -4\\ 0 & -2\end{bmatrix},\quad C_3^6=\begin{bmatrix}7 & 1\\ -2 & 6\end{bmatrix},\quad C_3^7=\begin{bmatrix}0 & 0\\ -3 & -3\end{bmatrix},\quad D_3^8=\begin{bmatrix}1 & -3\\ -3 & 0\end{bmatrix}.$$

Now, we compute the matrices, $D_1^1, D_1^2, D_1^3, D_1^4, D_1^5, D_1^6, D_1^7, C_1^8$ as follows,

$$D_1^1=\begin{bmatrix}3 & -6\\ 0 & 1\end{bmatrix},\quad D_1^2=\begin{bmatrix}0 & -3\\ 2 & -7\end{bmatrix},\quad D_1^3=\begin{bmatrix}5 & 9\\ -3 & 1\end{bmatrix},\quad D_1^4=\begin{bmatrix}0 & 2\\ -2 & 6\end{bmatrix}$$

$$D_1^5=\begin{bmatrix}5 & 3\\ -4 & -2\end{bmatrix},\quad D_1^6=\begin{bmatrix}2 & 0\\ 1 & -4\end{bmatrix},\quad D_1^7=\begin{bmatrix}-4 & -2\\ 0 & 3\end{bmatrix},\quad D_1^8=\begin{bmatrix}2 & -2\\ -3 & 0\end{bmatrix}.$$

Now, we compute the decryption key matrices, $D_2^1, D_2^2, D_2^3, D_2^4, D_2^5, D_2^6, D_2^7, C_2^8$ as follows,

$$D_2^1=\begin{bmatrix}1 & -2\\ 3 & 6\end{bmatrix},\quad D_2^2=\begin{bmatrix}2 & 0\\ 0 & 3\end{bmatrix},\quad D_2^3=\begin{bmatrix}-1 & 0\\ 5 & -9\end{bmatrix},\quad D_2^4=\begin{bmatrix}0 & 3\\ 0 & -2\end{bmatrix}$$

$$D_2^5=\begin{bmatrix}-2 & 3\\ 5 & -3\end{bmatrix},\quad D_2^6=\begin{bmatrix}6 & -5\\ 2 & 0\end{bmatrix},\quad D_2^7=\begin{bmatrix}-3 & 1\\ -4 & 2\end{bmatrix},\quad D_2^8=\begin{bmatrix}0 & 1\\ 2 & 2\end{bmatrix}.$$

Now, we compute the decryption key matrices, $D_3^1, D_3^2, D_3^3, D_3^4, D_3^5, D_3^6, D_3^7, D_3^8$ as follows,

$$D_3^1=\begin{bmatrix}2 & 1\\ 1 & 0\end{bmatrix},\quad D_3^2=\begin{bmatrix}0 & 2\\ -7 & 2\end{bmatrix},\quad D_3^3=\begin{bmatrix}0 & -1\\ 1 & -3\end{bmatrix},\quad D_3^4=\begin{bmatrix}-3 & 0\\ 6 & -2\end{bmatrix}$$

$$D_3^5=\begin{bmatrix}-3 & -2\\ -2 & -4\end{bmatrix},\quad D_3^6=\begin{bmatrix}5 & 6\\ -4 & 1\end{bmatrix},\quad D_3^7=\begin{bmatrix}-1 & -3\\ 3 & 0\end{bmatrix},\quad D_3^8=\begin{bmatrix}-1 & 0\\ 0 & -3\end{bmatrix}.$$

Step 2. In this step, the determinants of the decryption key matrices generated using $n = 1,2,\dots,8$ are calculated based on step (1).

Now, the elements $c_1^1, c_1^2, c_1^3, c_1^4, c_1^5, c_1^6, c_1^7, c_1^8$ are computed by substituting $n = 1,2,\dots,8$, into the following formula $c_1^n \to \det(B_1^n)$,

$c_1^1 = \det(B_1^1) = -11$, $c_1^2 = \det(B_1^2) = -7$, $c_1^3 = \det(B_1^3) = 16$, $c_1^4 = \det(B_1^4) = -4$, $c_1^5 = \det(B_1^5) = -4$, $c_1^6 = \det(B_1^6) = 0$, $c_1^7 = \det(B_1^7) = 3$, $c_1^8 = \det(B_1^8) = -2$.

The same idea, to find the elements $c_2^1, c_2^2, c_2^3, c_2^4, c_2^5, c_2^6, c_2^7, c_2^8$ we substitute into the following formula $c_2^n \to \det(B_2^n)$, $n = 1,2,\dots,8$,

$c_2^1 = \det(B_2^1) = 2$, $c_2^2 = \det(B_2^2) = 12$, $c_2^3 = \det(B_2^3) = 0$, $c_2^4 = \det(B_2^4) = 1$, $c_2^5 = \det(B_2^5) = -6$, $c_2^6 = \det(B_2^6) = 0$ $c_2^7 = \det(B_2^7) = 5$, $c_2^8 = \det(B_2^8) = 5$.

In a similar manner, the elements $c_3^1, c_3^2, c_3^3, c_3^4, c_3^5, c_3^6, c_3^7, c_3^8$ are obtained by substituting $n = 1,2,\dots,8$, into the formula: $c_3^n \to \det(B_3^n)$,

$c_3^1 = \det(B_3^1) = -4$, $c_3^2 = \det(B_3^2) = 28$, $c_3^3 = \det(B_3^3) = 0$, $c_3^4 = \det(B_3^4) = -3$, $c_3^5 = \det(B_3^5) = 0$, $c_3^6 = \det(B_3^6) = -27$ $c_3^7 = \det(B_3^7) = -9$, $c_3^8 = \det(B_3^8) = 1$.

The same idea, to find the elements $d_1^1, d_1^2, d_1^3, d_1^4, d_1^5, d_1^6, d_1^7, d_1^8$ we substitute into the following formula: $d_1^n \to \det(C_1^n)$, $n = 1,2,\dots,8$,

$d_1^1 = \det(C_1^1) = -6$, $d_1^2 = \det(C_1^2) = -2$, $d_1^3 = \det(C_1^3) = -16$, $d_1^4 = \det(C_1^4) = 2$, $d_1^5 = \det(C_1^5) = 8$, $d_1^6 = \det(C_1^6) = -14$, $d_1^7 = \det(C_1^7) = 0$, $d_1^8 = \det(C_1^8) = 1$.

Similarly, the elements $d_2^1, d_2^2, d_2^3, d_2^4, d_2^5, d_2^6, d_2^7, d_2^8$ are computed using the formula: $d_2^n \to \det(C_2^n)$, $n = 1,2,\dots,8$,

$d_2^1 = \det(C_2^1) = -1$, $d_2^2 = \det(C_2^2) = -2$, $d_2^3 = \det(C_2^3) = -2$, $d_2^4 = \det(C_2^4) = 0$, $d_2^5 = \det(C_2^5) = 4$, $d_2^6 = \det(C_2^6) = 4$, $d_2^7 = \det(C_2^7) = -9$, $d_2^8 = \det(C_2^8) = 6$.

Similarly, using the formula: $d_3^n \to \det(C_3^n)$, $n = 1,2,\dots,8$ to compute $d_3^1, d_3^2, d_3^3, d_3^4, d_3^5, d_3^6, d_3^7, d_3^8$ as follows,

$d_3^1 = \det(C_3^1) = 2$, $d_3^2 = \det(C_3^2) = 8$, $d_3^3 = \det(C_3^3) = -2$, $d_3^4 = \det(C_3^4) = 4$, $d_3^5 = \det(C_3^5) = 0$, $d_3^6 = \det(C_3^6) = 44$, $d_3^7 = \det(C_3^7) = 0$, $d_3^8 = \det(C_3^8) = -9$.

***Received**: 05-01-2026 - **Accepted**: 04-03-2026 - **Published**: 11-03-2026*

The same idea, the elements $l_1^1, l_1^2, l_1^3, l_1^4, l_1^5, l_1^6, l_1^7, l_1^8$ are obtained by substituting $n = 1,2,\dots,8$, into the formula: $l_1^n \to \det(D_1^n)$,
$l_1^1 = \det(D_1^1) = 3$, $l_1^2 = \det(D_1^2) = 6$, $l_1^3 = \det(D_1^3) = 32$, $l_1^4 = \det(D_1^4) = 4$, $l_1^5 = \det(D_1^5) = 2$,
$l_1^6 = \det(D_1^6) = -8$, $l_1^7 = \det(D_1^7) = -12$, $l_1^8 = \det(D_1^8) = -6$.

Similarly, we find the elements $l_2^1, l_2^2, l_2^3, l_2^4, l_2^5, l_2^6, l_2^7, l_2^8$ by substitute $n = 1,2,\dots,8$ into the following formula: $l_2^n \to \det(D_2^n)$,
$l_2^1 = \det(D_2^1) = 12$, $l_2^2 = \det(D_2^2) = 6$, $l_2^3 = \det(D_2^3) = 9$, $l_2^4 = \det(D_2^4) = 0$, $l_2^5 = \det(D_2^5) = -9$, $l_2^6 = \det(D_2^6) = 10$,
$l_2^7 = \det(D_2^7) = -2$, $l_2^8 = \det(D_2^8) = -2$.

Finally, the elements $l_3^1, l_3^2, l_3^3, l_3^4, l_3^5, l_3^6, l_3^7, l_3^8$ are computed using the formula: $l_3^n \to \det(D_3^n)$, $n = 1,2,\dots,8$,
$l_3^1 = \det(D_3^1) = -1$, $l_3^2 = \det(D_3^2) = 14$, $l_3^3 = \det(D_3^3) = 1$, $l_3^4 = \det(D_3^4) = 6$, $l_3^5 = \det(D_3^5) = 8$, $l_3^6 = \det(D_3^6) = 29$,
$l_3^7 = \det(D_3^7) = 9$, $l_3^8 = \det(D_3^8) = 3$.

Step 3. In this step, we compute the elements, $p_1^n, p_2^n, p_3^n, p_4^n, p_5^n, p_6^n, p_7^n, p_8^n, p_9^n, n = 1,2,\dots,8$. So the elements $p_1^1, p_1^2, p_1^3, p_1^4, p_1^5, p_1^6, p_1^7, p_1^8$ are obtained by substituting $n = 1,2,\dots,8$, into the adopted formulation $\frac{1}{\det(M_n)}[s_1^n C_1^n - s_2^n d_1^n - s_3^n l_1^n] \to p_1^n$, resulting in eight distinct values that vary with n,

$$p_1^1 = \frac{1}{\det(M_1)}[s_1^1 C_1^1 - s_2^1 d_1^1 - s_3^1 l_1^1] = -108, \quad p_1^2 = \frac{1}{\det(M_2)}[s_1^2 C_1^2 - s_2^2 d_1^2 - s_3^2 l_1^2] = -1955,$$
$$p_1^3 = \frac{1}{\det(M_3)}[s_1^3 C_1^3 - s_2^3 d_1^3 - s_3^3 l_1^3] = 4080, \quad p_1^4 = \frac{1}{\det(M_4)}[s_1^4 C_1^4 - s_2^4 d_1^4 - s_3^4 l_1^4] = -3960,$$
$$p_1^5 = \frac{1}{\det(M_5)}[s_1^5 C_1^5 - s_2^5 d_1^5 - s_3^5 l_1^5] = -9072, \quad p_1^6 = \frac{1}{\det(M_6)}[s_1^6 C_1^6 - s_2^6 d_1^6 - s_3^6 l_1^6] = 2464,$$
$$p_1^7 = \frac{1}{\det(M_7)}[s_1^7 C_1^7 - s_2^7 d_1^7 - s_3^7 l_1^7] = 4524, \quad p_1^8 = \frac{1}{\det(M_8)}[s_1^8 C_1^8 - s_2^8 d_1^8 - s_3^8 l_1^8] = 495.$$

Following an approach analogous to the previous step, the elements $p_2^1, p_2^2, p_2^3, p_2^4, p_2^5, p_2^6, p_2^7, p_2^8$ are computed by substituting $n = 1,2,\dots,8$, into the adopted formulation $\frac{1}{\det(M_n)}[s_4^n C_1^n - s_5^n d_1^n - s_6^n l_1^n] \to p_2^n$, as follows,

$$p_2^1 = \frac{1}{\det(M_1)}[s_4^1 C_1^1 - s_5^1 d_1^1 - s_6^1 l_1^1] = -1029, \quad p_2^2 = \frac{1}{\det(M_2)}[s_4^2 C_1^2 - s_5^2 d_1^2 - s_6^2 l_1^2] = -4669,$$
$$p_2^3 = \frac{1}{\det(M_3)}[s_4^3 C_1^3 - s_5^3 d_1^3 - s_6^3 l_1^3] = -7680, \quad p_2^4 = \frac{1}{\det(M_4)}[s_4^4 C_1^4 - s_5^4 d_1^4 - s_6^4 l_1^4] = -3096,$$
$$p_2^5 = \frac{1}{\det(M_5)}[s_4^5 C_1^5 - s_5^5 d_1^5 - s_6^5 l_1^5] = -8304, \quad p_2^6 = \frac{1}{\det(M_6)}[s_4^6 C_1^6 - s_5^6 d_1^6 - s_6^6 l_1^6] = 4642,$$
$$p_2^7 = \frac{1}{\det(M_7)}[s_4^7 C_1^7 - s_5^7 d_1^7 - s_6^7 l_1^7] = 5655, \quad p_2^8 = \frac{1}{\det(M_8)}[s_4^8 C_1^8 - s_5^8 d_1^8 - s_6^8 l_1^8] = 99.$$

Following the same idea, the elements $p_3^1, p_3^2, p_3^3, p_3^4, p_3^5, p_3^6, p_3^7, p_3^8$ are obtained by substituting $n = 1,2,\dots,8$, into the formula: $\frac{1}{\det(M_n)}[s_7^n C_1^n - s_8^n d_1^n - s_9^n l_1^n] \to p_3^n$,

$$p_3^1 = \frac{1}{\det(M_1)}[s_7^1 C_1^1 - s_8^1 d_1^1 - s_9^1 l_1^1] = -648, \quad p_3^2 = \frac{1}{\det(M_2)}[s_7^2 C_1^2 - s_8^2 d_1^2 - s_9^2 l_1^2] = -5474,$$
$$p_3^3 = \frac{1}{\det(M_3)}[s_7^3 C_1^3 - s_8^3 d_1^3 - s_9^3 l_1^3] = 1416, \quad p_3^4 = \frac{1}{\det(M_4)}[s_7^4 C_1^4 - s_8^4 d_1^4 - s_9^4 l_1^4] = -3348,$$
$$p_3^5 = \frac{1}{\det(M_5)}[s_7^5 C_1^5 - s_8^5 d_1^5 - s_9^5 l_1^5] = -8160, \quad p_3^6 = \frac{1}{\det(M_6)}[s_7^6 C_1^6 - s_8^6 d_1^6 - s_9^6 l_1^6] = 3212,$$
$$p_3^7 = \frac{1}{\det(M_7)}[s_7^7 C_1^7 - s_8^7 d_1^7 - s_9^7 l_1^7] = 5967, \quad p_3^8 = \frac{1}{\det(M_8)}[s_7^8 C_1^8 - s_8^8 d_1^8 - s_9^8 l_1^8] = 1584.$$

In a similar manner, the elements $p_4^1, p_4^2, p_4^3, p_4^4, p_4^5, p_4^6, p_4^7, p_4^8$ are computed using the following formula: $\frac{1}{\det(M_n)}[s_1^n C_2^n - s_2^n d_2^n - s_3^n l_2^n] \to p_4^n, n = 1,2,\dots,8$

$$p_4^1 = \frac{1}{\det(M_1)}[s_1^1 C_2^1 - s_2^1 d_2^1 - s_3^1 l_2^1] = -639, \quad p_4^2 = \frac{1}{\det(M_2)}[s_1^2 C_2^2 - s_2^2 d_2^2 - s_3^2 l_2^2] = 1104,$$
$$p_4^3 = \frac{1}{\det(M_3)}[s_1^3 C_2^3 - s_2^3 d_2^3 - s_3^3 l_2^3] = -4272, \quad p_4^4 = \frac{1}{\det(M_4)}[s_1^4 C_2^4 - s_2^4 d_2^4 - s_3^4 l_2^4] = 270,$$
$$p_4^5 = \frac{1}{\det(M_5)}[s_1^5 C_2^5 - s_2^5 d_2^5 - s_3^5 l_2^5] = -1224, \quad p_4^6 = \frac{1}{\det(M_6)}[s_1^6 C_2^6 - s_2^6 d_2^6 - s_3^6 l_2^6] = -704,$$
$$p_4^7 = \frac{1}{\det(M_7)}[s_1^7 C_2^7 - s_2^7 d_2^7 - s_3^7 l_2^7] = 1573, \quad p_4^8 = \frac{1}{\det(M_8)}[s_1^8 C_2^8 - s_2^8 d_2^8 - s_3^8 l_2^8] = 1287.$$

Similarly, the elements $p_5^1, p_5^2, p_5^3, p_5^4, p_5^5, p_5^6, p_5^7, p_5^8$ are computed using the following formula: $\frac{1}{\det(M_n)}[s_4^n C_2^n - s_5^n d_2^n - s_6^n l_2^n] \to p_5^n, n = 1,2,\dots,8$

***Received**: 05-01-2026 - **Accepted**: 04-03-2026 - **Published**: 11-03-2026*

$$p_5^1 = \frac{1}{\det(M_1)}[s_4^1 C_2^1 - s_5^1 d_2^1 - s_6^1 l_2^1] = -114,\ \ p_5^2 = \frac{1}{\det(M_2)}[s_4^2 C_2^2 - s_5^2 d_2^2 - s_6^2 l_2^2] = 3634,$$
$$p_5^3 = \frac{1}{\det(M_3)}[s_4^3 C_2^3 - s_5^3 d_2^3 - s_6^3 l_2^3] = 216,\ \ p_5^4 = \frac{1}{\det(M_4)}[s_4^4 C_2^4 - s_5^4 d_2^4 - s_6^4 l_2^4] = 198,$$
$$p_5^5 = \frac{1}{\det(M_5)}[s_4^5 C_2^5 - s_5^5 d_2^5 - s_6^5 l_2^5] = -2184,\ \ p_5^6 = \frac{1}{\det(M_6)}[s_4^6 C_2^6 - s_5^6 d_2^6 - s_6^6 l_2^6] = -1496,$$
$$p_5^7 = \frac{1}{\det(M_7)}[s_4^7 C_2^7 - s_5^7 d_2^7 - s_6^7 l_2^7] = 3692,\ \ p_5^8 = \frac{1}{\det(M_8)}[s_4^8 C_2^8 - s_5^8 d_2^8 - s_6^8 l_2^8] = -3333.$$

The same idea, to find the elements $p_6^1, p_6^2, p_6^3, p_6^4, p_6^5, p_6^6, p_6^7, p_6^8$ we substitute into the following formula: $\frac{1}{\det(M_n)}[s_7^n C_2^n - s_8^n d_2^n - s_9^n l_2^n] \to p_6^n, n = 1,2, \dots, 8,$

$$p_6^1 = \frac{1}{\det(M_1)}[s_7^1 C_2^1 - s_8^1 d_2^1 - s_9^1 l_2^1] = -39,\ \ p_6^2 = \frac{1}{\det(M_2)}[s_7^2 C_2^2 - s_8^2 d_2^2 - s_9^2 l_2^2] = 3266,$$
$$p_6^3 = \frac{1}{\det(M_3)}[s_7^3 C_2^3 - s_8^3 d_2^3 - s_9^3 l_2^3] = -3768,\ \ p_6^4 = \frac{1}{\det(M_4)}[s_7^4 C_2^4 - s_8^4 d_2^4 - s_9^4 l_2^4] = 558,$$
$$p_6^5 = \frac{1}{\det(M_5)}[s_7^5 C_2^5 - s_5^5 d_2^5 - s_9^5 l_2^5] = -4752,\ \ p_6^6 = \frac{1}{\det(M_6)}[s_7^6 C_2^6 - s_8^6 d_2^6 - s_9^6 l_2^6] = -2530,$$
$$p_6^7 = \frac{1}{\det(M_7)}[s_7^7 C_2^7 - s_8^7 d_2^7 - s_9^7 l_2^7] = 5265,\ \ p_6^8 = \frac{1}{\det(M_8)}[s_7^8 C_2^8 - s_8^8 d_2^8 - s_9^8 l_2^8] = 528.$$

Similarly, the elements $p_7^1, p_7^2, p_7^3, p_7^4, p_7^5, p_7^6, p_7^7, p_7^8$ are obtained by substituting $n = 1,2, \dots, 8$, into the following formula: $\frac{1}{\det(M_n)}[s_1^n C_3^n - s_2^n d_3^n - s_3^n l_3^n] \to p_7^n,$

$$p_7^1 = \frac{1}{\det(M_1)}[s_1^1 C_3^1 - s_2^1 d_3^1 - s_3^1 l_3^1] = -309,\ \ p_7^2 = \frac{1}{\det(M_2)}[s_1^2 C_3^2 - s_2^2 d_3^2 - s_3^2 l_3^2] = -2668,$$
$$p_7^3 = \frac{1}{\det(M_3)}[s_1^3 C_3^3 - s_2^3 d_3^3 - s_3^3 l_3^3] = -48,\ \ p_7^4 = \frac{1}{\det(M_4)}[s_1^4 C_3^4 - s_2^4 d_3^4 - s_3^4 l_3^4] = -5598,$$
$$p_7^5 = \frac{1}{\det(M_5)}[s_1^5 C_3^5 - s_2^5 d_3^5 - s_3^5 l_3^5] = -5184,\ \ p_7^6 = \frac{1}{\det(M_6)}[s_1^6 C_3^6 - s_2^6 d_3^6 - s_3^6 l_3^6] = -14872,$$
$$p_7^7 = \frac{1}{\det(M_7)}[s_1^7 C_3^7 - s_2^7 d_3^7 - s_3^7 l_3^7] = -3393,\ \ p_7^8 = \frac{1}{\det(M_8)}[s_1^8 C_3^8 - s_2^8 d_3^8 - s_3^8 l_3^8] = 2277.$$

Similarly, substituting $n = 1,2, \dots, 8$, into the following formula: $\frac{1}{\det(M_n)}[s_4^n C_3^n - s_5^n d_3^n - s_6^n l_3^n] \to p_8^n$ We obtain the elements $p_8^1, p_8^2, p_8^3, p_8^4, p_8^5, p_8^6, p_8^7, p_8^8$,

$$p_8^1 = \frac{1}{\det(M_1)}[s_4^1 C_3^1 - s_5^1 d_3^1 - s_6^1 l_3^1] = -393,\ \ p_8^2 = \frac{1}{\det(M_2)}[s_4^2 C_3^2 - s_5^2 d_3^2 - s_6^2 l_3^2] = 8188,$$
$$p_8^3 = \frac{1}{\det(M_3)}[s_4^3 C_3^3 - s_5^3 d_3^3 - s_6^3 l_3^3] = 792,\ \ p_8^4 = \frac{1}{\det(M_4)}[s_4^4 C_3^4 - s_5^4 d_3^4 - s_6^4 l_3^4] = -4122,$$
$$p_8^5 = \frac{1}{\det(M_5)}[s_4^5 C_3^5 - s_5^5 d_3^5 - s_6^5 l_3^5] = -4032,\ \ p_8^6 = \frac{1}{\det(M_6)}[s_4^6 C_3^6 - s_5^6 d_3^6 - s_6^6 l_3^6] = -19129,$$
$$p_8^7 = \frac{1}{\det(M_7)}[s_4^7 C_3^7 - s_5^7 d_3^7 - s_6^7 l_3^7] = -6084,\ \ p_8^8 = \frac{1}{\det(M_8)}[s_4^8 C_3^8 - s_5^8 d_3^8 - s_6^8 l_3^8] = 9207$$

Finally, we find the elements $p_9^1, p_9^2, p_9^3, p_9^4, p_9^5, p_9^6, p_9^7, p_9^8$ and by substituting $n = 1,2, \dots, 8$, into the following formula: $\frac{1}{\det(M_n)}[s_7^n C_3^n - s_8^n d_3^n - s_9^n l_3^n] \to p_9^n,$

$$p_9^1 = \frac{1}{\det(M_1)}[s_7^1 C_3^1 - s_8^1 d_3^1 - s_9^1 l_3^1] = -474,\ \ p_9^2 = \frac{1}{\det(M_2)}[s_7^2 C_3^2 - s_8^2 d_3^2 - s_9^2 l_3^2] = 920,$$
$$p_9^3 = \frac{1}{\det(M_3)}[s_7^3 C_3^3 - s_8^3 d_3^3 - s_9^3 l_3^3] = 264,\ \ p_9^4 = \frac{1}{\det(M_4)}[s_7^4 C_3^4 - s_8^4 d_3^4 - s_9^4 l_3^4] = -3726,$$
$$p_9^5 = \frac{1}{\det(M_5)}[s_7^5 C_3^5 - s_8^5 d_3^5 - s_9^5 l_3^5] = -768,\ \ p_9^6 = \frac{1}{\det(M_6)}[s_7^6 C_3^6 - s_8^6 d_3^6 - s_9^6 l_3^6] = -17732,$$
$$p_9^7 = \frac{1}{\det(M_7)}[s_7^7 C_3^7 - s_8^7 d_3^7 - s_9^7 l_3^7] = -6669,\ \ p_9^8 = \frac{1}{\det(M_8)}[s_7^8 C_3^8 - s_8^8 d_3^8 - s_9^8 l_3^8] = -792.$$

Step 4. Compute the elements, $g_1^n, g_5^n, g_9^n,\ n = 1, 2, \dots, 8$, as follows:

$$p_r^n - a_r^n \to g_h^n, \qquad r = h = t = 1, 5, 9,$$

then

Received*: 05-01-2026 -* ***Accepted****: 04-03-2026 -* ***Published****: 11-03-2026*

Table 5(a). Algebraic Recovery Table for Ciphertext Matrix Elements

$r=h=t=1$	g_1^1	g_1^2	g_1^3	g_1^4	g_1^5	g_1^6	g_1^7	g_1^8
	31	2	22	0	26	9	7	32
$r=h=t=5$	g_5^1	g_5^2	g_5^3	g_5^4	g_5^5	g_5^6	g_5^7	g_5^8
	33	0	9	21	29	10	13	32
$r=h=t=9$	g_9^1	g_9^2	g_9^3	g_9^4	g_9^5	g_9^6	g_9^7	g_9^8
	18	10	13	18	0	9	11	9

And we compute the elements, $g_2^n, g_3^n, g_4^n, g_6^n, g_7^n, g_8^n \;\; n = 1, 2, \ldots, 8$, as follows:

Table 5(b). Algebraic Recovery Table for Ciphertext Matrix Elements

$r=4, h=2$	g_2^1	g_2^2	g_2^3	g_2^4	g_2^5	g_2^6	g_2^7	g_2^8
	22	14	31	18	32	20	33	24
$r=7, h=3$	g_3^1	g_3^2	g_3^3	g_3^4	g_3^5	g_3^6	g_3^7	g_3^8
	6	27	22	2	31	0	2	0
$r=2, h=4$	g_4^1	g_4^2	g_4^3	g_4^4	g_4^5	g_4^6	g_4^7	g_4^8
	18	22	12	19	29	25	11	30
$r=8, h=6$	g_6^1	g_6^2	g_6^3	g_6^4	g_6^5	g_6^6	g_6^7	g_6^8
	25	1	18	3	18	15	9	25
$r=3, h=7$	g_7^1	g_7^2	g_7^3	g_7^4	g_7^5	g_7^6	g_7^7	g_7^8
	18	21	16	9	30	18	10	9
$r=6, h=8$	g_8^1	g_8^2	g_8^3	g_8^4	g_8^5	g_8^6	g_8^7	g_8^8
	31	9	11	1	7	25	17	9

Step 5. Construct the matrix $T = \begin{bmatrix} g_1^1 & g_2^1 & g_3^1 & g_1^2 & g_2^2 & g_3^2 & \cdots & g_1^p & g_2^p & g_3^p \\ g_4^1 & g_5^1 & g_6^1 & g_4^2 & g_5^2 & g_6^2 & \cdots & g_4^p & g_5^p & g_6^p \\ g_7^1 & g_8^1 & g_9^1 & g_7^2 & g_8^2 & g_9^2 & \cdots & g_7^p & g_8^p & g_9^p \end{bmatrix}$, so

$$T = \begin{bmatrix} 31 & 22 & 6 & 2 & 14 & 27 & 22 & 31 & 22 & 0 & 18 & 2 & 26 & 32 & 31 & 9 & 20 & 0 & 7 & 33 & 2 & 32 & 24 & 0 \\ 18 & 33 & 25 & 22 & 0 & 1 & 12 & 9 & 18 & 19 & 21 & 3 & 29 & 29 & 18 & 25 & 10 & 15 & 11 & 13 & 9 & 30 & 32 & 25 \\ 18 & 31 & 18 & 21 & 9 & 10 & 16 & 11 & 13 & 9 & 1 & 18 & 30 & 7 & 0 & 18 & 25 & 9 & 10 & 17 & 11 & 9 & 9 & 9 \end{bmatrix},$$

therefore,

$$T = \begin{bmatrix} N & E & X & T & - & G & E & N & E & R & A & T & I & O & N & \theta & C & R & Y & P & T & O & G & R \\ A & P & H & E & R & S & : & \theta & A & B & D & U & L & L & A & H & (& 1 &) & , & \theta & M & O & H \\ A & N & A & D & \theta & (& 2 &) & , & \theta & S & A & M & Y & R & A & H & \theta & (& 3 &) & \theta & \theta & \theta \end{bmatrix}.$$

Step 6. End of algorithm.

Comparative Analysis and Practical Considerations

The proposed MSA algorithm is a symmetric block cipher that operates on 3×3 matrix blocks. For each block, a distinct pair of randomly generated matrix keys is assigned, increasing structural diversity and key variability across encrypted blocks.

From a theoretical perspective, MSA can be compared with the Advanced Encryption Standard (AES), as both belong to the category of symmetric block ciphers. However, AES is based on a well-established substitution–permutation network and has undergone extensive cryptanalytic evaluation over the past two decades. In contrast, MSA relies primarily on matrix multiplication operations and element-level mathematical transformations within each block.

In terms of computational structure, MSA depends on fixed-dimension 3×3 matrix operations, resulting in a theoretically bounded per-block computational complexity. Nevertheless, practical performance metrics such as execution time, memory consumption, and resistance against established cryptanalytic attacks require experimental validation.

Therefore, the present comparison remains theoretical in nature, and comprehensive empirical evaluation is recommended before real-world deployment.

Table (6). Theoretical Comparison Between the Proposed MSA Algorithm and AES Algorithm

Feature	MSA	AES
Type	Symmetric	Symmetric
Block-based	Yes (3×3 matrices)	Yes (128-bit blocks)
Key Structure	Multiple matrix keys	Fixed-length binary key
Mathematical Basis	Matrix operations	Substitution–Permutation Network
Practical Validation	Not yet experimentally tested	Extensively tested

***Received**: 05-01-2026 - **Accepted**: 04-03-2026 - **Published**: 11-03-2026*

Computational Complexity Analysis

The MSA algorithm operates on fixed-size 3×3 matrix blocks. Each encryption step involves matrix multiplication and element-wise mathematical transformations within each block.

Matrix multiplication of two 3×3 matrices requires a constant number of arithmetic operations. Therefore, the computational cost per block can be considered constant.

If the plaintext consists of n blocks, the total computational complexity of the algorithm becomes linear with respect to the number of blocks.

Thus, the overall time complexity scales proportionally with the number of processed blocks. However, empirical benchmarking is required to determine actual runtime efficiency and memory consumption in practical implementations.

Future Work

Future research directions include:

1. Extending the algorithm to larger matrix dimensions (e.g., 4×4 or 8×8).
2. Conducting comprehensive security analysis against differential, linear, and algebraic attacks.
3. Implementing hardware-based prototypes for performance benchmarking.
4. Testing the algorithm on large real-world datasets.
5. Investigating integration with secure communication protocols.

Discussion

The proposed MSA algorithm introduces a structured block encryption framework that significantly enhances the security characteristics of classical block-based cryptosystems. By dividing the plaintext into 3×3 matrix blocks and assigning two independently generated encryption keys to each block, the algorithm increases both key diversity and encryption complexity. This block-wise independence ensures that compromising a single block does not provide meaningful information about other blocks, thereby improving resistance to cryptanalytic attacks. One of the key strengths of the proposed approach lies in the element-level encryption within each block. Encrypting each element individually using a combined mechanism based on two keys introduces a high degree of diffusion and confusion, which are fundamental requirements for secure cryptographic systems. Unlike conventional block encryption schemes that rely on a single key structure, the MSA algorithm employs dynamically generated key pairs, making statistical analysis and pattern recognition considerably more difficult. Another important aspect of the MSA algorithm is the asymmetric structure between encryption and decryption keys. While encryption is performed using 3×3 key matrices, decryption relies on mathematically derived 2×2 matrices with randomized permutations of key elements. This structural mismatch further strengthens the security of the system by preventing direct inversion or straightforward reconstruction of the encryption keys. The use of indirect key generation and controlled randomness enhances protection against brute-force and algebraic attacks. Moreover, the dynamic character encoding mechanism, which depends on the number of blocks rather than a fixed mapping, adds an additional layer of unpredictability. This feature ensures that the same character may be represented differently across different encryption instances, even when the plaintext content is similar. Such variability contributes to improved robustness against known-plaintext and chosen-plaintext attacks. Overall, the discussion demonstrates that the proposed MSA block encryption scheme achieves a strong balance between structural simplicity and cryptographic strength. Its modular design allows scalability with respect to the number of blocks, while maintaining a high level of security suitable for protecting sensitive data in modern information systems.

Conclusion

This paper presented a novel block encryption and decryption algorithm, referred to as the MSA algorithm, which is based on partitioning plaintext into matrix blocks and encrypting each block independently using dynamically generated key pairs. The proposed approach employs 3×3 block matrices for encryption and utilizes mathematically derived 2×2 matrices for decryption, introducing a structural distinction that enhances overall system security. By encrypting each element within a block individually through complex mathematical operations, the MSA algorithm achieves a high level of diffusion and confusion, making cryptanalysis significantly more challenging. The dependence of both key generation and character encoding on the number of blocks further increases randomness and reduces vulnerability to traditional attack models. The results indicate that the proposed block-based MSA scheme provides effective protection for sensitive information while maintaining flexibility and scalability. Compared to many conventional block encryption techniques, the algorithm demonstrates improved resistance to cryptanalytic attacks due to its multi-key structure, indirect key generation process, and dynamic encoding strategy. Future work may focus on performance evaluation, implementation optimization, and comparative analysis with standard block ciphers under different attack scenarios. The MSA algorithm offers a promising foundation for further research in block-based cryptographic systems and secure data transmission.

***Received**: 05-01-2026 - **Accepted**: 04-03-2026 - **Published**: 11-03-2026*

References

1. Aljalali O. A, Altirban A. A, Abu Irzayzah S. M, El Bolati T. A. A Novel Approach to Algorithmic Encoding and Decoding by Tribonacci Matrices, Iraqi Journal of Science, 2026, Vol. 67, No. 1, pp: 365-378. DOI: https://doi.org/10.24996/ijs.2026.67.1.30
2. Zeriouh M, Chillali A, Boua A. Cryptography based on the matrices, Bol. Soc. Parana. Mat. 37 (2019), no. 3, 75–83. doi:10.5269/bspm.v37i3.34542
3. Kannan J, Somanath M, Mahalakshmi M, Raja K. Encryption Decryption Algorithm Using Solutions of Pell Equation, International Journal of Mathematics and its Applications, 10(1) (2022), 1–8.
4. Kumari M, Tanti J. A public key cryptography using multinacci block matrices.
5. Prasad, K.; Mahato, H. Cryptography using generalized Fibonacci matrices with Affine-Hill cipher, Discrete Mathematical Sciences and Cryptography, 2022, 25, 2341–2352
6. Durcheva M, Danilchenko K. Secure Key Exchange in Tropical Cryptography: Leveraging Efficiency with Advanced Block Matrix Protocols, Mathematics 2024, 12, 1429. https://doi.org/10.3390/math12101429
7. Kannan J, Mahalakshmi M, Deepshika A. Cryptographic Algorithm involving the Matrix Q^{p*}, Korean J. Math., 30(3)(2022), 533-538. https://doi.org/10.11568/kjm.2022.30.3.533
8. Rodtes K, Anwar M. F. Permanents of block matrices, Linear Algebra and its Applications, Volume 698, 1 October 2024, pages 94-101.
9. Abu Irzayzah S, Aljalali O, Altirban A, Arebi R. SOA Algorithm for Secure Data Encryption and Decryption: A New Random Key-Based Encryption Method, Alqalam Journal of Medical and Applied Sciences. 2025; 8(3):1864-1871.
10. Tas N, Ucar S, and Ozgur N.Y. Pell coding and pell decoding methods with some applications. arXiv preprint arXiv:1706.04377. 2017.
11. Ucar S, N. Tas N, Ozgur N. Y. A New Application to Coding Theory via Fibonacci and Lucas Numbers, Mathematical Sciences and Applications E-Notes, 7 (1) (2019), 62-70.
12. Singh, G. A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 2013;67(19).
13. Kumari M, Tanti J. Cryptography using multinacci block matrices, Int. J. Nonlinear Anal. Appl. 14 (2023) 10, 57–65.
14. Koshy T. Elementary Number Theory with Applications, Academic Press, 2nd edition, Burlington, MA, 2007.

Received*: 05-01-2026 -* ***Accepted****: 04-03-2026 -* ***Published****: 11-03-2026*