APPLICATION OF SKEW CIRCULANT MATRICES IN CRYPTOGRAPHY

Vesna Simović[1]*,
[0009-0005-7388-1798]

Biljana Radičić[2]
[0000-0003-1072-2878]

[1]Student,
Academy of Applied Studies of Kosovo and Metohija,
Leposavić, Serbia

[2]Singidunum University,
Belgrade, Serbia

Abstract:

Skew circulant matrices are matrices that belong to the class of Toeplitz (or diagonal-constant) matrices. These matrices play an important role in many areas such as signal and image processing, probability, statistics, numerical analysis, economics, cryptography, coding theory, and engineering models. In this paper, we present the application of skew circulant matrices in cryptography. A public-key cryptosystem based on skew circulant matrices is proposed and illustrated by an example.

Keywords:

Skew Circulant Matrix, Cryptography, Encryption, Decryption, Algorithm.

INTRODUCTION

Suppose that q is any prime number and F_q is the field of the integers modulo a prime number q. The set of all n×n matrices over the field F_q we denote by $M_n(F_q)$. Let $C \in M_n(F_q)$. By $C_i\rightarrow$ we denote the ith row (i=1,…,n) of C. The main topic of this manuscript is skew circulant matrices and their application in cryptography. First, we define circulant matrices.

Definition 1. (*A circulant matrix*) A circulant matrix with the first row (c_0, c_1, c_2,⋯,c_{n-1}) is a square matrix satisfying the following conditions:

$$c_{i,j} = \begin{cases} c_{j-i} & i \le j \\ c_{n+j-i} & \text{otherwise} \end{cases} \tag{1}$$

i.e., a square matrix having the following form:

$$\begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-2} & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \cdots & c_{n-3} & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \cdots & c_{n-4} & c_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ c_2 & c_3 & c_4 & \cdots & c_0 & c_1 \\ c_1 & c_2 & c_3 & \cdots & c_{n-1} & c_0 \end{bmatrix}. \tag{2}$$

If the elements of a circulant matrix below the main diagonal are multiplied by -1, then such a matrix is called a skew circulant matrix. Namely,

Correspondence:
Vesna Simović

e-mail:
vesna.simovic@akademijakm.edu.rs

DOI: 10.15308/Sinteza-2026-329-333

Definition 2. (*A skew circulant matrix*) A skew circulant matrix with the first row $(c_0, c_1, c_2, \cdots, c_{n-1})$ is a square matrix satisfying the following conditions:

$$c_{i,j} = \begin{cases} c_{j-i} & i \le j \\ -c_{n+j-i} & \text{otherwise} \end{cases} \tag{3}$$

i.e., a square matrix having the following form:

$$\begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-2} & c_{n-1} \\ -c_{n-1} & c_0 & c_1 & \cdots & c_{n-3} & c_{n-2} \\ -c_{n-2} & -c_{n-1} & c_0 & \cdots & c_{n-4} & c_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ -c_2 & -c_3 & -c_4 & \cdots & c_0 & c_1 \\ -c_1 & -c_2 & -c_3 & \cdots & -c_{n-1} & c_0 \end{bmatrix}. \tag{4}$$

A skew circulant matrix is completely determined by its first row. If C is a skew circulant matrix with the first row $(c_0, c_1, c_2, \cdots, c_{n-1})$, we shall write $C = circ_n \{(c_0, c_1, c_2, \cdots, c_{n-1})_{-1}\}$. The set of all $n \times n$ skew circulant matrices over the field F_q will be denoted by $M_{n,-1}(F_q)$. Signal and image processing, probability, statistics, numerical analysis, economy, cryptography, coding theory, and engineering models are some of the areas where these matrices have a wide range of applications (see [1], [2], [3], [4], and [5]). In this paper, we shall present the application of skew circulant matrices in cryptography. Based on the fact "*the multiplication of circulant matrices is commutative*" (see [6]) and the following lemma

Lemma 1. (Lemma 3. [7]) Let A be any complex matrix (of order n), w is any n^{th} root of -1, and W is a diagonal matrix (of order n) such that w^i, $i = 0, \cdots, n-1$, are elements of its main diagonal. Then, A is a skew circulant matrix if and only if $A = WCW^{-1}$, for some circulant matrix C, the fact

"The multiplication of skew circulant matrices is commutative" (5)

can be easily proven.

Before we present the application of skew circulant matrices in cryptography, let us recall that there are two types of cryptography:

1) *Symmetric key cryptography* (or Secret key cryptography) – **SKC** – primary method of encryption, known as *single-key encryption* because the same keys are used for data encryption and decryption;

where $E(P,K)$ is encryption algorithm and $D(C,K)$ is decryption algorithm (see Figure 1).

By taking a closer look at symmetric cryptographic algorithms, we can notice their division into: algorithms that encrypt data streams - cipher stream, and algorithms that encrypt data in blocks - block ciphers. Algorithms that work with stream ciphers are: RC4, SEAL (The Simple Encryption Algorithm), ..., while those that encrypt data in blocks are: DES (Data Encryption Standard), 3DES (Triple DES), AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish, RC6, Serpent, Twofish, TEA (Tiny Encryption Algorithm), CAST (Carlisle Adams and Stafford Tavares), RC2, …

2) *Asymmetric key cryptography* (or Public key cryptography) – **PKC** - introduced in the 1970s, uses two keys, i.e., the key pairs (a public key and a private key). The public key is used for encryption, and the private key is used for decryption. These keys are mathematically related, but it is practically impossible to calculate the private key from the public key (see Figure 2). Some of the most well-known asymmetric algorithms are: RSA (Rivest-Shamir-Adleman), DH (Diffie-Hellman), ECC (Elliptic Curve Cryptography), ...

Each of these algorithms has its own characteristics, advantages, and disadvantages; they process data at different speeds and are more or less resistant to attacks. Their more detailed analysis is given in the following papers [8], [9], [10], [11], and [12].

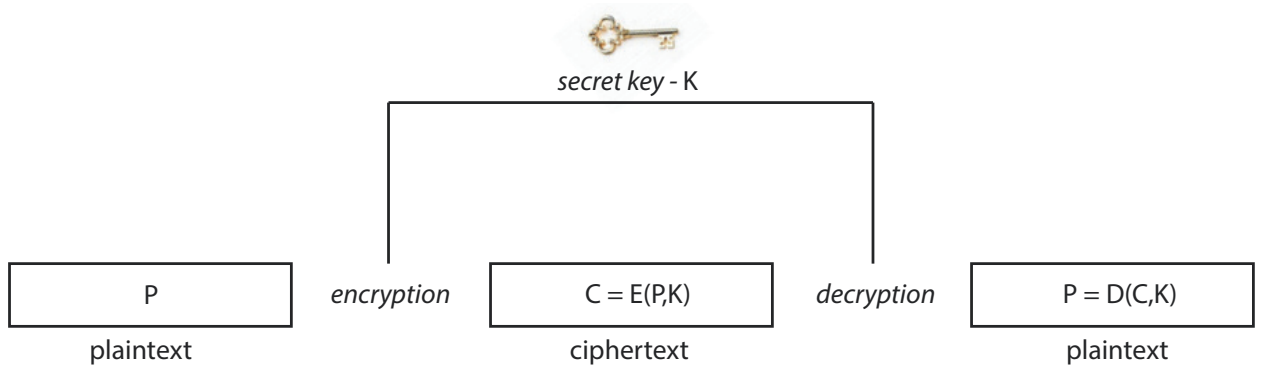

Figure 1. Scheme of symmetric key cryptography

where $E(P,K_E)$ is encryption algorithm and $D(C,K_D)$ is decryption algorithm (see Figure 2).

In the next section, we shall present a public key cryptosystem based on skew circulant matrices.

2. A PUBLIC KEY CRYPTOSYSTEM BASED ON SKEW CIRCULANT MATRICES

Suppose that Alice and Bob want to exchange a message of length $m \in N$ (i.e., a message that has m characters). They choose $a, b \in Z$ and the matrix $Q \in M_n(F_q)$, where $n \in \mathcal{N}$ satisfies the following condition: $m = n^2$ or $(n\text{-}1)^2 < m < n^2$.

Alice selects an invertible matrix $P \in M_{n,-1}(F_q)$ such that $PQ \neq QP$, computes

$$\mathrm{p} = \mathrm{P}^{\mathrm{a}}\mathrm{Q}\mathrm{P}^{\mathrm{b}}, \tag{6}$$

and sends the obtained result p to Bob.

Bob selects an invertible matrix $R \in M_{n,-1}(F_q)$ such that RQ≠QR, computes

$$\mathrm{r} = \mathrm{R}^{\mathrm{a}}\mathrm{Q}\mathrm{R}^{\mathrm{b}}, \tag{7}$$

and sends the obtained result r to Alice.

After exchanging the obtained results, Alice computes $K_1 = P^arP^b$, and Bob computes $K_2 = R^apR^b$.

Since the multiplication of skew circulant matrices is commutative, it follows

$$\mathrm{K}_1 = \mathrm{P}^{\mathrm{a}}\mathrm{r}\mathrm{P}^{\mathrm{b}} = \mathrm{P}^{\mathrm{a}}\mathrm{R}^{\mathrm{a}}\mathrm{Q}\mathrm{R}^{\mathrm{b}}\mathrm{P}^{\mathrm{b}} = \mathrm{R}^{\mathrm{a}}\mathrm{P}^{\mathrm{a}}\mathrm{Q}\mathrm{P}^{\mathrm{b}}\mathrm{R}^{\mathrm{b}} = \mathrm{R}^{\mathrm{a}}\mathrm{p}\mathrm{R}^{\mathrm{b}} = \mathrm{K}_2 \tag{8}$$

i.e., ***both parties share the same common key***.

In this paper, q will be equal to 29. Suppose that Alice and Bob want to send a message of length 13 (i.e., a message that has 13 characters). Since $3^2 < 13 < 4^2$, they choose $n = 4$ i.e. the matrix

$$\mathrm{Q} = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 1 & 3 & 2 & 1 \\ 0 & 2 & 3 & 0 \\ 1 & 2 & 2 & 1 \end{bmatrix}, \tag{9}$$

and $a = 3$, $b = 2$.

1. Alice selects the invertible matrix $P = circ_4\{(2,1,3,1)_{-1}\}$ and checks the condition $PQ \neq QP$. Since,

$$\mathrm{PQ} = \begin{bmatrix} 4 & 11 & 15 & 6 \\ 4 & 14 & 12 & 3 \\ 26 & 3 & 3 & 23 \\ 27 & 22 & 23 & 26 \end{bmatrix} \quad \text{and} \quad \mathrm{QP} = \begin{bmatrix} 26 & 23 & 3 & 6 \\ 21 & 2 & 9 & 14 \\ 18 & 1 & 8 & 9 \\ 22 & 0 & 8 & 11 \end{bmatrix}. \tag{10}$$

The condition PQ ≠ QP is satisfied. Next, Alice calculates $p = P^3QP^2$, gets

$$\mathrm{p} = \begin{bmatrix} 3 & 21 & 24 & 15 \\ 11 & 26 & 14 & 26 \\ 16 & 17 & 11 & 5 \\ 28 & 28 & 11 & 3 \end{bmatrix} \tag{11}$$

and sends the obtained result p to Bob.

2. Bob chooses the invertible matrix $R = circ_3\{(1,2,1,2)_{-1}\}$ and checks the condition $RQ \neq QR$. Since,

$$\mathrm{RQ} = \begin{bmatrix} 5 & 12 & 12 & 6 \\ 0 & 9 & 8 & 27 \\ 28 & 0 & 2 & 27 \\ 27 & 24 & 21 & 25 \end{bmatrix} \quad \text{and} \quad \mathrm{QR} = \begin{bmatrix} 25 & 27 & 27 & 6 \\ 20 & 0 & 7 & 10 \\ 22 & 25 & 7 & 8 \\ 22 & 28 & 5 & 9 \end{bmatrix}. \tag{12}$$

The condition $RQ \neq QR$ is satisfied. Next, Bob calculates $r = R^3QR^2$, gets

$$\mathrm{r} = \begin{bmatrix} 8 & 10 & 6 & 23 \\ 11 & 12 & 16 & 18 \\ 6 & 23 & 1 & 9 \\ 3 & 15 & 14 & 23 \end{bmatrix} \tag{13}$$

and sends the obtained result r to Alice.

3. Alice calculates $K_1 = P^3rP^2$ and Bob calculates $K_2 = R^3pR^2$. They get

$$\mathrm{P}^3\mathrm{r}\mathrm{P}^2 = \mathrm{R}^3\mathrm{p}\mathrm{R}^2 = \begin{bmatrix} 21 & 27 & 10 & 6 \\ 9 & 25 & 3 & 15 \\ 8 & 28 & 6 & 3 \\ 3 & 24 & 6 & 17 \end{bmatrix} = \mathrm{K}_{1,2} \tag{14}$$

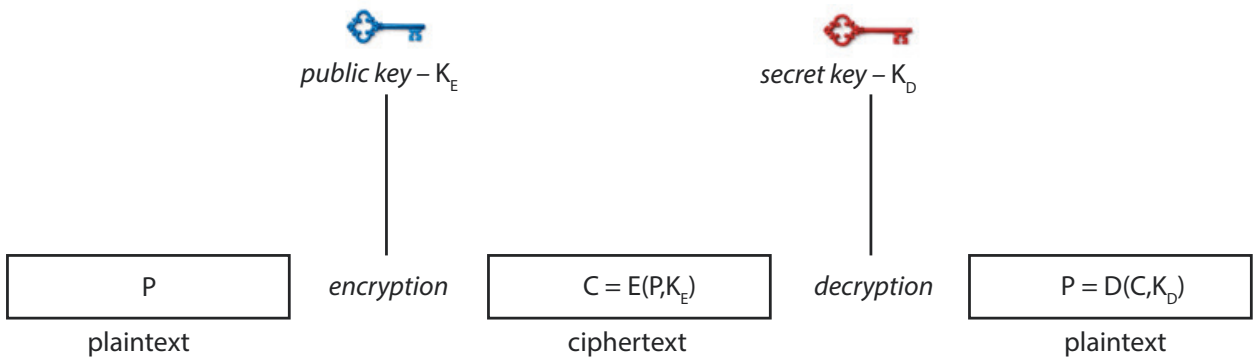

Figure 2. Scheme of asymmetric key cryptography

Before we give the example, let us emphasize that the following table will be used for each letter of the English alphabet, the period (.), the question mark (?), and the blank space ␣.

Example 1. The secret message is: „SINTEZA XIII."

Matrix $K_{1,2} \in M_4(F_{29})$ and Alice form a plaintext $P_1 \in M_4(F_{29})$ using the Hill Cipher algorithm. Therefore, using the Hill Cipher algorithm, Alice gets that $P_1 \in M_4(F_{29})$ has the following form:

$$P_1 = \begin{bmatrix} 19 & 9 & 14 & 20 \\ 5 & 26 & 1 & 0 \\ 24 & 9 & 9 & 9 \\ 27 & 0 & 0 & 0 \end{bmatrix}. \quad (15)$$

Encryption. Using P_1 Alice gets gets the ciphertext $C(P_1)$ such that

$$C(P_1) = K_{1,2} + P_1 = \begin{bmatrix} 21 & 27 & 10 & 6 \\ 9 & 25 & 3 & 15 \\ 8 & 28 & 6 & 3 \\ 3 & 24 & 6 & 17 \end{bmatrix} + \begin{bmatrix} 19 & 9 & 14 & 20 \\ 5 & 26 & 1 & 0 \\ 24 & 9 & 9 & 9 \\ 27 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 11 & 7 & 24 & 26 \\ 14 & 22 & 4 & 15 \\ 3 & 8 & 15 & 12 \\ 1 & 24 & 6 & 17 \end{bmatrix} \quad (16)$$

and sends the obtained ciphertext $C(P_1)$ to Bob.

Decryption. After receiving the ciphertext (P_1), Bob calculates $D(C) = C(P_1) - K_{1,2}$ and gets

$$D(C) = C(P_1) - K_{1,2} = \begin{bmatrix} 11 & 7 & 24 & 26 \\ 14 & 22 & 4 & 15 \\ 3 & 8 & 15 & 12 \\ 1 & 24 & 6 & 17 \end{bmatrix} - \begin{bmatrix} 21 & 27 & 10 & 6 \\ 9 & 25 & 3 & 15 \\ 8 & 28 & 6 & 3 \\ 3 & 24 & 6 & 17 \end{bmatrix} = \begin{bmatrix} 19 & 9 & 14 & 20 \\ 5 & 26 & 1 & 0 \\ 24 & 9 & 9 & 9 \\ 27 & 0 & 0 & 0 \end{bmatrix}. \quad (17)$$

Using the Hill Cipher algorithm, Bob gets the message „SINTEZA XIII.".

What should be emphasized is that the previously described procedure can be interpreted as a key exchange protocol based on skew circulant matrices, inspired by the Diffie–Hellman algorithm (Figure 3). The essence of the Diffie–Hellman algorithm is reflected in the ability of each party to generate a pair of keys and send its public key to the other party, based on which both parties independently derive a secret key. This secret key is identical (shared) for both parties and is subsequently used within symmetric encryption algorithms (see [13], [14], [15], and [16]). Note that Diffie–Hellman's protocol mathematically calculates the secret data as an exponential value in a cyclic group, and that the protocol presented here, based on skew circulant matrices, provides an analogy with exponentiation and multiplication of matrices in matrix algebra. It is also necessary to indicate the papers in which the authors presented the protocol based on Polynomial Symmetrical Decomposition (PSD) (see [17]) and the protocol based on circulant matrices (see [18]).

The main purpose of the procedure presented here is to enable two parties to establish a shared matrix $K_{1,2}$ even when communicating over an insecure channel.

Table 1. The Hill Cipher algorithm

the symbol	is represented by
A	1
B	2
⋮	⋮
Z	26
.	27
?	28
␣	0

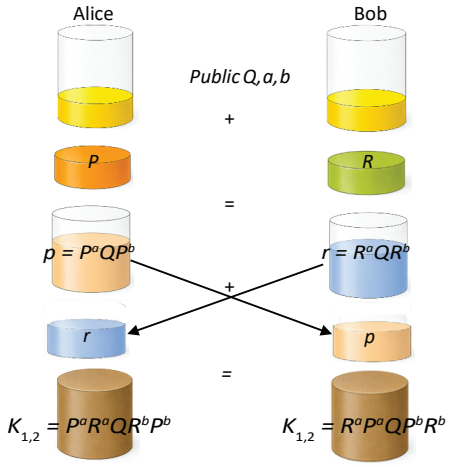

Figure 3. Scheme of the Diffie–Hellman algorithm applied to skew circulant matrices

Once the shared secret key $K_{1,2}$ is obtained, it is used in a second phase for secure message transmission. Specifically, since the message is represented as a matrix P_1, encryption is performed in a straightforward manner by computing $C(P_1) = K_{1,2} + P_1$, while decryption is achieved by subtracting the key $D(C) = C(P_1) - K_{1,2}$. We observe that this second step does not constitute an independent public-key cryptographic scheme, but rather a symmetric phase that naturally follows the key exchange process.

3. CONCLUSION

In this paper, we presented the application of skew circulant matrices in cryptography, proposing a public key cryptosystem based on these matrices. Specifically, we compared the proposed procedure with the Diffie–Hellman algorithm, which is one of the fundamental algorithms in asymmetric cryptography. The underlying mathematically hard problem that forms the core of this procedure is the computation of the shared secret key.

$K_{1,2} = P^a R^a Q R^b P^b = R^a P^a Q P^b R^b$ from publicly shared data Q, a, b. A complete complexity analysis of this problem and its impact on the security of the algorithm remains an open issue for future work. In essence, this approach provides a foundation for further research into matrix-based cryptographic constructions.

REFERENCES

[1] K. A. Reddy, B. Vishnuvardhan, M. Madhuviswanatham, and A. V. N. Krishna, "A modified Hill cipher based on circulant matrices" *Procedia Technol.*, vol. 4, pp. 114–118, 2012. doi: 10.1016/j.protcy.2012.05.017

[2] S. Al-Homidan, "Stabilizing circulant matrix in modeling of mechanical structures vibration using the interior point methods," *Arab. J. Sci. Eng.*, vol. 47, pp. 16523–16532, 2022.

[3] G. Zhao, "The inverse problem of anti-circulant matrices in signal processing," in *Proc. Pacific-Asia Conf. Knowl. Eng. Softw. Eng.*, pp. 47–50, 2009.

[4] E. J. Hannan, Time Series Analysis. London, U.K.: Methuen, 1960.

[5] S. Pollock, "Circulant matrices and time-series analysis," *Int. J. Math. Educ. Sci. Technol.*, vol. 33, no. 2, pp. 213–230, 2002.

[6] P. J. Davis, Circulant Matrices. Providence, RI, USA: AMS Chelsea, 1994.

[7] R. E. Cline, R. J. Plemmons, and G. Worm, Generalized Inverses of Certain Toeplitz Matrices, *Linear Algebra Appl.* 8(1) (1974), 25-33. doi: 10.1016/0024-3795(74)90013-9

[8] M. A. Qadir and N. Varol, "A review paper on cryptography," in *Proc. Int. Symp. Digit. Forensic Secur. (ISDFS)*, 2019. doi: 10.1109/ISDFS.2019.8757514

[9] A. Gupta and N. Kaur Walia, "Cryptography algorithms: A review," *Int. J. Eng. Develop. Res.*, vol. 2, no. 2, pp. 1666–1672, 2014.

[10] B. E. H. H. Hamouda, "Comparative study of different cryptographic algorithms," *J. Inf. Secur.*, vol. 11, no. 3, pp. 138–148, 2020.

[11] B. Nithya and P. Sripriya, "A review of cryptographic algorithms in network security," *Int. J. Eng. Technol. (IJET)*, vol. 8, no. 1, pp. 324–331, 2016.

[12] S. Tayal, N. Gupta, P. Gupta, D. Goyal, and M. Goyal, "A review paper on network security and cryptography," *Adv. Comput. Sci. Technol.*, vol. 10, no. 5, pp. 763–770, 2017.

[13] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976. doi: 10.1109/TIT.1976.1055638

[14 N. Li, "Research on Diffie–Hellman key exchange protocol," in *Proc. 2nd Int. Conf. Comput. Eng. Technol.*, vol. 4, pp. V4-634, Apr. 2010.

[15] A. S. Rawat and M. Deshmukh, "Efficient extended Diffie–Hellman key exchange protocol," in *Proc. Int. Conf. Comput., Power Commun. Technol. (GUCON)*, pp. 447–451, Sep. 2019.

[16] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 3rd ed. Boca Raton, FL, USA: CRC Press, 2020.

[17] L. Jinhui, Z. Huanguo, and J. Jianwei, "Cryptanalysis of Schemes Based on Polynomial Symmetrical Decomposition," *Chinese J Electronics*, vol. 26, no. 6, pp. 1139–1146, 2017. doi: 10.1049/cje.2017.09.006

[18] M. Maxrizal, I G. N. Y. Hartawan, P. Jana, and B. D. A. Prayanti, "Modified Public Key Cryptosystem Based On Circulant Matrix," in *Int. Conf. Math Nat. Sci.*, 2019 (IConMNS 2019).