Journal of Engineering Technology and Applied Sciences, 2025 *e-ISSN:* 2548-0391
Received 15 July 2024, Accepted 25 February 2025 *Vol. 10, No. 1, 21-27*
Published online 29 April 2025, Research Article *doi: 10.30931/jetas.1516337*

Citation: Dalkılıç, Ş., Kepekçi, A.E., Baştürk, M.Z., "Hill Cipher with r-Circulant Matrices". Journal of Engineering Technology and Applied Sciences 10 (1) 2025 : 21-27.

HILL CIPHER WITH R-CIRCULANT MATRICES[1]

Şeyda Dalkılıç[a]*, Ahmet Eren Kepekçi[b], Muhammed Zekeriya Baştürk[b]

[a*]*Ministry of National Education, Kilis, Turkey (*corresponding author)*
seyda468@gmail.com

[b]*Ministry of National Education, Kilis, Turkey*
aerenk7777@hotmail.com, zekeriya.basturkk@gmail.com

Abstract

The Hill cipher, a historic symmetric encryption method, has limitations in contemporary cryptography. This study explores enhancing its security by incorporating r-circulant matrices. Existing literature employs circulant matrices within the Hill cipher. In this study we propose a novel encryption algorithm that employs r-circulant matrices with the objective of increasing the algorithm's complexity and resistance to cryptanalysis. The developed algorithm demonstrably achieves a more secure and intricate encryption process which is supported by comparisons and numerical data. Once the algorithm has been identified, it is translated into a computer code and implemented as a program in the Python software language.

Keywords: Hill cipher, r −circulant matrices, cryptology, algorithm

1. Introduction

The Hill cipher, a foundational technique in classical cryptography, employs matrices and modular arithmetic to facilitate secure communication. In 1929, Lester S. Hill introduced a method that established the foundation for modern encryption techniques [1]. This article examines the fundamental principles of Hill encryption and considers potential avenues for enhancement through the utilization of r-circulant matrices. We commence by analyzing the original Hill cipher, wherein messages are partitioned into blocks and subjected to a linear transformation governed by a square matrix key. The aforementioned key matrix, in conjunction with the application of modular arithmetic operations, serves to encrypt the message. In order to decrypt, an invertible key matrix is required. Hill himself proposed enhancements to his invention. It is noteworthy that he introduced the concept of an additive

[1] This study was presented at the 11th International Congress of Fundamental and Applied Sciences (ICFAS) in 2024.

key component, thereby enhancing the overall security of the system [2]. Furthermore, the article examines the use of involutive keys, which allow decryption with the same key used for encryption; however, this restricts the range of available key selection options [3] [4].

The article will also investigate various strategies for enhancing the security of the Hill cipher. These advancements encompass alternative key generation methods, the generation of multiple ciphertexts for a single message, and the utilization of special key structures like Maximum Distance Separable (MDS) codes and self-invertible matrices [5, 6, 7, 8, 9]. The central focus of this article is the potential of r-circulant matrices to enhance the reliability of Hill encryption. This study differs from the work of Reddy et al. [9] in that it considers the use of r-circulant matrices as key components.

A review of the extant literature on the Hill Cipher reveals three principal categories of research: integration into applications of daily life, use in image encryption, and studies aimed at improving the algorithm. Haouri et al. presented an image processing algorithm that employs the traditional Hill encryption method [10].Wen et al. presented the simulation cipher time, chosen plaintext attack and chosen ciphertext attack results for the VCH-CHES algorithm [11].

A novel approach to digital image security has been proposed, which entails the integration of Hill and Advanced Encryption Standard (AES) encryption algorithms [13]. Similarly, chaotic maps were employed in the construction of Hill matrices and utilized for image encryption purposes [14]. Handoku et al. introduced a three-layer encryption algorithm by combining Hill encryption and other encryption algorithms [15]. Salman et al. proposed a novel algorithmic approach based on Gaussian integers for enhancing data security in a banking system [16]. Sitepu et al. demonstrated the efficacy of their developed super-encryption algorithm in securing employee salaries [17]. While Sujorwu [18] was working on key selection in $m \times m$ matrices in the Hill cipher, Nauro et al. [19] were writing Python codes for The Hill 2 cipher.

The primary objective of this study is to assess the impact of these matrices on the robustness of the Hill cipher encryption algorithm. In order to embark on this exploration, it is essential to have a firm grasp of the underlying concepts. The article will subsequently define the necessary terms and present the fundamental principles before delving into the specifics of r-circulant matrices and their application within the Hill cipher framework.

2. Preliminaries

Definition 2.1 A circulant matrix of order n is a $n \times n$ matrix of the following form:

$$C = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & \cdots & a_0 \end{pmatrix}$$

This is the matrix obtained by shifting the base row $(a_0, a_1 \, \dots \, , \, a_{n-1})$ by one column in each row. Consequently, all circulant matrices can be defined by their first row or column. Thus, circulant matrices can be denoted as $C = (a_0, a_1 \, \dots \, , \, a_{n-1})$ [10].

Definition 2.2 Let r be a positive integer. An r −circulant matrix of order n is defined as

$$C_r = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ r.a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ r.a_{n-2} & r.a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r.a_1 & r.a_2 & \cdots & \cdots & a_0 \end{pmatrix}$$

This matrix is defined by its first row and the number r [11]. If $r = 1$, it will turn into a standard circulant matrix form.

3. The main result

Algorithm 3.1 (Encryption)

In the encryption algorithm we adapted with r-circulant matrices, the key consists of a word. The last letter of the key we generate will replace the r variable of our matrix. First of all

i. $A \coloneqq 0, B \coloneqq 1, \dots, Z$:=32, …, !:=37. The numbers are mapped to the combination of the Turkish alphabet and the English alphabet with the combination of UTF-8 characters and the key and plain text are converted into numbers.

ii. Let the keyword be of length $n + 1$. A circulant matrix is created with the first n characters $(a_0, a_1 \ \dots \ , \ a_{n-1})$ and $r \ = \ a_n$

iii. The following circulant matrix is created with $(a_0, a_1 \ \dots \ , \ a_{n-1})$ and $r \ = \ a_n$.
It is checked whether it is reversible. If it is non-invertible, a different key is selected.

iv. The plain text is divided into row matrices of length n. If the last part is missing, the empty parts are completed with the letter a. The letter a is preferred because it corresponds to 0 for ease of operation. Let m be the text length divided by the key length minus one. Let these row matrices be $A_1, A_2, \dots, A_m$

v. Multiply the transpositions of the r −circulant matrix and the row matrices to get the encrypted columns. The transpose is taken and written side by side. The ciphertext is ready.

Algorithm 3.2 (Decryption)

i. The first three steps are applied exactly to the ciphertext.

ii. The inverse of matrix C_r is calculated, and the resulting matrix is then $D_1, D_2, \dots, D_m$ column matrices multiplied by matrix. The matrices are then combined to form the encrypted text.

Example 3.3

The text to be encrypted is "Mathematics is Beautiful!" and the keyword is "LESTER"
In accordance with the Turkish alphabet, numbers and letters must be matched.

$$M \rightarrow 15, A \rightarrow 0, T \rightarrow 23, H \rightarrow 9, E \rightarrow 5, \dot{I} \rightarrow 11, C \rightarrow 2\ , S \rightarrow 21, B \rightarrow 1, F \rightarrow 6, U = \\ \rightarrow 24, L \rightarrow 14, G \rightarrow 7, R \rightarrow 20$$

The text is converted to the following numerical sequence: $15 - 0 - 23 - 9 - 5 - 15 - 0 - 23 - 11 - 2 - 21 - 11 - 21 - 1 - 5 - 0 - 24 - 23 - 11 - 6 - 24 - 14$

The key is converted to the following numerical sequence: $14 - 5 - 21 - 23 - 5 - 20$

$$r = 20$$

The r-circulant matrix is

$$C_r = \begin{pmatrix} 14 & 5 & 22 & 24 & 5 \\ 31 & 14 & 5 & 22 & 24 \\ 23 & 31 & 14 & 5 & 22 \\ 18 & 23 & 31 & 14 & 5 \\ 31 & 18 & 23 & 31 & 14 \end{pmatrix} \text{mod } 37$$

$A_1 = (15 \quad 0 \quad 24 \quad 9 \quad 5)$ mod 37

$A_2 = (15 \quad 0 \quad 24 \quad 11 \quad 2)$ mod 37

$A_3 = (22 \quad 11 \quad 22 \quad 1 \quad 5)$ mod 37

$A_4 = (0 \quad 25 \quad 24 \quad 11 \quad 6)$ mod 37

$A_5 = (25 \quad 14 \quad 36 \quad 0 \quad 0)$ mod 37

The column matrices are obtained by multiplying C_r by the transpose of the $A_n$matrices.

$$D_1 = \begin{pmatrix} 17 \\ 15 \\ 22 \\ 18 \\ 34 \end{pmatrix} \text{mod } 37,\ D_2 = \begin{pmatrix} 13 \\ 24 \\ 3 \\ 31 \\ 17 \end{pmatrix} \text{mod } 37,\ D_3 = \begin{pmatrix} 8 \\ 15 \\ 12 \\ 1 \\ 7 \end{pmatrix} \text{mod } 37,$$
$$D_4 = \begin{pmatrix} 22 \\ 5 \\ 3 \\ 23 \\ 21 \end{pmatrix} \text{mod } 37,\ D_5 = \begin{pmatrix} 28 \\ 4 \\ 33 \\ 1 \\ 5 \end{pmatrix} \text{mod } 37$$

The ciphertext is as follows,
omsöîktçzoğmjbgseçşrxdâbe2.

The process of decryption is analogous to that of encryption.

The Python code of the algorithm has been developed and a practical usage area has been presented. The encryption and decryption times have been calculated with the Python codes. The average encryption and decryption time for a word and a key from the Turkish alphabet is shown below (all of the tests were made with over 10^5 words).

Table 1. Average Durations

Average Durations	For three-letter keys	For four-letter keys	For five-letter keys
Avg. Encryption	0.000384 seconds	0.002 seconds	0.0028 seconds
Avg. Decryption	0.000384 seconds	0.002 seconds	0.0028 seconds
Avg. Brute-force	approx. 60 seconds	approx. 1200 seconds	approx. 14 hours

As demonstrated, the average time for a brute-force attack to break our encryption system increases significantly as the key length increases. The length of the key doesn't cause any disadvantages either, because the average time for encryption and decryption doesn't change enough to make a difference.

As illustrated in the table, the proposed method exhibits certain advantages in comparison to the classical hill cipher method.

Table 2. Comparison to the classical hill cipher method.

Cipher	Resistant towards frequency analysis	Strong against brute-force attack	Vulnerable to known plaintext attack	Vulnerable to known ciphertext attack	Decryption possibility
Original hill [6]	Yes	Yes	Yes	No Data	Sometimes
Modified Hill Cipher: A Simplified Approach [20]	Yes	Yes	No	No Data	Yes
r-circulant Hill Cipher	Yes	Yes	No	No	Sometimes

While the original Hill cipher is resistant to frequency analysis and brute-force attacks, it is vulnerable to known plaintext attacks, which refers to the ability of an attacker to compute the key matrix if he knows the ciphertext and the corresponding plaintext. While there is no data on known plaintext attacks, decryption is only possible in some cases. On the other hand, the 'Modified Hill Cipher: A Simplified Approach' is robust against frequency analysis and brute-force attacks, while it is not vulnerable to known plaintext attacks and can always be successfully decrypted. Finally, the r-circulant Hill cipher is resistant to known plaintext attacks and can only be broken in some cases, although it remains resistant to frequency analysis and brute-force attacks. These differences suggest that each method should be chosen according to security needs.

4. Conclusion and discussion

The objective of this paper is to present a novel encryption method that offers a more secure and practical alternative to the classical Hill cipher. The proposed method employs a matrix as the key and performs encryption with a specific type of matrices, designated as $r -$circulant matrices. Furthermore, the final letter variable (r) is employed in the encryption process. The proposed method offers significant advantages over classical methods, due to the innovative features that it possesses.

The presented encryption method is founded upon a robust theoretical framework. The method's distinctive features, including the utilization of matrix keys, r −circulant matrices, and the last letter variable, render it exceedingly challenging for third parties to decrypt. Furthermore, the Python implementation demonstrates the practical feasibility of the method. Moreover, the expeditious encryption and decryption capabilities of the method are regarded as a significant advantage. The performance of our method is shown in tables which includes its durability against variable attack types and the efficiency of our encryption/decryption process. It is also compared with other Hill cipher methods on this topic.Nevertheless, this approach is not without its constraints. The following limitations are identified:

As the size of the matrix keys increases, the encryption and decryption processes become slower. The number of r −circulant matrices is limited, which restricts the diversity of key selection. The fixed nature of the last letter variable (r) may contribute to the predictability of the encryption process to some extent. In light of these limitations, further development and optimization of this method are necessary in future work. The investigation of alternative key types and encryption functions could enhance the method's security and practicality.

References

[1] Hill, L., “Cryptography in an algebraic alphabet”, The American Mathematical Monthly 36(6) (1929) : 306-312.

[2] Hill, L., “Concerning certain linear transformation apparatus in cryptography”, The Mathematical Monthly 38(3) (1931) : 135-154.

[3] Christensen, C., “Review of codes, ciphers and spies: tales of military intelligence in world war i by John F. Dooley”, Cyrptologia 40(6) (2016) : 563-566.

[4] Christensen, C., “Lester Hill Revisited”, Cryptologia 38(8) (2014) : 293-332.

[5] Magamba, K., Kadaleka, S., Kasambara, A., “Variable-length hill cipher with MDS key matrix”, International Journal of Computer Applications 57(13) (2012) : 43-45.

[6] Acharya, B., Rath, G.S., Patra, S.K., Panigrahy, S.K., “Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm”, International Journal of Security (IJS) 1(1) (2007) : 14-21.

[7] Lin, C.H., Lee, C.Y., Lee, C.Y., “Comments on saeednia’s improved scheme for the hill cipher”, Journal of the Chinese Institute of Engineers 27(5) (2004) : 743-746.

[8] Mahendran, R., Mani, K., “Generation of key matrix for hill cipher encryption using classical cipher” in 2017 World Congress on Computing and Communication Technologies (WCCCT) (2017).

[9] Reddy, K.A., Vishnuvardhan, B., Krishna, A.V.N., “A modified hill cipher based on circulant matrices”, Procedia Technology 4 (2012) : 114-118.

[10] J. Davis, Circulant matrices, New York: Wiley (1979).

[11] Tuglu, N., Kızılateş, C., “On the norms of circulant and r-circulant matrices with the hyperharmonic Fibonacci numbers”, Journal of Inequalities and Applications 2015(1) (2015) : 1-11.

[12] Hraoui, S., Gmira, F., Abbou, M.F., Oulidi, A.J., Jarjar, A., “A New Cryptosystem of Color Image Using a Dynamic-Chaos Hill Cipher Algorithm”, Procedia Computer Science, (148) (2019) : 399–408.

[13] Wen, H., Lin, Y., Yang, L., Chen, R., “Cryptanalysis of an image encryption scheme using variant Hill cipher and chaos”, Expert Systems with Applications (250) (2024) : 123748.

[14] Ranti, D., Fauzi, A., Sitompul, M.P.U., “Digital Image Security Analysis using Hill Cipher and AES Algorithm”, Journal of Artificial Intelligence and Engineering Applications (JAIEA) 4(1) (2024) : 487–496.

[15] Rrghout, H., Kattass, M., Qobbi, Y., Benazzi, N., JarJar, A., Benazzi, A. “New image encryption approach using a dynamic-chaotic variant of Hill cipher in Z/4096Z”, International Journal of Electrical & Computer Engineering 14(5) (2024) : 5330-5343.

[16] Handoko, L.B., Umam, C., “A Super Encryption Approach for Enhancing Digital Security using Column Transposition - Hill Cipher for 3D Image”, Protection Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control 9(3) (2024) : 267-276.

[17] Salman, S., Mohialden, Y.M., Abdulhameed, A., Hussien, N.M., “A Novel Method for Hill Cipher Encryption and Decryption Using Gaussian Integers Implemented in Banking Systems”, Iraqi Journal For Computer Science and Mathematics 5(1) (2024) : 277-284.

[18] Sıtepu, E.B., Fauzı, A., Rahmadanı, R., “Super Encryption of the Hill Cipher Method and the AES Method for Security of Employee Salary Data”, International Journal of Informatics, Economics, Management and Science 3(1) (2024) : 29-37.

[19] Sujarwo, S. “Key analysis of the hill cipher algorithm (Study of literature)”, Jurnal Mandiri IT 2(3) (2024). 135–141.

[20] Noura A.A., Raiga A.A., Fouad S.A. “The Hill 2-Cipher with Python”, African Journal of Advanced Pure and Applied Sciences (AJAPAS) 3(1) (2024) : 58–71.

[21] Paragas, J.R., Sison, A.M., Medina, R.P., “Hill Cipher Modification: A Simplified Approach”, 2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN), Chongqing, China, (2019) : 821-825, doi: 10.1109/ICCSN.2019.8905360.