UJM 13 (2) 2024

UNNES Journal of Mathematics

http://journal.unnes.ac.id/sju/index.php/ujm

Determine the Determinant of $4 \times n$ Non-Square Matrix Using Radić's Determinant

Intan Wahyuningsih*, Kristina Wijayanti

Department of Mathematics, Faculty of Mathematics and Natural Science,
Universitas Negeri Semarang, Semarang, 50229, Indonesia

Article Info

Article History:
Received …….
Accepted …..
Published …..

Keywords:
Determinant, Non-Square Matrix, Radić's Determinant, Modified Double-Guard Hill Cipher

Abstract

A non-square matrix is a matrix that has a different number of rows and columns. In the modified double-guard Hill cipher algorithm, a non-square matrix is used as the private key matrix that plays a role in the message encryption and decryption process. Therefore, the determinant of the key matrix is needed to obtain the inverse of the key matrix. Mirko Radić defined the determinant of matrix $A_{m\times n}, m \leq n$ as the signed sum of the determinants of the $m \times m$ submatrices as many as C_m^n. Radić's determinant can be used to determine the general formula for the determinant of certain non-square matrices. The purpose of this research is to find out the determinant of matrix $R = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & a_1 & a_2 & \cdots & a_i & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}, a_i \in \mathbb{R}, \forall i = 1,2,\ldots,n-2$ where $n > 4$, using Radić's determinant and an example of its use. The result of this research are the following theorem. If a non-square matrix $R = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & a_1 & a_2 & \cdots & a_i & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}, a_i \in \mathbb{R}, \forall i = 1,2,\ldots,n-2$ where $n > 4$, then

$$|R| = \begin{cases} \sum_{i=2}^{n-2} (-1)^{i+1} a_i \ , for\ n\ odd \\ \sum_{i=2}^{n-2} (-1)^{i} a_i \, , for\ n\ even \end{cases} .$$

The use of the theorem is shown in an example problem using the modified double-guard Hill cipher where matrix R is chosen as the private key matrix. Several conditions must be met by the matrix R to be selected as the key matrix, including all elements of matrix R being positive integers, $|R| \neq 0$, and R invertible in modulo 128.

How to cite:

Wahyuningsih, I. & Wijayanti, K. 2024. Menentukan Determinan Matriks Non Persegi $4 \times n$ Menggunakan Determinan Radić. *UNNES Journal of Mathematics*. 13 (2): 29-38

*Correspondence Address
E-mail: intanwahyuningsih.iw@gmailcom

p-ISSN 2252-6943
e-ISSN 2460-5859

1. Introduction

A non-square matrix is a matrix that has a different number of rows and columns (Zaini, 2016). Let A be an $m \times n$ matrix. If $m < n$ then A called the horizontal matrix and if $m > n$ then A called the vertical matrix (Arunkumar *et al.*, 2011).

The concept of matrix can be applied in cryptography. Cryptography is the art of disguising messages so that only certain people can read them (Hardy *et al.,* 2009). To keep a message secret, an algorithm is needed. Cryptographic algorithms are mathematical functions used for encryption and decryption (Munir, 2004). Encryption is the process of encoding plaintext (the original message) into ciphertext (the original message that has been encrypted) and decryption is the process of returning ciphertext into plaintext. The modified double-guard Hill cipher is one of the cryptographic algorithms modified from the double-guard Hill cipher algorithm. The modified double-guard Hill cipher algorithm utilizes a non-square matrix as the private key matrix (Thangammal *et al.*, 2016). The key matrix must be invertible in modulo 128.

Originally, a non-square matrix does not have an inverse definition like a square matrix. However, there are non-square matrices that have a one-sided inverse, from the left side or the right side. If the inverse exists then the value is not unique (Addis, 2015). Suppose A is an mxn matrix. According to Strang (2006) if $m \leq n,\ A$ full row rank then A has a right inverse, and if $m \geq n, A$ full column rank then A has a left inverse.

Determinants are only defined for square matrix (Amiri *et al.*, 2010). However, the definition of the determinant of a square matrix can be extended so that the determinant of a non-square matrix can also be determined. One of them is introduced by Mirko Radić who defines that for a matrix then is the signed sum of the determinant of $m \times m$ submatrix as many as C_m^n (Radić, 1966). Based on this definition, Radić (1996) also defined the inverse of A. According to Abdollahi *et al.* (2015) Radić's determinant is an efficient definition of the non-square matrix because it has most of the properties in the determinant of the square matrix and has a geometric interpretation in R^2 and R^3.

Some previous research has discussed the use of Radić's determinant to determine the general formula of the determinant for certain non-square matrices. Research by Aryani & Hanita (2018) obtained the general formula of a determinant for an $3 \times n, n > 3$ non-square matrix where the matrix is

$$A_{3\times n} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & a_1 & a_2 & \cdots & a_{n-1} \\ 0 & 1 & 1 & \cdots & 1 \end{bmatrix}, a_i \in \mathbb{R}, \forall\ i = 1,2,\dots,n-1.$$

Then research by Delima (2018) obtained the general formula of a determinant for an $4 \times n, n > 4$ non-square matrix where the matrix is

$$A_{4\times n} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & a_1 & a_2 & a_3 & \cdots & a_{n-1} \\ 0 & 1 & 1 & 1 & \cdots & 1 \\ 0 & b_1 & b_2 & b_3 & \cdots & b_{n-1} \end{bmatrix}, \forall a_i, b_i \in \mathbb{R}, i = 1,2,\dots,n-1.$$

However, in these two studies, there is no explanation regarding the importance of the application of the general formula of determinant that has been obtained. In addition, the matrix can still be developed both in terms of size and elements. Therefore, the author is interested in further discussing the determinant of other certain non-square matrices using Radić's determinant and its application in cryptography.

In this research, the authors modified the matrix based on the matrix used by Delima (2018), which is matrix

$$R = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & a_1 & a_2 & \cdots & a_i & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}, a_i \in \mathbb{R}, \forall i = 1,2,\dots,n-2, \text{where } n > 4.$$

So, the interesting things that can be studied are how to determine the determinant of a non-square matrix R using Radić's determinant and an example of its use in the modified double guard Hill cipher algorithm. Therefore, the purpose of this research is to find out the general formula of the determinant of matrix

$$R = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & a_1 & a_2 & \cdots & a_i & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}, a_i \in \mathbb{R}, \forall i = 1,2,\dots,n-2 \text{ where } n > 4,$$

using Radić's determinant and an example of its use.

2. Method

The method used in this research is a literature study. Based on the studies on literature sources, the following problem-solving steps are obtained as follows: (1) Given a matrix R, it is a $4 \times n, n > 4$ non-square matrix, (2) Determine the determinant of matrix R from order 4x5 to order 4x10, (3) Deduce the general formula of the matrix determinant from its recursive pattern, (4) Proving the general formula of matrix determinant using direct proof.

The Radić's determinant by Mirko Radić is stated in Definition 1. Based on that definition, Radić also defined inverse non-square matrix stated in Definition 2.

Definition 1

If $A = (a_{ij})$ an $m \times n$ matrix with $m \leq n$, the determinant of matrix A is defined as

$$\det(A) = \sum_{j_1<\cdots<j_m} (-1)^{r+s} \begin{vmatrix} a_{1j_1} & \cdots & a_{1j_m} \\ \cdots & \cdots & \cdots \\ a_{mj_1} & \cdots & a_{mj_m} \end{vmatrix}$$

where $j_1, j_2, \dots, j_m \in \{1,2,\dots,n\}, r = 1 + 2 + \cdots + m$, and $s = j_1 + j_2 + \cdots + j_m$.

Definition 2
If $\det(A) \neq 0$ then

$$A^{-1} = \frac{1}{\det(A)} \begin{vmatrix} A_{11} & \dots & A_{m1} \\ \dots & \dots & \dots \\ A_{1n} & \dots & A_{mn} \end{vmatrix}$$

where $A_{ij} = (-1)^{i+j} \det(M_{ij}), i = 1,2,\dots,m$ and $j = 1,2,\dots,n$. The M_{ij} matrix is obtained by deleting the i-th row and j-th column from matrix A.

3. Results and Discussions

3.1. Results

3.1.1. Determine the Determinant of a $4 \times n, n > 4$ Non-Square Matrix Using Radić's Determinant

The $4 \times n, n > 4$ non-square matrix, which is to be determined the determinant is the matrix

$$R = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & a_1 & a_2 & \cdots & a_i & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}, a_i \in \mathbb{R}, \forall i = 1,2,\dots,n-2 \text{ where } n > 4.$$

By using Definition 1, we get

$$|R| = \sum_{1 \le j_1 < \cdots < j_m \le n} (-1)^{(1+2+3+4)+(j_1+\cdots+j_m)} \begin{vmatrix} a_{1j_1} & a_{2j_2} & \cdots & a_{1j_m} \\ a_{2j_1} & a_{2j_2} & \cdots & a_{2j_m} \\ a_{3j_1} & a_{3j_2} & \cdots & a_{3j_m} \\ a_{4j_1} & a_{4j_2} & \cdots & a_{4j_m} \end{vmatrix}$$

To get the general formula for determinant of matrix R we will calculate the determinant of matrix R from order 4×5 to 4×10 as follows.

Determinant of matrix R order 4×5

Given a matrix $R_{4\times5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & a_1 & a_2 & a_3 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$.

By using Definition 1, it will be obtained

$|R_{4\times5}| = -a_2 + a_3$.

Determinant of matrix R order 4×6

Given a matrix $R_{4\times6} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & a_1 & a_2 & a_3 & a_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$.

By using Definition 1, it will be obtained

$|R_{4\times6}| = a_2 - a_3 + a_4$.

Determinant of matrix R order 4×7

Given a matrix $R_{4\times7} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & a_1 & a_2 & a_3 & a_4 & a_5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$.

By using Definition 1, it will be obtained

$|R_{4\times 7}| = -a_2 + a_3 - a_4 + a_5.$

Determinant of matrix $\boldsymbol{R}$ order $\mathbf{4 \times 8}$

Given a matrix $R_{4\times 8} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$

By using Definition 1, it will be obtained

$|R_{4\times 8}| = a_2 - a_3 + a_4 - a_5 + a_6.$

Determinant of matrix $\boldsymbol{R}$ order $\mathbf{4 \times 9}$

Given a matrix $R_{4\times 9} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$

By using Definition 1, it will be obtained

$|R_{4\times 9}| = -a_2 + a_3 - a_4 + a_5 - a_6 + a_7.$

Determinant of matrix $\boldsymbol{R}$ order $\mathbf{4 \times 10}$

Given a matrix $R_{4\times 10} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$

By using Definition 1, it will be obtained

$|R_{4\times 10}| = a_2 - a_3 + a_4 - a_5 + a_6 - a_7 + a_8.$

Based on the calculation of the determinant of matrix R from order 4×5 to 4×10, it can be obtained:

$$|R_{4\times 5}| = -a_2 + a_3 \qquad (1)$$
$$|R_{4\times 6}| = a_2 - a_3 + a_4 \qquad (2)$$
$$|R_{4\times 7}| = -a_2 + a_3 - a_4 + a_5 \qquad (3)$$
$$|R_{4\times 8}| = a_2 - a_3 + a_4 - a_5 + a_6 \qquad (4)$$
$$|R_{4\times 9}| = -a_2 + a_3 - a_4 + a_5 - a_6 + a_7 \qquad (5)$$
$$|R_{4\times 10}| = a_2 - a_3 + a_4 - a_5 + a_6 - a_7 + a_8 \qquad (6)$$

Based on Equations (1) to (6), the determinant of matrix R has two forms, namely the determinant for n is odd and n is even. From Equations (1), (3), and (5) **it can be assumed** that the general formula for the determinant of matrix R when n odd is

$$|R| = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & a_1 & a_2 & \cdots & a_i & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{vmatrix} = \sum_{i=2}^{n-2} (-1)^{i+1} a_i \qquad (7)$$

and from Equations (2), (4), and (6) **it can be assumed** that the general formula for the determinant of matrix R when n even is

$$|R| = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & a_1 & a_2 & \cdots & a_i & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{vmatrix} = \sum_{i=2}^{n-2} (-1)^{i} a_i \qquad (8)$$

Based on the assumptions in Equations (7) and (8), the truth of the assumptions will be proven in the following Theorem 1.

Theorem 1

If a non-square matrix

$$R = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & a_1 & a_2 & \cdots & a_i & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}, a_i \in \mathbb{R}, \forall i = 1,2,\dots,n-2 \text{ where } n > 4,$$

then

$$|R| = \begin{cases} \sum_{i=2}^{n-2} (-1)^{i+1} a_i \text{ , } for\ n\ odd \\ \sum_{i=2}^{n-2} (-1)^{i} a_i \text{ , } for\ n\ even \end{cases}$$

Proof.

i. Proof for n is odd

Given a matrix $R = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & a_1 & a_2 & \cdots & a_i & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}, a_i \in \mathbb{R}, \forall i = 1,2,\dots,n-2$ where $n > 4$.

By using Definition 1, $|R|$ can be obtained from the sum of the determinant of the submatrices of R which is shown in the following 4 cases.

Case 1: If A_1 is the submatrix of R whose columns are K_1, K_2, K_j, K_n where $j = 3,4,\dots,n-1$ then there are C_1^{n-3} possible forms of A_1 and

$$|A_1| = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & a_1 & a_i & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}, \forall i = 2,3,\dots,n-2$$
$$= (-1)^{(1+2+3+4)+(1+2+j+n)} a_i.$$

Case 2: If A_2 is the submatrix of R whose columns are K_1, K_2, K_p, K_q or K_1, K_p, K_q, K_n or K_2, K_p, K_q, K_n where $3 \le p \le n-2$ and $4 \le q \le n-1$ then the possible forms of $|A_2|$ are

$$|A_2| = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & a_1 & a_{p-1} & a_{q-1} \\ 0 & 0 & 0 & 0 \end{vmatrix} = 0 \text{ or } |A_2| = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & a_{p-1} & a_{q-1} & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} = 0 \text{ or } |A_2| = \begin{vmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ a_1 & a_{p-1} & a_{q-1} & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} = 0$$

Case 3: If A_3 is the submatrix of R whose columns are K_1, K_r, K_s, K_t or K_2, K_r, K_s, K_t or K_r, K_s, K_t, K_n where $3 \le r < n-2; 4 \le s \le n-1;\ 5 \le t \le n$ the the possible forms of $|A_3|$ are

$$|A_3| = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & a_{r-1} & a_{s-1} & a_{t-1} \\ 0 & 0 & 0 & 0 \end{vmatrix} = 0 \text{ or } |A_3| = \begin{vmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & a_{r-1} & a_{s-1} & a_{t-1} \\ 0 & 0 & 0 & 0 \end{vmatrix} = 0 \text{ or}$$

$$|A_3| = \begin{vmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ a_{r-1} & a_{s-1} & a_{t-1} & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} = 0$$

Case 4: If A_4 is the submatrix of R whose columns are K_u, K_v, K_w, K_x where $3 \le u < n-3;\ 4 \le v \le n-2;$

$5 \le w \le n-1; 6 \le x \le n$ the possible forms of $|A_4|$ are

$$|A_4| = \begin{vmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ a_{u-1} & a_{v-1} & a_{w-1} & a_{x-1} \\ 0 & 0 & 0 & 0 \end{vmatrix} = 0.$$

As the result,

$$|R| = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & a_1 & a_2 & \cdots & a_i & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{vmatrix}, a_i \in \mathbb{R}, \forall i = 1,2,\dots,n-2, \text{where } n > 4$$

$$= \sum|A_1| + \sum|A_2| + \sum|A_3| + \sum|A_4|$$

$$= \sum_{j=3}^{n-1}\sum_{i=2}^{n-2}(-1)^{(1+2+3+4)+(1+2+j+n)}\, a_i.$$

So that, for $j = 3,4,\dots,n-1$ we get

$$|R| = -a_2 + a_3 - \cdots - a_{n-3} + a_{n-2} = \sum_{i=2}^{n-2}(-1)^{i+1}\, a_i.$$

ii. Proof for n is even

Given a matrix $R = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & a_1 & a_2 & \cdots & a_i & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}, a_i \in \mathbb{R}, \forall i = 1,2,\dots,n-2$ where $n > 4$.

By using Definition 1, $|R|$ can be obtained from the sum of the determinant of the submatrices of R which is shown in the following 4 cases. The cases are the same as the proof for n is odd. So, they will not be rewritten in this section.

As the result,

$$|R| = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & a_1 & a_2 & \cdots & a_i & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{vmatrix}, a_i \in \mathbb{R}, \forall i = 1,2,\dots,n-2, \text{where } n > 4$$

$$= \sum|A_1| + \sum|A_2| + \sum|A_3| + \sum|A_4|$$

$$= \sum_{j=3}^{n-1}\sum_{i=2}^{n-2}(-1)^{(1+2+3+4)+(1+2+j+n)}\, a_i.$$

So that, for $j = 3,4,\dots,n-1$ we get

$$|R| = a_2 - a_3 + \cdots - a_{n-3} + a_{n-2} = \sum_{i=2}^{n-2}(-1)^{i}\, a_i.$$

So, based on the proof (i) and (ii) Theorem 1 proved.

3.1.2. The use of Determinant of a $4 \times n, n > 4$ Non-Square Matrix

The modified double-guard Hill cipher is a modification of the double-guard Hill cipher algorithm. This algorithm uses a non-square matrix of order $p \times q$ as the private key matrix K. In addition, just like the double-guard Hill cipher algorithm, the modified double-guard Hill cipher algorithm is also capable of encrypting up to 128 characters of ASCII values. In the decryption process, the modified double guard Hill cipher algorithm requires the inverse of the key matrix K^{-1} to decrypt the encrypted text (ciphertext) into the original text (plaintext). To obtain K^{-1}, the determinant of matrix K is required. The modified double-guard Hill cipher plays an important role in wireless sensor networks (WSN) to secure the data transmitted to the base station. This algorithm will encrypt the data and keep the data confidential during the transmission process.

Theorem 1 can be used to calculate the determinant of the private key matrix K in the modified double-guard Hill cipher algorithm. The use of Theorem 1 in the modified double-guard Hill cipher algorithm where matrix R is chosen as the private key matrix presented in the following example problem.

Example problem.

A person intends to send his friend a message that says

Aku belajar pukul 13:42!

The sender uses a modified double-guard Hill cipher algorithm and chooses a matrix R of order 4×5 as the private key matrix K. Before encryption, each letter in the message is substituted into ASCII values as follows.

ASCII values: [65 107 117 32 98 101 108 97 106 97 114 32 112 117 107 117 108 32 49 51 58 52 50 33]

Encryption process

1) Suppose a key matrix $K = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 3 & 2 & 9 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$.

To check whether the matrix K has an inverse, an elementary row operation will be performed to determine the rank of the matrix.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 3 & 2 & 9 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} -3\widetilde{R_2 +} R_3 \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 9 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Based on the calculations on matrix K above, it is obtained that the rank of matrix K is $r = 4$. Since the rank is equal to the number of rows of matrix K, then the matrix K has a right inverse.

2) Since the key matrix K is 4×5 then the message matrix M will has size $m \times 4$, where

$$m = \frac{\text{the numbers of elements matrix M}}{4} = \frac{24}{4} = 6.$$

So, the message matrix can be written as

$$M = \begin{bmatrix} A & l & p & 1 \\ k & a & u & 3 \\ u & j & k & : \\ SP & a & u & 4 \\ b & r & l & 2 \\ e & SP & SP & ! \end{bmatrix} = \begin{bmatrix} 65 & 108 & 112 & 49 \\ 107 & 97 & 117 & 51 \\ 117 & 106 & 107 & 58 \\ 32 & 97 & 117 & 52 \\ 98 & 114 & 108 & 50 \\ 101 & 32 & 32 & 33 \end{bmatrix}.$$

3) The cipher matrix can be obtained with

$$C = MK = \begin{bmatrix} 65 & 444 & 224 & 1008 & 49 \\ 107 & 448 & 234 & 1053 & 51 \\ 117 & 427 & 214 & 963 & 58 \\ 32 & 448 & 234 & 1053 & 52 \\ 98 & 438 & 216 & 972 & 50 \\ 101 & 128 & 64 & 288 & 33 \end{bmatrix}.$$

4) Before transmitting, the matrix C is transposed as

$$C^* = \begin{bmatrix} 65 & 107 & 117 & 32 & 98 & 101 \\ 444 & 448 & 427 & 448 & 438 & 128 \\ 224 & 234 & 214 & 234 & 216 & 64 \\ 1008 & 1053 & 963 & 1053 & 972 & 288 \\ 49 & 51 & 58 & 52 & 50 & 33 \end{bmatrix}.$$

Decryption process

1) After transmitted, the receiver of the message re-transposed the C^* matrix so that it becomes a C matrix.
2) By Definition 2, it can be obtained

$$K^{-1} = \frac{1}{|K|}\begin{vmatrix} K_{11} & \dots & K_{41} \\ \dots & \dots & \dots \\ K_{15} & \dots & K_{45} \end{vmatrix}$$

where $K_{ij} = (-1)^{i+j}\det(K_{ij}), i = 1,\dots,4$ and $j = 1,\dots,5$. The K_{ij} matrix is obtained by deleting the i-th row and j-th column of matrix K. So, the $K^{-1}(mod\ 128)$ is

$$K^{-1} = |K|^{-1}(mod\ 128) \times \begin{vmatrix} K_{11} & \dots & K_{41} \\ \dots & \dots & \dots \\ K_{15} & \dots & K_{45} \end{vmatrix}$$

Determinant of matrix K can be obtained using Theorem 1 as follow

$$|K| = \sum_{i=2}^{3}(-1)^{i+1}a_i = -a_2 + a_3 = -2 + 9 = 7.$$

So that, $|K|^{-1} = 7^{-1} = 55\ (mod\ 128)$. It means that inverse of 7 in modulo 128 is 55.

Next, determine the $K_{ij}, i = 1,\dots,4$ and $j = 1,\dots,5$. It be obtained a matrix $\begin{bmatrix} 7 & 0 & -9 & 2 & 0 \\ 0 & 7 & -6 & -1 & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & -9 & 2 & 7 \end{bmatrix}$.

Then, the $K^{-1}(mod\ 128)$ is

$$K^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 17 & 54 & 73 & 17 \\ 110 & 73 & 55 & 110 \\ 0 & 0 & 0 & 1 \end{bmatrix}(mod\ 128).$$

3) As the result, it can be obtained

$$M = CK^{-1}(mod\ 128)$$

$$= \begin{bmatrix} 65 & 444 & 224 & 1008 & 49 \\ 107 & 448 & 234 & 1053 & 51 \\ 117 & 427 & 214 & 963 & 58 \\ 32 & 448 & 234 & 1053 & 52 \\ 98 & 438 & 216 & 972 & 50 \\ 101 & 128 & 64 & 288 & 33 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 17 & 54 & 73 & 17 \\ 110 & 73 & 55 & 110 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 65 & 108 & 112 & 49 \\ 107 & 97 & 117 & 51 \\ 117 & 106 & 107 & 58 \\ 32 & 97 & 117 & 52 \\ 98 & 114 & 108 & 50 \\ 101 & 32 & 32 & 33 \end{bmatrix} (mod\ 128)$$

If the matrix M above is substituted back into ASCII values, then it is obtains the message sent is Aku belajar pukul 13:42!.

3.2. Discussions

Based on the calculation results using Definition 1 on the matrix $R_{4\times5}$ to $R_{4\times10}$, the general formula of the determinant of matrix R can be obtained which is divided into two conditions, when n is odd and n is even as stated in Theorem 1. As an application, the general formula of the determinant of matrix R in Theorem 1 is applied in the modified double-guard Hill cipher algorithm which requires the determinant of key matrix K to obtain matrix K^{-1}. In this case, any size of matrix R is chosen as the key matrix K. However, there are several conditions for a matrix R to be chosen as the key matrix in the modified double-guard Hill cipher algorithm as follows.

1) All elements of matrix R are positive integers or can be written as
$$R = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & a_1 & a_2 & \cdots & a_i & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}, a_i \in \mathbb{Z}^+, \forall i = 1,2,\dots,n-2 \text{ where } n > 4.$$
2) $|\boldsymbol{R}| \neq \boldsymbol{0}$
3) Matrix $\boldsymbol{R}$ invertible in modulo 128. It means matrix $\boldsymbol{R}$ have an inverse in modulo 128. Number 128 indicates the number of characters that can be encrypted by the modified double-guard Hill cipher algorithm.

In the given example problem, the matrix $R_{4\times5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 3 & 2 & 9 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ is chosen as key matrix K.

The message sent is Aku belajar pukul 13:42! and it is stated by matrix $M_{6\times4}$. In the encryption process, the matrix M and the matrix K are multiplied to obtain cipher matrix C, which contains the encrypted message. Determinants play a role in the decryption process to obtain the matrix K^{-1} (mod 128) which is used to decrypted matrix C so that the message will be known. Matrix K^{-1} is obtained using Definition 2. So, to obtain K^{-1} (mod 128), $|K|$ (mod 128) is required. By using Theorem 1, it is obtained that $|K| = 7$ then $|K|^{-1} = 7^{-1}$ (mod 128) is 55 cause $7 \times 55 \equiv 1$ (mod 128). Based on the calculations that have been carried out, it obtains $K^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 17 & 54 & 73 & 17 \\ 110 & 73 & 55 & 110 \\ 0 & 0 & 0 & 1 \end{bmatrix} (mod\ 128)$.

To decrypt the message, multiply matrix K^{-1} mod 128 and matrix C and it will be known that the message sent is “Aku belajar pukul 13:42!”.

4. Conclusions

Based on the results of the analysis that has been carried out, the following conclusions as follows:

If a non-square matrix

$$\boldsymbol{R} = \begin{bmatrix} \boldsymbol{1} & \boldsymbol{0} & \boldsymbol{0} & \cdots & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{1} & \boldsymbol{0} & \cdots & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{a_1} & \boldsymbol{a_2} & \cdots & \boldsymbol{a_i} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \cdots & \boldsymbol{0} & \boldsymbol{1} \end{bmatrix}, \boldsymbol{a_i} \in \mathbb{R}, \forall \boldsymbol{i} = \boldsymbol{1}, \boldsymbol{2}, \dots, \boldsymbol{n-2} \text{ where } \boldsymbol{n} > \boldsymbol{4},$$

then

$$|\boldsymbol{R}| = \begin{cases} \sum_{i=2}^{n-2}(-\boldsymbol{1})^{i+1}\boldsymbol{a_i}\ , \textbf{for n odd} \\ \sum_{i=2}^{n-2}(-\boldsymbol{1})^{i}\boldsymbol{a_i}\ , \textbf{for n even} \end{cases}.$$

One of its uses is in the modified double-guard Hill cipher algorithm, where matrix $\boldsymbol{R}$ is chosen as the key matrix with the following conditions:

i. All elements of matrix $\boldsymbol{R}$ are positive integers or can be written as $$\boldsymbol{R}=\begin{bmatrix}\mathbf{1} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0}\\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0}\\ \mathbf{0} & \boldsymbol{a_1} & \boldsymbol{a_2} & \cdots & \boldsymbol{a_i} & \mathbf{0}\\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{1}\end{bmatrix}, \boldsymbol{a_i} \in \mathbb{Z}^+, \forall \boldsymbol{i}=\mathbf{1},\mathbf{2},\dots,\boldsymbol{n}-\mathbf{2} \text{ where } \boldsymbol{n}>\mathbf{4}.$$
ii. $|\boldsymbol{R}| \neq \mathbf{0}$.
iii. Matrix $\boldsymbol{R}$ invertible in modulo 128.

References

Abdollahi, N., Jafari, M., Bayat, M., Amiri, A., & Fathy, M. (2015). An efficient parallel algorithm for computing determinant of non-square matrices based on Radic's definition. *International Journal of Distributed and Parallel Systems*, *6*(4). https://doi.org/10.5121/ijdps.2015.6401

Addis, G. M. (2015). Left-Invertible Matrices. *International Journal of Science and Research (IJSR)*, *4*(9), 288–291.

Amiri, A., Fathy, M., & Bayat, M. (2010). Generalization of some determinantal identities for non-square matrices based on Radic's Definition. *TWMS Journal of Pure and Applied Mathematics*, *1*(2), 163–175. https://pdfs.semanticscholar.org/7670/48e2cc9d1ef1a553f6ae43ab49eb6ada93d1.pdf

Anton, H., & Rorres, C. (2014). *Elementary linear algebra (applications version)* (11th ed.). Wiley.

Arunkumar, M., Murthy, S., & G, G. (2011). Determinant for non-square matrices. *International Journal of Math Science & Engineering Applications (IJMSEA)*, *5*(5), 389–401.

Aryani, F., & Hanita. (2018). Determinan matriks tidak bujur sangkar berbentuk khusus menggunakan Metode Radic. *Jurnal Sains Matematika Dan Statistika*, *4*(1), 36–42. https://doi.org/10.24014/jsms.v5i2.8904

Delima, D. (2018). *Metode Radic dalam menentukan determinan matriks tak bujur sangkar 4xn*. Universitas Islam Negeri Sultan Syarif Kasim Riau.

Ginting, D. B. (2010). Peranan Aritmetika Modulo dan Bilangan Prima pada Algoritma Kriptografi RSA (Rivest-Shamir-Adleman). *Media Informatika*, *9*(2), 48–57.

Hardy, D. W., Richman, F., & Walker, C. L. (2009). *Applied algebra codes, ciphers, and discrete algorithms* (K. H. Rosen (ed.); 2nd ed.). CRC Press Taylor & Francis Group.

Jacques-García, F. A., Uribe-Mejía, D., Macías-Bobadilla, G., & Chaparro-Sánchez, R. (2022). On modular inverse matrices a computation approach. *South Florida Journal of Development*, *3*(3), 3100–3111. https://doi.org/10.46932/sfjdv3n3-005

Jacques García, F. A., Canchola Magdaleno, S. L., & Avecilla Ramírez, G. N. (2016). Sistema de Criptografía Simétrico para la Enseñanza de las Matrices Inversas Modulares. *Tecnología Educativa Revista CONAIC*, *3*(3), 57–62. https://doi.org/10.32671/terc.v3i3.120

Makarewicz, A., Mozgawa, W., & Pikuta, P. (2016). Volumes of polyhedra in terms of determinants of rectangular matrices. *Bulletin De La Societe Des Science Et Des Lettres de Lodz*, *LXVI*(2), 105–117.

Munir, R. (2004). *Pengantar Kriptografi*. Informatika.Stei.Itb.Ac.Id. http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Pengantar Kriptografi.pdf

Radić, M. (1966). A definition of determinant of rectangular matrix. *Glasnik Matematički. Serija III*, *21*(1), 17–21. https://books.google.co.id/books?id=5z0GkLQ6LfgC&pg=PA17&redir_esc=y&hl=id#v=onepage&q&f=false

Radić, M. (2005). About a determinant of rectangular 2 × n matrix and its geometric interpretation. *Beiträge Zur Algebra Und Geometrie*, *46*(2), 321–349. https://www.emis.de/journals/BAG/vol.46/no.2/3.html

Strang, G. (2006). *Linear algebra and its applications* (4th ed.). Academic Pres.

Sušanj, R., & Radić, M. (1994). Geometrical meaning of one generalization of the determinant of a square matrix. *Glasnik Matematički*, *29*(49), 217–233.

Thangammal, C. B., Praveena, D., & Rangarajan, P. (2016). Secured Data Transmission Using Modified LEHS Algorithm in Wireless Sensor Network. *Circuits and Systems*, *07*, 1190–1198. https://doi.org/10.4236/cs.2016.78102

Zaini, Z. (2016). *Determinan matriks persegi & non persegi*. Uwais Inspirasi Indonesia.

https://books.google.com/books/about/DETERMINAN_MATRIKS_PERSEGI_NON_PERSEGI.html?id=ujSODwAAQBAJ