Academic Science Journal

Generating Self-Invertible Matrices by Hill Cipher Algorithm In Gaussian Integers

Ayat A. Jafaar and Rifaat Z. Khalaf

Department of Mathematics, College of science, University of Diyala, Diyala, Iraq
ayatalsdy@gmail.com

Received: 28 October 2022 **Accepted: 22 November 2022**

DOI: https://doi.org/10.24237/ASJ.02.01.701B

Abstract

In this paper, the Creating self-reflexive matrices for the Hill Cipher algorithm in Gaussian integers is discussed. It's not always possible to find the inverse of the matrix that was used to encrypt the plaintext. Therefore, the encrypted text cannot be deciphered if the matrix is not invertible. The encryption matrix utilized in the self-reflexive matrix Creating method is self-reflexive as well. As a result, we do not need to find the matrix's inverse during decryption. Additionally, this approach does away with the computational cost of determining the matrix's inverse during decryption. We also provided an example showing the work of Hill-Cipher using a self-reflecting matrix in Gaussian integers.

Keywords: Hill Cipher (HC), self-reflexive matrix, Gaussian Integers, Euclidean Algorithm.

إنشاء المصفوفات ذاتية الانعكاس في الاعداد الصحيحة الغاوسية لاستخدامها في شفره هيل

آيات علي جعفر و , رفعت زيدان خلف

قسم الرياضيات- كلية العلوم - جامعة ديالى

الخلاصة

في هذا البحث ، تمت مناقشة تكوين مصفوفات ذاتية الانعكاس لخوارزمية شفره هيل في الأعداد الصحيحة الغاوسية. ليس من الممكن دائمًا العثور على معكوس المصفوفة التي تم استخدامها لتشفير النص الصريح. لذلك ، لا يمكن فك تشفير النص

المشفر إذا كانت المصفوفة غير قابلة للعكس. مصفوفة التشفير المستخدمة في طريقة إنشاء المصفوفة ذاتية الانعكاس هي أيضًا ذاتية الانعكاس. نتيجة لذلك ، لا نحتاج إلى إيجاد معكوس المصفوفة أثناء فك التشفير. بالإضافة إلى ذلك ، يلغي هذا النهج التكلفة الحسابية لتحديد معكوس المصفوفة أثناء فك التشفير. قدمنا أيضًا مثالًا يوضح عمل شفره هيل باستخدام مصفوفة ذاتية الانعكاس في الأعداد الصحيحة الغاوسية.

الكلمات المفتاحية: شفره هيل, مصفوفة ذاتية الانعكاس, الاعداد الصحيحة الغاوسية, خوارزمية اقليدس

Introduction

In this day, there is undoubtedly a necessity retain the data securely of global electronic connectedness from hackers, viruses, electronic surveillance, and electronic hoaxes. This will result in a high awareness of the need to safeguard systems from network-based attacks, ensure the legitimacy of messages and information, and protect resources and information from exposure [1]. Cellular communications, e-commerce, computer passwords, pay-TV, email transmission, Automated teller machine (ATM) card security, money transmission, and digital signatures are just a few of the aspects of our daily life that are impacted by cryptography, the art of encryption.The science or art of enclosing the methods and principles for transforming a message from plaintext into cipher text, which makes no sense, and back to plaintext again is known as cryptography [1].

Today, cryptography is regarded as a field of both computer-science and mathematics and is closely related to information theory, engineering, and computer security[2]. Even yet, in the distant past, the term "cryptography" exclusively applied to the encryption and decryption of messages .Asymmetric and symmetric cryptography are now the two main classifications used. Asymmetric cryptography uses two separate keys, whereas in symmetric cryptography the sender and receiver utilize the same key for encryption and decoding. Each of these cryptosystems has benefits and drawbacks. For instance, symmetric cryptography is less secure than asymmetric cryptography, but it consumes less computational resources. Only a few cryptosystems, including Advanced Encryption Standard,(AES),Twofish, River-Cipher 4 (RC4), and Data Encryption Standard, are currently used widely (DES). On the other hand, the genesis of these Classic cryptosystems is known. The foundation for Classic cryptology is provided by conventional ciphers such the Caesar, Hill, and Vigenere ciphers.

This paper focuses on the Hill-Cipher, which was created by mathematician Lester S.-Hill and initially published in the American Mathematical Monthly in 1929.

The Gaussian integers $\mathbb{Z}[i]$ are complex number of the form $a+bi$ with $a,b\in\ \mathbb{Z}$ integers and $i=\sqrt{-1}$. The number a is called the real part and b is the imaginary part. We add two numbers as [3]

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$

And multiply as

$$(a+bi)(c+di)=(ac-bd)+(bc+ad)i$$

In this study, we suggest creating self-reflexive matrices In Gaussian Integers that can be applied to the Hill cipher technique. The goal of this study is to eliminate the drawback of utilizing a random key matrix for Hill cipher encryption when the matrix is not message invertible. Furthermore, the computational complexity can be decreased by skipping the step of obtaining the matrix inverse during decryption,

The rest of the paper is structured as follows. In section 1, the Hill-Cipher algorithm is discussed. In section 2, the Gaussian integers are explained briefly. In section 3, the modular arithmetic in Gaussian integers are covered. In section 4, the proposed method is presented. Finally, the conclusions is provided.

1. Hill Cipher (HC)

Lester Hill introduced the Hill Cipher in 1929 [4]. The Hill cipher, a famous cryptographic algorithm, is based on linear algebra. The plaintext is organized as a matrix of blocks. The Hill Cipher employs matrix multiplication and matrix inverse techniques. Hill Cipher encryption keys are square matrices, where n is the block size [5]. These matrices should be invertible because their inverses are the decryption keys [6]. A square matrix is only invertible if its determinant is not equal to zero [6].

In the conventional Hill cipher, Formula 1 and Formula 2 conduct the encryption and decryption processes, respectively.

$$C \equiv K \cdot P \ (mod\ 26) \tag{1}$$

$$P \equiv K^{-1} \cdot C \ (mod\ 26)) \tag{2}$$

where $P =$ the plaintext,

$C =$ the ciphertext,

$K =$ the encryption key,

$K^{-1} =$ the decryption key.

2. THE GAUSSIAN INTEGERS

The Gaussian integers are an interesting topic in number Theory. In this section, we give basic definitions and theorems of the Gaussian integers, see [7, 8].

Definition 2.1: (The Gaussian Integers) The Gaussian integers are given as

$$Z[i] = \{x + yi : x, y \in \mathbb{Z}, i = \sqrt{-1}\}$$

Definition 2.2: (The Conjugate) Let $\alpha = x + yi$ be a Gaussian integer, then the conjugate of α is

$$\bar{\alpha} = x - yi.$$

Note 2.1: $Z[i]$ is a commutative ring of the field of the complex numbers under the usual addition and multiplication.

Definition 2.3: (**The Norm**) Let $\alpha = x + yi$ be a Gaussian integer, then the norm of α is given as

$$N(\alpha) = \alpha\bar{\alpha} = (x + yi)(x - yi) = x^2 + y^2.$$

Proposition 2.1:

1. If $\alpha, \beta \in Z[i]$, then $N(\alpha\beta) = N(\alpha)N(B)$
2. If $\gamma \in \mathbb{Q}$, then $N(\gamma) = \gamma^2$.

Theorem 2.1: (Division Theorem): Let $\alpha, \beta \in Z[i]$, where $\beta \neq 0$, then there are $q, r \in Z[i]$, such that, $\alpha = bq + r$ and $N(r) < N(\beta)$.

Theorem 2.2: (Euclidian Algorithm): Let $\alpha, \beta \in Z[i]$ be two Gaussian integers, then by the division theorem, we have

$$\alpha = \beta\gamma_1 + \rho_1, \quad N(\rho_1) < N(\beta)$$

$$\beta = \rho_1\gamma_2 + \rho_2, \quad N(\rho_2) < N(\rho_1)$$

$$\rho_1 = \rho_2\gamma_3 + \rho_3, \quad N(\rho_3) < N(\rho_2)$$

$$\vdots$$

$$\rho_{k-2} = \rho_{k-1}\gamma_k + \rho_k, \quad N(\rho_k) < N(\rho_{k-1})$$

$$\rho_{\ k-1} = \rho_k\gamma_{k+1}.$$

The last non-zero remainder ρ_k is the greatest common divisor of α and β, and it is denoted by $\gcd(\alpha, \beta)$.

3. Modular Arithmetic In Gaussian Integers

The mathematical operations that are discussed in this article are addition, subtraction, unary operation, multiplication, and division[9] .This is the basis for creating the self-reflexive matrix for the Hill cipher method. Several characteristics of the congruence modulo operator include:

1. $\alpha \equiv \beta\ (mod\ \mu)$ if $\mu \,|\, (\alpha - \beta)$
2. $(\alpha\ mod\ \mu) = \beta\ (mod\ \mu) \Longrightarrow \alpha \equiv \beta\ mod\ \mu$
3. If $\alpha \equiv \beta\ (mod\ \mu)$ and $\beta \equiv \gamma\ (mod\ \mu) \Longrightarrow$ and $\alpha \equiv \gamma\ (mod\ \mu)$
4. If $\alpha \equiv \beta\ (mod\ \mu) \Longrightarrow \beta \equiv \alpha\ (mod\ \mu)$

Let $Z[i]_\mu^* = [0, 1, \mu - \alpha]$ the set of residues modulo μ if modular arithmetic is performed within set $Z[i]_\mu^*$, the following equation present the arithmetic operations:

Addition:

$$(\alpha + \beta) mod\ \mu = [(\alpha\ mod\ \mu) + (\beta\ mod\ \mu)]\ mod\ \mu$$

Negation:

$$-\alpha\ mod\ \mu = \ \mu - (\alpha\ mod\ \mu)$$

Subtraction:

$$(\alpha - \beta)\ mod\ \mu = [(\alpha\ mod\ \mu) - (\beta\ mod\ \mu)]\ mod\ \mu$$

Multiplication:

$$(\alpha * \beta)\ mod\ \mu = [(\alpha\ mod\ \mu) * (\beta\ mod\ \mu)]\ mod\ \mu$$

Division:

$$\left({}^{\alpha}/_{\beta}\right)\ mod\ \mu = \gamma \text{ when } \alpha = (\beta * \gamma)\ mod\ \mu$$

The following, exhibits the properties of modular in Gaussian integers.

Commutative law:

$$(\alpha + \beta) mod\ \mu = (\beta + \alpha) mod\ \mu$$

$$(\alpha * \beta)\ mod\ \mu = (\beta * \alpha)\ mod\ \mu$$

Associative

Law:

$$[(\alpha + \beta) + \gamma]\ mod\ \mu = [\alpha + (\beta + \gamma)]\ mod\ \mu$$

Distribution Law:

$$[\alpha * (\beta + \gamma)]\ mod\ \mu = \left[\left((\alpha * \beta)\ mod\ \mu\right) * \left((\alpha * \gamma)\ mod\ \mu\right)\right] mod\ \mu$$

Identities:

$$(0 + \alpha)\ mod\ \mu = \alpha\ mod\ \mu$$

$$(1 * \alpha)\ mod\ \mu = \alpha\ mod\ \mu$$

Inverses:

For each $\alpha \in Z[i]_{\mu}^{*}$, $\exists\, \beta$ such that

$$(\alpha + \beta) mod\ \mu = 0 \text{ then } \beta = -\alpha$$

For each $\alpha \in Z[i]_{\mu}^{*}$, $\exists\, \beta$ such that

$$(\alpha * \beta) mod\ \mu = 1.$$

4. *Proposed Methods: (Creating self-reflexive matrices In Gaussian Integers*)

Since the inverse of the matrix is necessary for Hill cipher decryption, it presents a challenge because it is not always present [8]. The matrix must be invertible in order for the encrypted text to be decoded. We suggest using a self-reflexive matrix generating method when using the Hill Cipher to encrypt data in order to solve this issue. The encryption matrix in the self-reflexive matrix creation method is invertible in and of itself .As a result, we don't need to find the matrix's inverse during decryption. Additionally, by using this approach, the computationally challenging task of determining the matrix's inverse during decryption is eliminated.

A self-reflexive matrix *is* a matrix whose inverse is its original value and is given by

$$B = B^{-1}.$$

Where B is Matrix of size $n \times n$.

In the proposed method, the Creating self-reflexive matrices in Gaussian Integers, where the components of the used matrices are Gaussian integers. That is, Z[i] is used in the proposed method instead of Z. By considering the finite field of Gaussian integers, Table 1 shows the corresponding Gaussian integers to the letters modulo 1+5i.

Table 1: the letters and their corresponding values of Gaussian integers.

The letter	The Integer	The corresponding Gaussian integers	The Letter	The Integer	The corresponding Gaussian integers
A	1	1	N	14	14
B	2	$1+i$	O	15	15
C	3	3	P	16	$4i$
D	4	$2i$	Q	17	$1+4i$
E	5	$1+2i$	R	18	$3+3i$
F	6	6	S	19	19
G	7	7	T	20	$2+4i$
H	8	$2+2i$	U	21	21
I	9	$3i$	V	22	22
J	10	$1+3i$	W	23	23
K	11	11	X	24	24
L	12	12	Y	25	$5i$
M	13	2+3i	Z	26	$1+5i$ or 0

4.1 Creating self-reflexive matrix(2×2) on Gaussian Integers

This segment generalizes the generation of self-reflexive 2×2 matrix over Gaussian integers z[i].

Let

$$B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}, \text{consequently } B^{-1} = \frac{1}{\Delta b}\begin{bmatrix} b_{22} & -b_{12} \\ -b_{21} & b_{11} \end{bmatrix},$$

where Δb is the determinant of matrix (B). Hence, B is said to be self-reflexive if $B^{-1} = B$ So,

1. $b_{12} = \frac{-b_{12}}{\Delta b}$ and, $b_{21} = \frac{-b_{21}}{\Delta b} \Longrightarrow \Delta b = -1$
2. $b_{11} = -b_{22} \Longrightarrow b_{11} + b_{22} = 0$

Example: (For modulo $2+3i$)

$B = \begin{bmatrix} 12i & 11i \\ i & i \end{bmatrix}$ then, $\Delta b = -1$ and $B^{-1} = \frac{1}{-1}\begin{bmatrix} i & -11i \\ -i & 12i \end{bmatrix}$,

By Euclid's algorithm we get $B^{-1} = \begin{bmatrix} 12i & 11i \\ i & i \end{bmatrix}$,

So, $B = B^{-1}$

4.2 *Creating self-reflexive matrix* **(3 × 3)** *on Gaussian Integers*

In this subsection, we broaden the definition of what it means to produce a self-reflexive 3×3 matrix on a Gaussian integer z[i].Let

$$B = \left[\begin{array}{c|cc} b_{11} & b_{12} & b_{13} \\ \hline b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{array}\right] = \left[\begin{array}{c|c} B_{11} & B_{12} \\ \hline B_{21} & B_{22} \end{array}\right],$$

Where $B_{11} = [b_{11}]$, $B_{12} = [b_{12} \quad b_{13}]$, $B_{21} = \begin{bmatrix} b_{21} \\ b_{31} \end{bmatrix}$, and $B_{22} = \begin{bmatrix} b_{22} & b_{23} \\ b_{32} & b_{33} \end{bmatrix}$, If B is self-reflexive then,

$$B_{11}^2 + B_{12}B_{21} = I,$$

$$B_{11}B_{12} + B_{12}B_{22} = 0,$$

$$B_{21}B_{11} + B_{22}B_{21} = 0,$$

and

$$B_{21}B_{12} + {B_{22}}^2 = \mathrm{I}$$

Since $B_{11} = [b_{11}]$, and $B_{21}(b_{11}I + B_{22}) = 0$, It is necessary for a non-trivial solution that, $(b_{11}I + B_{22}) = 0$.

So

$$B_{21}B_{12} = I - {B_{22}}^2, \qquad \dots (3)$$

A non-trivial solution to equation (3) will also meet this condition $B_{12}B_{21} = 1 - {b_{11}}^2$

Algorithm:

1. Select any arbitrary, 2×2 matrix B_{22}.
2. We obtain, $B_{11} = b_{11} = -$ (one of the Eigen values of B_{22})

3. Take $B_{21}B_{12} = \begin{bmatrix} b_{21} & 0 \\ b_{31} & 0 \end{bmatrix} \begin{bmatrix} b_{12} & b_{13} \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} b_{21}b_{12} & b_{21}b_{13} \\ b_{31}b_{12} & b_{31}b_{13} \end{bmatrix}$ and $B_{21}B_{12} = I - {B_{22}}^2$
4. We get $B_{12} = [b_{12} \quad b_{13}], B_{21} = \begin{bmatrix} b_{21} \\ b_{31} \end{bmatrix}$,
5. Form the matrix completely.

Example: (For modulo 2+3i)

Consider $B_{22} = \begin{bmatrix} -i & 2i \\ -i & i \end{bmatrix}$ which has Eigen value $\lambda = \mp 1$, and $b_{11} = -(-1) = 1$ or $-1 = 12$

If $b_{11} = 1$, implies

$$B_{21}B_{12} = I - {B_{22}}^2 = I - \begin{bmatrix} -i & 2i \\ -i & i \end{bmatrix} \begin{bmatrix} -i & 2i \\ -i & i \end{bmatrix} = I - \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$b_{21}b_{12} = 0.$ So $b_{21} = 0,$ and $b_{12} = 0,$

$b_{21}b_{13} = 0.$ So $b_{13} = 0$ and $b_{31} = 0,$

So the matrix will be $B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -i & 2i \\ 0 & -i & i \end{bmatrix}$. Other matrix can also be obtained if we take $b_{11} = 12$.

4.3 Creating self-reflexive matrix (4×4) on Gaussian Integers.

Here we extend the notion of what it means to generate a 4×4 self-reflexive matrix on a Gaussian integers z[i] to a more general context. Let

$$B = \left[\begin{array}{cc|cc} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ \hline b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{array}\right]$$

be self-reflexive matrix partitioned as $B = \left[\begin{array}{c|c} B_{11} & B_{12} \\ \hline B_{21} & B_{22} \end{array}\right]$

Where $B_{11} = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$, $B_{12} = \begin{bmatrix} b_{13} & b_{14} \\ b_{23} & b_{24} \end{bmatrix}$, $B_{21} = \begin{bmatrix} b_{31} & b_{32} \\ b_{41} & b_{42} \end{bmatrix}$, $B_{22} = \begin{bmatrix} b_{33} & b_{34} \\ b_{43} & b_{42} \end{bmatrix}$,

Then $B_{12}B_{21} = I - B_{11}^2 \Longrightarrow B_{12}B_{21} = (I - B_{11})(I + B_{11})$

$B_{11}B_{12} + B_{12}B_{22} = 0, B_{21}B_{11} + B_{22}B_{21} = 0,$ and $B_{21}B_{12} = I - {B_{22}}^2$

In order to obtain, solution for all the four matrix equations $B_{12}B_{21}$ can be factorized as

Then $B_{11}B_{12} + B_{12}B_{22} = B_{11}(I - B_{11})k + (I - B_{11})kB_{22}$ or $k(B_{11} + B_{22})\ (I - B_{11})$

So $B_{11} + B_{22} = 0$ or $B_{11} = I$,

Since, $B_{11} = I$ is a trivial solution then, $B_{11} + B_{22} = 0$ is taken.

The same solution is found when the third and fourth matrix equations are solved.

Algorithm:

1. Select any arbitrary, 2×2 matrix B_{22}.
2. We obtain, $B_{11} = -B_{22.}$
3. Let, $B_{12} = (I - B_{11})k$ or $(I + B_{11})k$ for k a scalar constant
4. Then, $B_{21} = (I + B_{11})\frac{1}{k}$ or $(I - B_{11})\frac{1}{k}$,
5. Form the matrix completely.

Example: (For Modulo $\mathbf{2 + 3}\boldsymbol{i}$)

Take $B_{22} = \begin{bmatrix} 1 & 3 \\ 2 + 2i & 2i \end{bmatrix}$, then, $B_{11} = \begin{bmatrix} 12 & 10 \\ -2 - 2i & -2i \end{bmatrix}$

If k is selected as 1, $B_{12} = I - B_{11},$, then

$$B_{12} = \begin{bmatrix} 2 & 3 \\ 2 + 2i & 1 + 2i \end{bmatrix} \text{ and } B_{21} = \begin{bmatrix} 0 & 10 \\ -2 - 2i & 1 - 2i \end{bmatrix},$$

We have

$$B=\begin{bmatrix} 12 & 10 & 2 & 3 \\ -2-2i & -2i & 2+2i & 1+2i \\ 0 & 10 & 1 & 3 \\ -2-2i & 1-2i & 2+2i & 2i \end{bmatrix}$$

4.4 A general method of creating an even self-reflexive matrix on Gaussian Integers.

Let $B=\left[\begin{array}{ccc|cc} b_{11} & b_{12} & \dots & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & \dots & b_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ \hline \dots & \dots & \dots & \dots & \dots \\ b_{n1} & b_{n2} & \dots & \dots & b_{nn} \end{array}\right]$ be an $n \times n$ self-reflexive matrix partitioned to

$B=\left[\begin{array}{c|c} B_{11} & B_{12} \\ \hline B_{21} & B_{22} \end{array}\right]$, where n is even and $B_{11},\ B_{12},\ B_{21}$ and B_{22} are matrices of order $\frac{n}{2} \times \frac{n}{2}$ each.

So,

$$B_{12}B_{21}=I-B_{11}^{2}=(I-B_{11})(I+B_{11}),$$

If B_{12} is one of the factors of $I-B_{11}^{2}$ then, B_{21} is the other.

Solving the 2^{nd} matrix equation results $B_{11}+B_{22}=0$, Then form the matrix.

Algorithm:

1. Select any arbitrary, $\frac{n}{2} \times \frac{n}{2}$ matrix B_{22}.
2. We get, $B_{11}=-B_{22.}$
3. Let, $B_{12}=(I-B_{11})k$ or $(I+B_{11})k$ for k a scalar constant
4. Then, $B_{21}=(I+B_{11})\frac{1}{k}$ or $(I-B_{11})\frac{1}{k}$,
5. Form the matrix completely.

Example: (For modulo $2+3i$)

Consider the following matrix

$$B_{22} = \begin{bmatrix} 1+3i & 1+i \\ 3 & 2i \end{bmatrix},$$

then,

$$B_{11} = \begin{bmatrix} -1-3i & -1-i \\ 10 & -2i \end{bmatrix}$$

Take $B_{12} = k(I - B_{11})$, with $k = 2$, then

$$B_{12} = \begin{bmatrix} 4+6i & 2+2i \\ 6 & 2+4i \end{bmatrix}.$$

by Euclid’s algorithm we get

$$B_{12} = \begin{bmatrix} 0 & 2+2i \\ 6 & 2+4i \end{bmatrix}, \text{ and } B_{21} = (I + B_{11})\frac{1}{k} \ = \begin{bmatrix} 1 & 2 \\ 5 & 12 \end{bmatrix},$$

Therefore

$$B = \begin{bmatrix} -1-3i & -1-i & 0 & 2+2i \\ 10 & -2i & 6 & 2+4i \\ 1 & 2 & 1+3i & 1+i \\ 5 & 12 & 3 & 2i \end{bmatrix}$$

5. Application of Hill-Cipher by self-reflecting matrices in Gaussian integers

The following example shows the work Hill-Cipher on a self-reflecting matrix 2x2 in Gaussian integers.

Encryption:

Choose Plaintext : AYAT: $\begin{bmatrix} 1 & 1 \\ 5i & 2+4i \end{bmatrix}$

$key = \begin{bmatrix} 12i & 11i \\ i & i \end{bmatrix}$ is self-reflecting matrices, then

$C \equiv K \cdot P \ (mod\ 2+3i)$

$\equiv \begin{bmatrix} 12i & 11i \\ i & i \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 5i & 2+4i \end{bmatrix} (mod\ 2+3i)$

$$\equiv \begin{bmatrix} -55+12i & -44+34i \\ -5+i & -4+3i \end{bmatrix} (mod\ 2+3i)$$

by Euclid’s algorithm we get

$$C \equiv \begin{bmatrix} 2 & -1+i \\ 2i & -1+i \end{bmatrix}$$

Decryption;

$$P \equiv K^{-1} \cdot C\ (mod\ 2+3i)$$

$$\equiv \begin{bmatrix} 12i & 11i \\ i & i \end{bmatrix} \begin{bmatrix} 2 & -1+i \\ 2i & -1+i \end{bmatrix} (mod\ 2+3i)$$

$$\equiv \begin{bmatrix} -22+24i & -23-23i \\ -2+2i & -2-2i \end{bmatrix} (mod\ 2+3i)$$

by Euclid’s algorithm we get

$$P \equiv \begin{bmatrix} 1 & 1 \\ 5i & 2+4i \end{bmatrix} = \begin{bmatrix} A & A \\ Y & T \end{bmatrix}$$

Conclusions

In order to create self-reflexive matrices for the Hill-Cipher algorithm in Gaussian integers. This study presents effective methods. As it is known that the Hill Cipher decoding process does not require matrix reversal, these methods are less computationally complicated. In addition, these proposed methods for creating self-reflexive matrices can be applied to other algorithms that call for matrix inversion. Also, Gaussian integers are used to change the number of the plaintext to a different number. So, in the proposed method, the time it takes to attack needs to be doubled compared to the time it takes to attack in the classic Hill-Cipher. Because of this, the new method is more reliable and stronger than the old one . Finally, We provided an example showing the working of Hill-Cipher using an self-reflecting matrix in Gaussian integers.

References

1. William Stallings " Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

2. Al-Saidi, N.M.G. and M.R.M. Said, 2009. A new approach in cryptographic systems using fractal image coding. J. Math. Stat., 5: 183-189. DOI: 10.3844/jmssp.2009.183.189
3. Alexandria, Kaeli, William, " The Arithmetic of the Gaussian Integers " MATH 444 Assignment 8 June 29, 2020
4. Forouzan, B.A. and Mukhopadhyay, D., 2015. Cryptography and network security (Vol. 12). New York, NY, USA:: Mc Graw Hill Education (India) Private Limited.
5. Widyanarko, Arya. 2007. Studi dan Analisis mengenai Hill Cipher, Teknik Kriptanalisisdan Upaya Penanggulangannya. Makalah Program Studi Teknik Informatika Institut Teknologi Bandung.
6. Mollin, A. R. 2007. An Introduction to Cryptography. Second Edition. Taylor & Francis Group. LLC.

7. J. Stillwell, Elements of Number Theory. New York, NY: Springer New York, 2003. doi: 10.1007/978-0-387-21735-2.
8. A. Koval, "Algorithm for Gaussian Integer Exponentiation," Advances in Intelligent Systems and Computing, pp. 1075–1085, 2016, doi: 10.1007/978-3-319-32467-8_93.
9. Bruce Schneir, "Applied Cryptography**",** 2nd edition, John Wiley & Sons, 1996