BAREKENG: Journal of Mathematics and Its Applications
June 2025 Volume 19 Issue 2 Page 0767–0776
P-ISSN: 1978-7227 E-ISSN: 2615-3017
https://doi.org/10.30598/barekengvol19iss2pp0767-0776

INTRODUCTION TO DOMINO KLEIN-4 GROUP CRYPTOGRAPHY

Asido Saragih [1*], Regina Ayunita Tarigan[2]

[1]*Department of Electrical Engineering, Faculty of Informatics and Electrical Engineering, Institut Teknologi Del*
[2]*Department of Metallurgical Engineering, Faculty of Industrial Technology, Institut Teknologi Del*
Jln. Sisingamangaraja, Toba-Sumatera Utara, 22381, Indonesia

*Corresponding author's e-mail: *asido.saragih@del.ac.id*

Article History:

Received: 30th June 2024
Revised: 30th January 2025
Accepted: 28th February 2025
Published: 1st April 2025

Keywords:

Cryptography;
Domino Card;
Domino Numbering;
Klein-4 Group.

ABSTRACT

As a type of simple group in mathematics, the concept of the Klein-4 group finds applications in various fields such as biology, 2D materials, games, and more. This research combines the idea of the Klein-4 group with the rules of domino cards to create a binary operation. This binary operation serves as the encryption key, and its inverse serves as the decryption key. The comprehensive process in this study represents a novel application of the Klein-4 group in cryptography. By leveraging the structural properties of the Klein-4 group, this method introduces a unique approach to securing information. The combination of group theory and modular forms in this study enhances the complexity of the encryption and decryption processes, making it more difficult for unauthorized parties to access or interpret the data. As a result, the security of the data is significantly improved. The encryption algorithm is not only efficient but also resistant to common cryptographic attacks. This study demonstrates the potential of abstract algebraic concepts in developing practical solutions for modern-day cryptographic challenges. The research methods and proposed hypotheses in this study have been validated through the proof of the given theorems. However, this study limits the data to alphabet. Researchers interested in the field of cryptography can further develop this idea to apply cryptographic processes to other types of data.

How to cite this article:

A. Saragih and R. A. Tarigan., "INTRODUCTION TO DOMINO KLEIN-4 GROUP CRYPTOGRAPHY" *BAREKENG: J. Math. & App.*, vol. 19, iss. 2, pp. 0767-0776, June, 2025.

Journal homepage: *https://ojs3.unpatti.ac.id/index.php/barekeng/*
Journal e-mail: *barekeng.math@yahoo.com; barekeng.journal@mail.unpatti.ac.id*

Research Article · Open Access

1. INTRODUCTION

Group theory is a branch of old mathematics topics theory. As a general topic in mathematics, group theory is a topic that is usually discussed in abstract algebra. This topic consists of many concepts and their operation that began from a set. Specifically, group theory discusses specific sets with a certain rule inside. Many researchers still work on this theory and its application for some mathematics needs such as complex mathematics problem [1], graph theory [2], [3], [4] and [5]. Some of the group theory concepts apply to specific fields such as molecular biology [6], 2D materials [7], enlarging group theory to a new concept related to domino card [8] and in cryptography [9].

This study discussed an application of a part of group theory named Klein-4 group and its application to cryptography. The researcher used their previous research result related to the application of the Klein-4 group in domino card rules as the function of encryption to map characters. The method used in this study is to encrypt alphabets by the rule of domino cards Klein-4 group. The domino cards rule in the Klein-4 group will scramble the arranged letters. This scrambled letter will have many probabilities to be decrypted then. The main result of this study is to present the new concept of cryptography by encrypting characters in the alphabet that guides us to an introduction of a new application of the Klein-4 group in cryptography. This study concludes that the simple concept of the Klein 4 group is applicable in cryptography.

In this study, the researcher intends to give a new application of the Klein-4 group in cryptography. In the previous research, some researchers also gave their research results regarding the relationship between group theory and cryptography, such as [10], [11], [12], and [13]. The novelty of this research will be the use of the rules in domino cards playing as the binary operation between characters as the function of the encryption.

As a part of group theory, the Klein-4 group should fulfill the group requirements. Usually, in mathematics, a group G with binary operation $*$ is denoted by $(G, *)$ [14]. A group G is a non-empty set with a binary closure operation $*$ so that for every $a, b \in$ G, $a * b \in$ G. The binary operation * should be associative so that for every $a, b, c \in G$, $(a * b) * c = a * (b * c)$. For every $a \in G$, there exists an identity element $e \in G$, so that $a * e = a$. The last of the requirements is, for every $a \in G$ there exists an inverse element $a^{-1} = b \in G$, so that $a * b = b * a = e$ [15][16]. The Klein-4 group is a kind of simple group consisting of four elements including its identity. Let G be a group and $e, a, b, c \in G$ where e is the identity element. Then G is a Klein-4 group if for every non-identity element $a \in G$, the binary operation $*$ produces $a * a = e$, and for every non-identity element, the binary operation $*$ produces another non-identity element so that $a * b = c$, $a * c = b$, and $a * c = b$ [17]. The Klein-4 group only has a bijective mapping therefore it is an isomorphic group [18]. Since its binary operation is commutative, then it is an abelian group [19][20].

The principles of the Klein-4 group apply to the domino cards rule of play. Domino cards are a set of cards whose surface is divided into two parts consisting of several dots on their surface for each part. Generally, the domino cards consist of a combination of zero to six dots. By enlarging the concept for the research needs, the researcher defined the number of dots on both parts of the domino card surface as p and q dots, where p and q are whole numbers. In this study, the researcher used domino numbering (p, q) to notate the surface of domino cards consisting of p and q dots. The rule of playing domino cards is that two cards will replace the same number of dots on their surface by the different number of dots. Let $*$ be the binary operation between two domino cards that is defined as $*$: "deleting the same pattern", then the first domino card consists of (p, q) dots and the second domino card consists of (q, r) dots will produce $(p, q) * (q, r) = (p, r)$, and p, q, and r, are elements of whole numbers. This rule will produce $(0, 0)$ when we operate the same pattern of two cards.

The collection of domino cards that can form a Klein-4 group must be sets of four cards which the number of dots on its surface should fully fill the requirement in **Equation (4)** represented in the next section, and the $(0, 0)$ card as the identity element [8]. The idea of forming a set of Klein-4 group with the binary operation $*$: "deleting the same pattern" will be used in this study to create a cryptography encryption algorithm.

Grammatically, the word "cryptography" means unknown and invisible writing that comes from Greek words such as "Kryptos" and "Graphikos" [21]. The text that needs to be encrypted is called "plaintext input". The text that has been encrypted is called "transmitted ciphertext", and the text that has been decrypted is called "plaintext output". The scrambling process of the plaintext input to be transmitted ciphertext is called encryption, and the process of reversing the ciphertext to plaintext output is called decryption. The scrambling

function of the plaintext input to be transmitted ciphertext is called the encryption algorithm, and the function of transmitted ciphertext decryption to be plaintext output is called the decryption algorithm [22]. Since the cryptography created in this study used the concept of the domino card rules of play in the Klein-4 group, the cryptography will be named The Domino Klein-4 Group Cryptography.

The concept of creating The Domino Klein-4 Group Cryptography (DK-4C) adopts the principle of the symmetric chipper model, which is the model of cryptography when the sender and the recipient of text or message use the same key [23]. In the symmetric cipher model, the sender encrypts the plaintext input using an encryption secret key, producing the transmitted ciphertext. The next step is to decrypt the transmitted ciphertext to produce the plaintext output. This process will be handled by the decryption algorithm using the secret decryption key. The decrypted text will be the same as the plain input text that we call plaintext output. The plaintext output will be able to be read by the recipient as the same text as the plaintext input.

Various researchers have explored different algorithms to enhance data security. Some have focused on identifying weaknesses in cryptography [24], while others have evaluated the effectiveness of algorithms by comparing symmetric and asymmetric cryptography [25]. Additionally, some researchers have developed methods to convert data into bits and invert them to protect against attacks [26]. Other studies have explored cryptographic concepts using modular forms [27]. However, the security of the encryption and decryption process could be further enhanced by integrating modular forms with other approaches. In this study, the researchers introduce a new perspective on data encryption and decryption by developing a novel cryptographic technique. This technique integrates the concept of the Klein-4 group, the binary operation in domino cards to produce certain types such as the pattern randomizer, modular arithmetic, and applying them to the encryption and decryption of textual data. At the end of this study, the researcher formulates the idea of using the step function concept as the encryption and decryption key. The step function is a type of non-continuous function in mathematics [28].

2. RESEARCH METHODS

The researcher used the literature study method to achieve this study's purpose. Using the concept of symmetric chipper model cryptography, the researcher combines the idea of Klein-4 group and the binary operation on domino cards to create a new concept of cryptography. This study begins by representing each letter of the alphabet as a combination of numerical values on the surface of a domino card. For sentences composed of words with exactly four letters, the encryption and decryption processes can be directly performed using the binary operation mapping function in the Domino Klein-4 Group, referred to in this study as The Special 4 Cryptography. Meanwhile, for sentences with a random number of letters, the researchers propose an integrated approach combining the Klein-4 group, the Klein-4 domino group, and modular arithmetic, which is introduced in this study as The Domino Klein-4 Cryptography. Visually, the model of symmetric cipher is given by the following scheme:

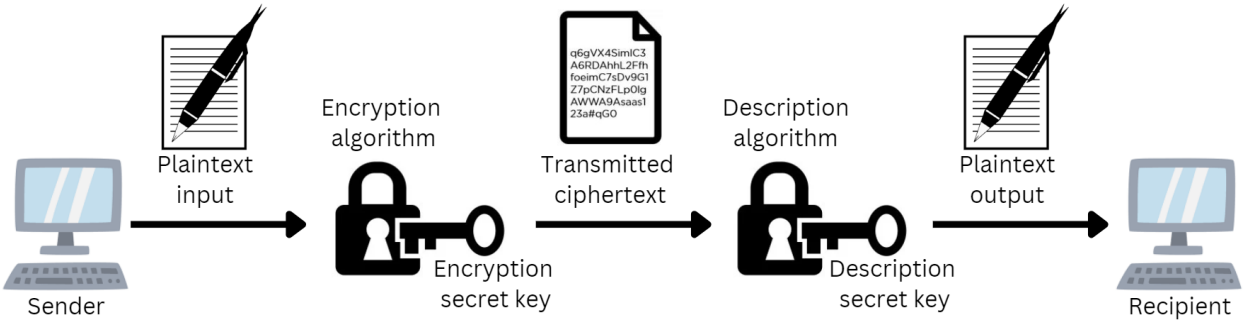

Figure 1. Symmetric Cipher Model

The cryptographic DK-4C encrypting and decrypting method used the Klein-4 group mapping concept. Let $\boldsymbol{e}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \boldsymbol{G}$ be a set; then the Klein-4 group of $\boldsymbol{G}$ with $\boldsymbol{f}$ as its binary operation is given by the following Cayley table.

Table 1. Cayley Table of Klein-4 Group

f	e	a	b	c	
e	e	a	b	c	
a	a	e	c	b	type 1
b	b	c	e	a	type 2
c	c	b	a	e	type 3

At this step, we use the first line elements of Cayley table $\boldsymbol{eabc}$ as our plaintext input, with $\boldsymbol{f}$ as our encryption secret key. The type 1 of DK-4C yields $\boldsymbol{aecb}$ as the transmitted ciphertext. The type 2 ciphertext is $\boldsymbol{bcea}$, and the type 3 is $\boldsymbol{cbae}$. Using function notation and the key $\boldsymbol{f}$ as the function, the DK-4C of Table 1 above provide the following mapping of encryption:

$$\begin{aligned} \boldsymbol{f}(\boldsymbol{eabc}) &= \boldsymbol{aecb} && \text{type 1} \\ \boldsymbol{f}(\boldsymbol{eabc}) &= \boldsymbol{bcea} && \text{type 2} \\ \boldsymbol{f}(\boldsymbol{eabc}) &= \boldsymbol{cbae} && \text{type 3} \end{aligned} \tag{1}$$

Remember that for every type of encryption DK-4C obtained from the binary $\boldsymbol{f}$ operation between $\boldsymbol{eabc}$ and a single non-identity element, for example, type 1 DK-4C can simply be written in binary notation as:

$$\begin{aligned} \boldsymbol{e\,f\,a} &= \boldsymbol{a} \\ \boldsymbol{a\,f\,a} &= \boldsymbol{e} \\ \boldsymbol{b\,f\,a} &= \boldsymbol{c} \\ \boldsymbol{c\,f\,a} &= \boldsymbol{b} \end{aligned} \tag{2}$$

Therefore, type 1 of the encryption of DK-4C, is obtained by binary operation between every element in $\boldsymbol{G}$ to the element $\boldsymbol{a}$. Type 2 and type 3 are also obtained using the same binary operation to the single element $\boldsymbol{b}$ and $\boldsymbol{c}$. Therefore, using the key $\boldsymbol{f^{-1}}$ as the inverse of $\boldsymbol{f}$, we can decrypt the transmitted ciphertext to be the plaintext output. For example, the transmitted ciphertext of type 1 can be decrypt to the plaintext output as

$$\begin{aligned} \boldsymbol{a\,f^{-1}\,a} &= \boldsymbol{e} \\ \boldsymbol{e\,f^{-1}\,a} &= \boldsymbol{a} \\ \boldsymbol{c\,f^{-1}\,a} &= \boldsymbol{b} \\ \boldsymbol{b\,f^{-1}\,a} &= \boldsymbol{c}, \end{aligned} \tag{3}$$

or simply by function notation, it can be stated as $\boldsymbol{f^{-1}}(\boldsymbol{aecb}) = \boldsymbol{eabc}$. The same principle can be used to decrypt type 2 and type 3 DK-4C encryption. The $\boldsymbol{f^{-1}}$ decryption secret key uses same rule of binary operation in the Klein-4 group. The explanation regarding to $\boldsymbol{f} = \boldsymbol{f^{-1}}$ will be provided in the next section as Theorem 1.

The concept of the Klein-4 group has been applied to the rules of play for Domino cards [8]. For the examples of the operation of binary operation $*$ between two domino cards is represented by Figure 2 below.

(a) **(b)**

Figure 2. (a) Two Different Patterns (3, 5) and (5, 4) of Domino Cards Produce (3, 4), (b) Two of The Same Pattern Of Domino Cards Produce (0, 0)

The possibility of the sets of four domino cards form a Klein-4 group should fulfill the requirement:

$$(\boldsymbol{p}, \boldsymbol{q}) * (\boldsymbol{q}, \boldsymbol{r}) = (\boldsymbol{p}, \boldsymbol{r}) \tag{4}$$

where $\boldsymbol{p}$, $\boldsymbol{q}$, $\boldsymbol{r}$ are whole numbers [8]. Using the same concept, let us transform every letter in the alphabet to domino numbering, as shown in the following figure.

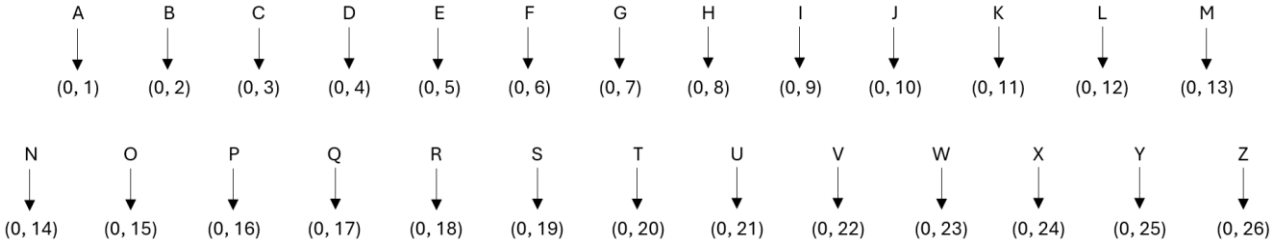

Figure 3. Transformation of Alphabet to Number

After transforming alphabetic letters to domino numbering notation, we will create the encryption key using binary operation $*$ for every converted alphabet, which can form **Equation (1)**. In this study, the researcher labels the type of the encryption algorithm using numbers. The type $\boldsymbol{i}$ for $1 \leq \boldsymbol{i} \leq 25$ indicates the number of skipped letters in the alphabet.

By arranging alphabetic letters in **Figure 3**, we can form sets of the Klein-4 group alphabetic so that every character in the alphabet can be encrypted. Using the transformation in **Figure 3,** encrypted characters that form elements of the Klein-4 group, forming **Equation (4)**, can be listed as follows.

Table 2. List of Paired Element Forming Klein-4 Group in Encryption Algorithm

Identity element (element $\boldsymbol{e}$)	Plaintext input alphabet letters (element $\boldsymbol{a}$)	Key element (element $\boldsymbol{b}$)	Transmitted alphabet letters (element $\boldsymbol{c}$)	Letter encryption description	Type of encryption
(0, 0)	(0, 1)	(1, 2)	(0, 2)	A → B	type 1
		(1, 3)	(0, 3)	A → C	type 2
		(1, 4)	(0, 4)	A → D	type 3
		(1, 5)	(0, 5)	A → E	type 4
		(1, 6)	(0, 6)	A → F	type 5
	⋮	⋮	⋮	⋮	⋮
	(0, 25)	(25, 26)	(0, 26)	Y → Z	type 1
	(0, 26)	(26, 1)	(0, 1)	Z → A	type 1

Based on **Table 2** above, we introduce an encryption key function that depends on the plaintext input alphabet letters. The researcher formulates this function as both the encryption and decryption key, represented by the following equation. Let $(\boldsymbol{0}, \boldsymbol{j})$ be an alphabetic letter that is used to form the plaintext input that is encrypted by type-$\boldsymbol{i}$ encryption, then the encryption key denoted as $\boldsymbol{\phi}$ function defined as:

$$\boldsymbol{\phi}[(\boldsymbol{0}, \boldsymbol{j})] = (\boldsymbol{0}, \boldsymbol{j} + \boldsymbol{i}) = (\boldsymbol{0}, \boldsymbol{l}); \textbf{ such as } \boldsymbol{l} = \boldsymbol{j} + \boldsymbol{i}. \tag{5}$$

Therefore, the decryption key defined as:

$$\boldsymbol{\phi}^{-1}[(\boldsymbol{0}, \boldsymbol{l})] = (\boldsymbol{0}, \boldsymbol{l} - \boldsymbol{i}) = (\boldsymbol{0}, \boldsymbol{j}). \tag{6}$$

3. RESULTS AND DISCUSSION

In the previous section, it has been mentioned that the key for encryption and decryption functions with identical mapping. The complete statement and proof of this argument are given in the following theorem.

Theorem 1. *Let f be an encryption key of Domino Klein-4 Cryptography. If f^{-1} is the decryption key, then $f = f^{-1}$.*

Proof. Since *f* is an encryption key of DK-4C, then *f* will map every element in DK-4C as well as shown in **Equation (2)**. Assume $f \neq f^{-1}$, but the decryption map should give us the **Equation (3)**, then the assumption is wrong. Hence, our assertion is proved. ■

Before discussing the main purpose of this study, the researcher provides a brief preliminary on the special case of the Klein-4 group cryptography. This case is the condition for encrypting four letters of the alphabet using the concept of the Klein-4 Group.

3.1 The Special 4 Cryptography

The Special 4 Cryptography (S-4C) is a method for encrypting and decrypting sentences where each word has only four letters. The cryptography key used in S-4C adopts the binary operation principle of the Klein-4 group, which has a single identity element and non-identity elements for the remaining three letters. The encryption algorithm uses the binary operation in the Klein-4 group for each type. For the decryption algorithm in S-4C, since it adopts the concept of the Klein-4 group, we need to know the type of encryption used. Using **Theorem 1**, the decryption key follows the same operational and binary principles as the encryption key. An example of S-4C will be provided as follows.

Example 1. Let us encrypt the sentence "JOHN EATS SOME FOOD" using S-4C method of type 2 from **Table 1**. The results will be as follows:

Table 3. Encryption Example of TS-4C

Plaintext input	J	O	H	N	E	A	T	S	S	O	M	E	F	O	O	D
As element of group	*e*	*a*	*b*	*c*	*e*	*a*	*b*	*c*	*e*	*a*	*b*	*c*	*e*	*a*	*b*	*c*
Transmitted ciphertext	H	N	J	O	T	S	E	A	M	E	S	O	O	D	F	O

Now we have "HNJO TSEA MESO ODFO" as the transmitted ciphertext. There are several possibilities for pairing each letter as the identity or non-identity of the Klein-4 group. Additionally, there are 24 ways to arrange each letter as an element of the Klein-4 group for each word. Using the same operation as the encryption key, we define the decryption key. Simply, for the decryption example, we will decrypt the transmitted text above, which was obtained using type 2 encryption. Therefore, the decryption will also use type 2, following the **Theorem 1**. Using the decryption type 2, we must operate every letter in the transmitted ciphertext with element *b*. The complete process is given in the following table.

Table 4. Decryption Example of TS-4C

Transmitted ciphertext	H	N	J	O	T	S	E	A	M	E	S	O	O	D	F	O
As element of group	*e*	*a*	*b*	*c*	*e*	*a*	*B*	*c*	*e*	*a*	*b*	*c*	*e*	*a*	*b*	*c*
Plaintext output	J	O	H	N	E	A	T	S	S	O	M	E	F	O	O	D

Using binary operation $*$ as the encryption key and $*^{-1}$ decryption key, we can write:

$*$ (JOHN EATS SOME FOOD) = HNJO TSEA MESO ODFO

and

$*^{-1}$ (HNJO TSEA MESO ODFO) = JOHN EATS SOME FOOD

such that $* = *^{-1}$.

Unfortunately, sentences are not always formed by four letters of the alphabet. Therefore, we need further exploration to create a new concept for this condition. This study will provide a random condition that works for every sentence by merging the ideas of the Klein-4 group and Domino Card rules of play explained in the next subsection.

3.2 The Domino Klein-4 Cryptography

The Domino Klein-4 Cryptography (DK-4C) is a data encryption and decryption method that adopts the principles of the Domino Klein-4 Group. The limitations of the encryption and decryption process using S-4C make DK-4C highly advantageous. After each letter is transformed into a pair of domino card numbers, as illustrated in **Figure 3**, the encryption transformation of letters proceeds according to the pattern specified in **Table 2**. The encryption key is determined using **Equation (5)**, while the decryption key is derived from **Equation (6)**. The following example demonstrates the application of DK-4C in the data encryption and decryption process.

Example 2. Let's take the plaintext input "HELLO" to be encrypted and decrypted using DK-4C type 3. The encryption process will be carried out as follows.
First, transform the alphabetic letters of plaintext input "HELLO" to the domino numbering such as:
$H = (0,8)$; $E = (0,5)$; $L = (0,12)$; $O = (0,15)$.
Second, use the encryption key of **Equation (5)** to encrypt the plaintext input, which will give us the following result:
$\phi[(0,8)] = (0,11) =$ K;
$\phi[(0,5)] = (0,8) =$ H;
$\phi[(0,12)] = (0,15) =$ O;
$\phi[(0,12)] = (0,15) =$ O;
$\phi[(0,15)] = (0,18) =$ R.

Finally, our transmitted ciphertext become "KHOOR".
Now, let us use **Equation (6)** as our decryption key to decrypt the transmitted ciphertext into the plaintext output.

First, transform the transmitted ciphertext "KHOOR" to the domino numbering as follows:
K = (0, 11); H = (0, 8); O = (0, 15); O = (0, 15); R = (0, 18).
Second, use the decryption key of **Equation (6)** to decrypt the transmitted ciphertext, which will give us the following result:

$\phi^{-1}[(0,11)] = (0, 8) =$ H;
$\phi^{-1}[(0,8)] = (0, 5) =$ E;
$\phi^{-1}[(0,15)] = (0, 12) =$ L;
$\phi^{-1}[(0,15)] = (0, 12) =$ L;
$\phi^{-1}[(0,18)] = (0, 15) =$ O.
Finally, we get "HELLO" as our plaintext output.

As mentioned in the previous section, the researcher formulates the idea of using a step function as the encryption and decryption key. For any transformed letter $(0, j_k)$; $1 \le k \le 26$, and any used type i_n, $n \in \mathbb{Z}^+$, we defined the encryption key as:

$$\boldsymbol{\phi}[(\mathbf{0}, \boldsymbol{j_k})] = \begin{cases} (\mathbf{0}, \boldsymbol{j_1} + \boldsymbol{i_1}) = (\mathbf{0}, \boldsymbol{l_1}); & \boldsymbol{p_1} \le \boldsymbol{j_1} \le \boldsymbol{p_2}, \ \textbf{as type } \boldsymbol{i_1} \\ (\mathbf{0}, \boldsymbol{j_2} + \boldsymbol{i_2}) = (\mathbf{0}, \boldsymbol{l_2}); & \boldsymbol{p_3} \le \boldsymbol{j_2} \le \boldsymbol{p_4}, \ \textbf{as type } \boldsymbol{i_2} \\ \vdots & \vdots \\ (\mathbf{0}, \boldsymbol{j_m} + \boldsymbol{i_m}) = (\mathbf{0}, \boldsymbol{l_m}); & \boldsymbol{p_x} \le \boldsymbol{j_m} \le \boldsymbol{p_y}, \ \textbf{as type } \boldsymbol{i_m}. \end{cases} \quad (7)$$

At this step, we now have $(0, l_1)$, $(0, l_2)$, . . ., $(0, l_m)$ as the transmitted cipher text domino numbering. Since the letters of plaintext input are added to each i_n, where $1 \le n \le m$, the domino numbers of transmitted ciphertext could become $(0, q)$ with $q > 26$. To ensure that every domino number of the transmitted ciphertext can be transformed into alphabetic letters, the researcher used the modular numbering concept. The modular concept is a numbering concept where a number is congruent to another number that is less than or equal to itself. The congruence is usually notated by $\equiv$ and pronounced as "congruent". For any positive integers a, b, and c, if we state $a \equiv b$ (mod c), it means c divides the difference $a - b$, or equivalently, "a is congruent to b modulo c". In this case, b is called the remainder when a divided by c **[29]**. In this research, the modular concept is used to ensure that every domino number representing letters will always be congruent to every positive integer less than or equals to 26. The researcher used the remainder as the congruent element to replace the domino number of the transmitted ciphertext if it exceeds 26. Using subtraction as the inverse of addition, let us denote every $(0, l_n)$; $1 \le n \le m$, as the transmitter cipher text domino numbering. Then, the decryption key is formulated as follows:

$$\boldsymbol{\phi^{-1}}[(\mathbf{0}, \boldsymbol{l_n})] = \begin{cases} (\mathbf{0}, \boldsymbol{l_1} - \boldsymbol{i_1}) = (\mathbf{0}, \boldsymbol{j_1}); \ \boldsymbol{p_1} + \boldsymbol{i_1}(\boldsymbol{mod}\ \mathbf{26}) \le \boldsymbol{l_1} \le \boldsymbol{p_2} + \boldsymbol{i_1}\ (\boldsymbol{mod}\ \mathbf{26}), \textbf{as type } \boldsymbol{i_1} \\ (\mathbf{0}, \boldsymbol{l_2} - \boldsymbol{i_2}) = (\mathbf{0}, \boldsymbol{j_2}); \ \boldsymbol{p_3} + \boldsymbol{i_2}(\boldsymbol{mod}\ \mathbf{26}) \le \boldsymbol{j_2} \le \boldsymbol{p_4} + \boldsymbol{i_2}\ (\boldsymbol{mod}\ \mathbf{26}), \textbf{as type } \boldsymbol{i_2} \\ \vdots \qquad\qquad \vdots \\ (\mathbf{0}, \boldsymbol{l_m} - \boldsymbol{i_m}) = (\mathbf{0}, \boldsymbol{j_m}); \boldsymbol{p_x} + \boldsymbol{i_m}(\boldsymbol{mod}\ \mathbf{26}) \le \boldsymbol{j_m} \le \boldsymbol{p_y} + \boldsymbol{i_m}\ (\boldsymbol{mod}\ \mathbf{26}), \textbf{as type } \boldsymbol{i_m}. \end{cases} \quad (8)$$

For a clear explanation of using the encryption and decryption keys given in **Equation (7)** and **Equation (8)**, the researcher provides the following example.

Example 3. Let us encrypt the sentence "I AM FULL" using DK-4C method with the following step function as the encryption key:

$$\phi[(0,j_k)] = \begin{cases} (0,j_1+2); & 0 \le j_1 \le 10 \\ (0,j_2+3); & 11 \le j_2 \le 15 \\ (0,j_3+1); & 16 \le j_3 \le 26. \end{cases}$$

First, transform the alphabetic letters of plaintext input "I AM FULL" to domino numbering as follows:
I = (0, 9); A = (0, 1); M = (0, 13); F = (0, 6); U = (0, 21); L = (0, 12); L = (0, 12).
Second, after applying the encryption key, the transmitted ciphertext obtained as "K CP HXOO".

Using the decryption equation by following the principal of **Equation (8)**, the decryption key formulated as:

$$\phi^{-1}[(0,l_n)] = \begin{cases} (0,l_1-2); & 2\ (mod\ 26) \le j_1 \le 12\ (mod\ 26) \\ (0,l_2-3); & 14\ (mod\ 26) \le j_2 \le 18\ (mod\ 26) \\ (0,l_3-1); & 17\ (mod\ 26) \le j_3 \le 27\ (mod\ 26) \end{cases}$$

After transforming the obtained transmitted ciphertext to the domino numbering, we can apply the decryption key mentioned above to decrypt and obtain "I AM FULL" as the plaintext output.

Examining the idea of Domino Klein-4 Cryptography further, the encryption and decryption processes can be made more complex to enhance data security compared to using only modular concepts. When relying solely on modular arithmetic, text data can be easily decrypted if the congruence equation is known. For comparison, the following example is provided:

Example 4. Let us encrypt the text "I AM FULL" using the encryption key is $\phi[(0,j_k)] \equiv (0,j_k+2)(mod\ 26)$. After representing every character, the decrypted data will be (0, 11), (0, 3), (0, 13), (0, 8), (0, 23), (0,14), (0, 14) which gives "K CO HWNN". Easily by using the uniform decryption key $\phi^{-1}[(0,l_n)] \equiv (0,j_k-2)(mod\ 26)$, we may obtain the plain text output.

4. CONCLUSIONS

Some previous research has applied the concept of the Klein-4 group in various fields. By combining the concept of the Klein-4 group with the rules of domino cards, this study introduces a new application of the Klein-4 group in cryptography. Specifically, this study focuses on cryptographic methods for alphabetic letters. When forming sentences using exactly four alphabetic letters, the mapped concept of the Klein-4 group suffices. For converting alphabetic letters into domino numbers under general conditions, the researcher uses

$$\phi[(0,j_k)] = \begin{cases} (0,j_1+i_1) = (0,l_1)\,; & p_1 \le j_1 \le p_2, & \text{as type } i_1 \\ (0,j_2+i_2) = (0,l_2); & p_3 \le j_2 \le p_4, & \text{as type } i_2 \\ \vdots & & \vdots \\ (0,j_m+i_m) = (0,l_m); & p_x \le j_m \le p_y, & \text{as type } i_m. \end{cases}$$

as the encryption key, and

$$\phi^{-1}[(0,l_n)] = \begin{cases} (0,l_1-i_1) = (0,j_1);\ p_1+i_1(mod\ 26) \le l_1 \le p_2+i_1\ (mod\ 26), \text{as type } i_1 \\ (0,l_2-i_2) = (0,j_2);\ p_3+i_2(mod\ 26) \le j_2 \le p_4+i_2\ (mod\ 26), \text{as type } i_2 \\ \vdots \qquad\qquad \vdots \\ (0,l_m-i_m) = (0,j_m);\ p_x+i_m(mod\ 26) \le j_m \le p_y+i_m\ (mod\ 26), \text{as type } i_m. \end{cases}$$

as the decryption key.

This section marks the final part of this study. With humility, the researchers acknowledge that there are still shortcomings and aspects that need further refinement to make this study completer and more beneficial. Researchers with an interest in cryptography are encouraged to further develop the Domino Klein-4 Cryptography by integrating additional mathematical concepts, just as this study combines the Klein-4 group, the Klein-4 domino group, and modular arithmetic.

Furthermore, researchers interested in encryption and decryption of data beyond alphabetic text—such as numbers, alphanumeric combinations, or even image and pattern data, if feasible—may find this an intriguing area for further exploration.

REFERENCES

[1] P. Goyat and D. A. K. Malik, "GROUP THEORY AND ITS APPLICATION FOR SOLVING COMPLEX MATHEMATICAL PROBLEM," *Turkish Journal of Computer and Mathematics Education*, vol. 11, no. 01, pp. 340–345, 2020.

[2] M. N. Husni, H. Syafitri, A. M. Siboro, A. G. Syarifudin, Q. Aini, and I. G. A. W. Wardhana, "THE HARMONIC INDEX AND THE GUTMAN INDEX OF COPRIME GRAPH OF INTEGER GROUP MODULO WITH ORDER OF PRIME POWER," *BAREKENG: Jurnal Ilmu Matematika dan Terapan*, vol. 16, no. 3, pp. 961–966, Sep. 2022, doi: 10.30598/barekengvol16iss3pp961-966.

[3] L. R. W. Putra, Z. Y. Awanis, S. Salwa, Q. Aini, and I. G. A. W. Wardhana, "THE POWER GRAPH REPRESENTATION FOR INTEGER MODULO GROUP WITH POWER PRIME ORDER," *BAREKENG: Jurnal Ilmu Matematika dan Terapan*, vol. 17, no. 3, pp. 1393–1400, Sep. 2023, doi: 10.30598/barekengvol17iss3pp1393-1400.

[4] A. S. Bawana, A. Sutjijana, and Y. Susanti, "ON THE GIRTH, INDEPENDENCE NUMBER, AND WIENER INDEX OF COPRIME GRAPH OF DIHEDRAL GROUP," *BAREKENG: Jurnal Ilmu Matematika dan Terapan*, vol. 17, no. 3, pp. 1695–1702, Sep. 2023, doi: 10.30598/barekengvol17iss3pp1695-1702.

[5] D. S. Ramdani, I. G. A. W. Wardhana, and Z. Y. Awanis, "THE INTERSECTION GRAPH REPRESENTATION OF A DIHEDRAL GROUP WITH PRIME ORDER AND ITS NUMERICAL INVARIANTS," *BAREKENG: Jurnal Ilmu Matematika dan Terapan*, vol. 16, no. 3, pp. 1013–1020, Sep. 2022, doi: 10.30598/barekengvol16iss3pp1013-1020.

[6] E. A. Rietman, R. L. Karp, and J. A. Tuszynski, "REVIEW AND APPLICATION OF GROUP THEORY TO MOLECULAR SYSTEMS BIOLOGY," *Theor Biol Med Model*, vol. 8, no. 1, 2011, doi: 10.1186/1742-4682-8-21.

[7] M. Y. H. Widianto and M. Saito, "APPLICATIONS OF DOUBLE GROUP THEORY IN 2D MATERIALS," *International Journal of Computing Science and Applied Mathematics*, vol. 9, no. 2, p. 60, 2023.

[8] A. Saragih and S. Chintia Purba, "APPLICATION OF KLEIN-4 GROUP ON DOMINO CARD," *International Journal of Applied Sciences and Smart Technologies*, vol. 2, no. 1, pp. 67–74, 2020.

[9] T. Wang and Z. Xu, "THE APPLICATION OF GROUP THEORY BEHIND MODERN CRYPTOGRAPHY," *Theoretical and Natural Science*, vol. 13, no. 1, pp. 195–201, Nov. 2023, doi: 10.54254/2753-8818/13/20240844.

[10] M. Ravi, "THE ROLE OF GROUP THEORY IN MODERN CRYPTOGRAPHY," *J Emerg Technol Innov Res*, 2023, [Online]. Available: www.jetir.org

[11] P. Arora, "USE OF GROIP THEORY IN CRYPTOGRAPHY," *International Journal of Advance Research and Innovative Ideas in Education(IJARIIE)*, vol. 2, no. 6, 2016, [Online]. Available: www.ijariie.com

[12] S. R. Blackburn, C. Cid, and C. Mullan, "GROUP THEORY IN CRYPTOGRAPHY," Jun. 2009, [Online]. Available: http://arxiv.org/abs/0906.5545

[13] D. Kahrobaei, R. Flores, and M. Noce, "GROUP-BASED CRYPTOGRAPHY IN THE QUANTUM ERA," *American Mathematics Society*, 2022.

[14] J. Amreen and S. Naduvath, "ORDER SUM GRAPH OF A GROUP," *Baghdad Science Journal*, vol. 20, no. 1, pp. 181–188, 2023, doi: 10.21123/bsj.2022.6480.

[15] G. T. Lee, *ABSTRACT ALGEBRA-AN INTRODUCTORY COURSE*. Switzerland: Springer, 2018. [Online]. Available: http://www.springer.com/series/3423

[16] M. M. Romsery, H. W. M. Patty, and M. W. Talakua, "IDENTIFIKASI BASIS GRÖBNER DALAM IDEAL RING POLINOMIAL," *BAREKENG: Jurnal Ilmu Matematika dan Terapan*, vol. 9, pp. 11–20, 2015.

[17] G. R. Pérez Teruel, G. R. Pérez, T. Communicated, J. Luis, and L. Bonilla, "MATRIX OPERATORS AND THE KLEIN FOUR GROUP," *Palestine Journal of Mathematics*, vol. 9, no. 1, pp. 402–410, 2020, [Online]. Available: https://www.researchgate.net/publication/336995210

[18] M. P. Lobo, "EVERY GROUP IS ISOMORPHIC TO A GROUP OF PERMUTATIONS," *Open Journal of Mathematics and Physics*, vol. 3, pp. 1–7, 2021, doi: 10.31219/osf.io/63pmy.

[19] M. Kobayashi, "HOPFIELD NEURAL NETWORKS USING KLEIN FOUR-GROUP," *Neurocomputing*, vol. 387, pp. 123–128, Apr. 2020.

[20] S. S. Carita and H. Kabetta, "MODIFICATION OF POLLARD RHO ALGORITHM USING NEGATION MAPPING," *BAREKENG: Jurnal Ilmu Matematika dan Terapan*, vol. 16, no. 4, pp. 1159–1166, Dec. 2022, doi: 10.30598/barekengvol16iss4pp1159-1166.

[21] P. Sharma, K. Yadav, and A. Kumar Tiwari, "A REVIEW PAPER ON NETWORK SECURITY AND CRYPTOGRAPHY," *World Journal of Research and Review (WJRR)*, vol. 14, no. 5, pp. 20–14, 2022, [Online]. Available: www.wjrr.org

[22] W. Stallings, *Cryptography and Network Security - Principles and Practice*, Seventh Edition. India: Pearson Education India, 2017.

[23] M. U. Bokhari and Q. M. Shallal, "A REVIEW ON SYMMETRIC KEY ENCRYPTION TECHNIQUES IN CRYPTOGRAPHY," *Int J Comput Appl*, vol. 147, no. 10, pp. 975–8887, 2016.

[24] S. A. Ahmad and A. B. Garko, "HYBRID CRYPTOGRAPHY ALGORITHMS IN CLOUD COMPUTING: A REVIEW," *15th Int. Conf. on Electronics, Computer and Computation (ICECCO)*, pp. 1–6, 2019.

[25] M. A. Al-Shabi, "A SURVEY ON SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY ALGORITHMS IN INFORMATION SECURITY," *International Journal of Scientific and Research Publications (IJSRP)*, vol. 9, no. 3, p. p8779, Mar. 2019, doi: 10.29322/ijsrp.9.03.2019.p8779.

[26] F. Bentil and I. Lartey, “CLOUD CRYPTOGRAPHY-A SECURITY ASPECT,” *International Journal of Engineering Research & Technology (IJERT)*, vol. 10, no. 05, pp. 448–450, 2021, [Online]. Available: http://aka.ms/mgmtcloud
[27] D. B. Ginting, “PERANAN ARITMETIKA MODULO DAN BILANGAN PRIMA PADA ALGORITMA KRIPTOGRAFI RSA,” *Media Informatika*, vol. 9, no. 2, pp. 48–57, 2010.
[28] V. C. Datey, “STEP FUNCTION MODEL FOR FORECASTING PROJECT CASH FLOW,” *International Journal of scientific research and management (IJSRM)* , vol. 3, no. 4, pp. 2812–2815, 2015, [Online]. Available: www.ijsrm.in
[29] D. R. Stinson and M. B. Paterson, CRYPTOGRAPHY THEORY AND PRACTICE FOURTH EDITION, Fourth Edition. Florida, United States: CRC Press, 2019.