Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/180411

On Rainbow Vertex Antimagic Coloring and Its Application to the Encryption Keystream Construction

Ika Hesti Agustin[1,2,*], *Dafik Dafik*[1,3], *Rosanita Nisviasari*[1], *Rifki Ilham Baihaki*[1], *Elsa Yuli Kurniawati*[1], *Sharifah Kartini Said Husain*[4,5], *and Vaishnavi Nagaraja*[4]

[1]PUI-PT Combinatorics and Graph, CGANT-University of Jember, 68121 Jember, Indonesia
[2]Department of Mathematics, University of Jember, 68121 Jember, Indonesia
[3]Department of Postgraduate Mathematics Education, University of Jember, 68121 Jember, Indonesia
[4]Institute for Mathematical Research, Universiti Putra Malaysia, Serdang, 40000 Selangor, Malaysia
[5]Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, Serdang, 40000 Selangor, Malaysia

Received: 7 Jan. 2024, Revised: 21 Mar. 2024, Accepted: 16 Apr. 2024
Published online: 1 Jul. 2024

Abstract: Let $G = (V,E)$ be a graph that is a simple, connected and un-directed graph. We now introduce a new notion of rainbow vertex antimagic coloring. This is a proper development of antimagic labeling with rainbow vertex coloring. The weight of a vertex $v \in V(G)$ under f for $f : E(G) \rightarrow \{1,2,\ldots,|E(G)|\}$ is $w_f(v) = \Sigma_{e\in E(v)} f(e)$, where $E(v)$ is the set of vertices incident to v. If each vertex has a different weight, afterwards the function f is also referred to as vertex antimagic edge labeling. If all internal vertices on the $u-v$ path have different edge weights for each vertex u and v, afterwards the path is assumed to be a rainbow path. The minimum amount of colors assigned over all rainbow colorings that result from rainbow vertex antimagic labelings of G is the rainbow vertex antimagic connection number of G, $rvac(G)$. For the purpose of trying to find some new lemmas or theorems about $rvac(G)$, we will prove the specific value of the rainbow vertex antimagic connection number of a specific family of graphs in this paper. Furthermore, based on our obtained lemmas and theorems, we use it for constructing an encryption keystream for robust symmetric cryptography. Moreover, to test the robustness of our model, we compare it with normal symmetric cryptography such as AES and DES.

Keywords: Rainbow vertex antimagic coloring, Encryption keystream construction, Symmetric cryptography

1 Introduction

A graph G is a pair of sets $(V(G),E(G))$ where $V(G)$ is a set of finite and non-empty vertices and $E(G)$ is a set of edges (edge) which may be empty of ordered pairs $\{u,v\}$ with dots $u,v \in V(G)$ [11]. The graph G is denoted by $G(V,E)$. So a graph must have at least one vertex and may not have edges [13]. One of the topics in graph theory is rainbow coloring [2]. There are many types of rainbow coloring, such as rainbow edge coloring, rainbow vertex coloring, and strong rainbow edge or vertex coloring [9].

Rainbow vertex antimagic coloring combines two concepts namely rainbow vertex connection and antimagic labeling [7]. The rainbow connection is first defined in [3]. A graph G is called a rainbow connection if there is at least one rainbow path from point u to point v [6]. Then, [8] developed the rainbow connection concept into two types, namely rainbow edge-connections and rainbow vertex-connections. Meanwhile, antimagic labeling or commonly called antimagic labeling was first introduced by Hartsfield and Ringel in 1990 [5].

Rainbow vertex antimagic coloring is a combination of rainbow vertex connections with antimagic labeling [7]. The f function is called antimagic edge labeling, if each point has a different weight. A path P on a graph G labeled as an edge is called a rainbow path if for any two points u and v, all interiors on the path $u-v$ have different weights [6]. The rainbow vertex antimagic connection number of graph G is denoted by $rvac(G)$, which is the smallest number of colors taken from all rainbow coloring induced by rainbow vertex antimagic labeling of graph G [10] .

Confidentiality, authentication, integrity, and non-repudiation are important are important cryptographic goals that needed to be achieved in a cryptosystem. Confidentiality helps authorized parties to

* Corresponding author e-mail: ikahesti.fmipa@unej.ac.id

keep information confidential. The purpose of confidentiality is to secure information so that it is not known by adversaries. A well-known method of sendty information secretly and secure is cryptography. Some applications of cryptography are to secure content distribution, improve digital rights management systems, solve security in mobile computing, etc. [12]. Two old encryption techniques are the Caesar cipher and the affine cipher. The development form of the Caesar cipher is the affine cipher. Affine block cipher uses an affine algorithm which is divided into blocks. The purpose of the affine algorithm is to generate [4] encryption and decryption.

Symmetric cryptography, also known as secret key or shared key cryptography, is a class of cryptographic algorithms that use a shared secret key for both encryption and decryption of information. In contrast, asymmetric cryptography uses different keys for encryption and decryption. In a monoalphabetic cipher, each letter in the plaintext is consistently replaced by a corresponding letter or symbol in the ciphertext. The substitution is based on a single fixed key or alphabet. Each occurrence of a particular character in the plaintext is replaced by the same character or symbol in the ciphertext throughout the encryption process. In contrast, in a polyalphabetic cipher, the substitution of letters is not based on a single fixed key or alphabet. Instead, multiple alphabets or keys are used during the encryption process. The key typically consists of a keyword or phrase that determines which alphabet or set of rules to use for each letter in the plaintext.

In this paper, we develop a research by applying rainbow vertex antimagic coloring as a cryptosystem. We apply rainbow vertex antimagic coloring to ladder graph and composition graph as an affine block cipher key. This key grows with the number of characters in the plaintext. To obtain the key, we need to find the function of rainbow vertex antimagic coloring in ladder graph and composition graph. To test the performance of this encryption method, we compare it with other symmetric type methods such as AES and DES. Below are some definitions and theorems used in the process of finding the function.

Definition 1 *Ladder graph (L_n) is an undirected graph and is a planar graph with point cardinality $2n$ and edge cardinality $3n-2$.*

Definition 2 *Composition graph is a graph that is built by graphs P_n and P_1 with disjoint sets of points $V(P_n)$ and $V(P_1)$ and edges E_1 and E_2. A Composition graph is a graph where $V(P_n) \times V(P_1)$ and $v = (v_1, v_2, ..., v_n)$ are adjacent to $u = (u_1, u_2)$ when $[v_1 adj u_1]$ or $[v_1 = u_1$ and $v_2 adj u_2]$ and so on. Composition graph is denoted by $P_n[P_2]$.*

Theorem 1 *Suppose G is a connected graph with rest(G), then $rvc(G) \geq still(G) - 1$.*

Lemma 1 *[1] The rainbow vertex connection number of the ladder graph $rvc(L_n)$ is $n-1$.*

2 Research Methods

Figure 1 shows the flow that we used in this research. There are three steps in this research: (1) Considering the rainbow vertex antimagic coloring labels on ladder graphs and composition graphs, (2) Taking the labeling results as keystream, (3) applying the keystream in a modified affine block cipher. At the third step, the plaintext is divided into four blocks and performs the vigenere cipher operation. Each encryption and decryption algorithm can be seen in Algorithm 1 and Algorithm 2.

Algorithm 1. Encryption using RVAC of Graph

```
Input: plain text, P
Output: cipher text, C
1.Start
2.Input P
3.Define size length P as s
4.Define size of graph as n using ⌈s/2⌉
5.Define the keystream from rainbow
  vertex antimagic coloring of graph
6.Define the order of alphabetical P
7.Define length of keystream
8.Implementation of affine cipher
  method
  Block 1 ⟶ C1 = (keystream + block
  1) mod 94
  Block 2 ⟶ C2 = (keystream + block
  2) mod 94
  Block 3 ⟶ C3 = (keystream + block
  3) mod 94
  Block 4 ⟶ C4 = (keystream + block
  4) mod 94
9.Combine every C in each block to
  obtain the cipher text
```

Algorithm 2. Decryption using RVAC of Graph

```
Input: cipher text, C
Output: plain text, P
1.Start
2.Input C
3.Define size length C as s
4.Define size of graph as n using ⌈s/2⌉
5.Define the keystream from rainbow
  vertex antimagic coloring of graph
6.Define the order of alphabetical C
7.Define length of keystream
8.Implementation of affine plain text
  method
  Block 1 ⟶ Block 1 = (C1 -
  keystream) mod 94
  Block 2 ⟶ Block 2 = (C2 -
  keystream) mod 94
  Block 3 ⟶ Block 3 = (C3 -
  keystream) mod 94
  Block 4 ⟶ Block 4 = (C4 -
  keystream) mod 94
```

```
9.Combine every P in each block to
  obtain the plain text
```

3 Research Findings

We obtained the new theorems regarding the rainbow vertex antimagic connection number. The graphs studied are ladder (L_n) and composition of path graph ($P_n[P_2]$). To prove the theorems of rainbow vertex antimagic connection number, we need theorem rainbow vertex connection number as lower bound.

Theorem 2 *Let $P_n[P_2]$ be a composition of path graph. For every positive integer $n \geq 3$, $rvc(P_n[P_2]) = n-2$*

Proof. The composition of path graph $P_n[P_2]$ is a connected graph with vertex set $V(P_n[P_2]) = \{a_j; 1 \geq j \geq n\} \cup \{b_j; 1 \geq j \geq n\}$ and edge set $E(P_n[P_2]) = \{a_j a_{j+1}; 1 \geq j \geq n-1\} \cup \{b_j b_{j+1}; 1 \geq j \geq n-1\} \cup \{a_j b_j; 1 \geq j \geq n\} \cup \{a_j b_{j+1}; 1 \geq j \geq n-1\} \cup \{a_{j+1} b_j; 1 \geq j \geq n-1\}$. The diameter of composition of path graph is $n-1$ and based on Lemma 1, we have $rvac(P_n[P_2]) \geq n-2$ as lower bound. We determine the upper bound of $rvac(P_n[P_2])$ by function of vertex colors as follows.

$$f(a_j)=\begin{cases} 1, & ; j=1,n \\ j-1, & ; 2 \leq j \leq n-1 \end{cases}$$

$$f(b_j)=\begin{cases} 1, & ; j=1,n \\ j-1, & ; 2 \leq j \leq n-1 \end{cases}$$

Since every vertex $u \in V(P_n[P_2])$ is assigned with a color, then internal vertices for every two different vertices have different weights. For more detail, it can be seen Table 1. Suppose that $u, u' \in V(P_n[P_2])$, there are five cases of rainbow paths in $P_n[P_2]$ as follows.

From the Table 1, we can concludes that the graph $P_n[P_2]$ has rainbow vertex antimagic coloring. Thus, we obtain $rvc(P_n[P_2]) = n-2$. □

Theorem 3 *Let L_n be a ladder graph. For every positive integer $n \geq 3$,*

$$rvac(L_n) = \begin{cases} n, & \text{for } n \text{ is odd} \\ n+1, & \text{for } n \text{ is even.} \end{cases}$$

Proof. The ladder graph L_n is a connected graph with vertex set $V(L_n) = \{a_j; 1 \geq j \geq n\} \cup \{b_j; 1 \geq j \geq n\}$ and edge set $E(L_n) = \{a_j a_{j+1}; 1 \geq j \geq n-1\} \cup \{b_j b_{j+1}; 1 \geq j \geq n-1\} \cup \{a_j b_j; 1 \geq j \geq n\}$. The diameter of ladder graph is n and based on Lemma 1, we have $rvac(L_n) \geq n-1$ as lower bound. We determine the upper bound of $rvac(L_n)$ by bijection function of edge labels in two cases.

Case 1. For n is even.

$$f(a_j b_j) = \begin{cases} 2n-1-j, & \text{for } 1 \leq j \leq n-1 \\ 2n-1, & \text{for } j = n \end{cases}$$

$$f(a_j a_{j+1}) = \begin{cases} 2n+j, & \text{for } 1 \leq j \leq n-2 \\ 2n, & \text{for } j = n-1 \end{cases}$$

$$f(b_j b_{j+1}) = \begin{cases} \frac{n-1+j}{2}, & \text{for } 1 \leq j \leq n-1, \ j \text{ is odd} \\ \frac{j}{2}, & \text{for } 1 \leq j \leq n-2, \ j \text{ is even} \end{cases}$$

We can determined the vertex weight from the edge label above, such that the function of vertex weight as follows.

$$w(a_j) = \begin{cases} 4n-1, & \text{for } j = 1, n \\ 6n+j-2, & \text{for } 2 \leq j \leq n-2 \\ 6n-2, & \text{for } j = n-1 \end{cases}$$

$$w(b_j) = \begin{cases} \frac{5n-4}{2}, & \text{for } 1 \leq j \leq n-1 \\ 3n-2, & \text{for } j = n \end{cases}$$

Case 2. For n is odd.

$$f(a_j b_j) = \begin{cases} 2n-1-j, & \text{for } 1 \leq j \leq n-1 \\ 2n-1, & \text{for } j = n \end{cases}$$

$$f(a_j a_{j+1}) = \begin{cases} 2n+j, & \text{for } 1 \leq j \leq n-2 \\ 2n, & \text{for } j = n-1 \end{cases}$$

$$f(b_j b_{j+1}) = \begin{cases} \frac{n+j}{2}, & \text{for } j \text{ is odd} \\ \frac{j}{2}, & \text{for } j \text{ is even} \end{cases}$$

And the function of vertex weight as follows.

$$w(a_j) = \begin{cases} 4n-1, & \text{for } j = 1, n \\ 6n+j-2, & \text{for } 2 \leq j \leq n-2 \\ 7n-3-j, & \text{for } j = n-1 \end{cases}$$

$$w(b_j) = \frac{5n-3}{2}, \text{ for } 1 \leq j \leq n$$

Based on the function of vertex weight, we get the vertex weight set $W(L_n) = \{\frac{5n-3}{2}, 4n-1, 6n-2, 6n, 6n+1, 6n+2, \ldots, 7n-5, 7n-4\}$ for n is odd and $W(L_n) = \{\frac{5n-4}{2}, 3n-2, 4n-1, 6n-2, 6n, 6n+1, 6n+2, \ldots, 7n-5, 7n-4\}$ for $n+1$ is even. The cardinality of vertex weight set is $|W(L_n)| = n+1$. Hence, ladder graph has $n+1$ different weights. Since every vertex $u \in V(L_n)$ is assigned with the color $w(u)$, then internal vertices for every two different vertices have different weights. For more detail, it can be seen Table 2. Suppose that $u, u' \in V(L_n)$, the following are five cases of rainbow paths in L_n.

From the Table 2, we can concludes that the graph L_n is rainbow vertex antimagic coloring. Thus, we obtain $rvac(L_n) = n+1$ for n is even and $rvac(L_n) = n$ for n is odd. □

Theorem 4 *Let $P_n[P_2]$ be a composition of path graph. For every positive integer $n \geq 3$, $rvac(P_n[P_2]) =$*

$$rvac(P_n[P_2])=\begin{cases} n+1, & for\ n = 3,4 \\ n+2, & for\ n \geq 5 \end{cases}$$

Proof. The composition of path graph $P_n[P_2]$ is a connected graph with vertex set $V(P_n[P_2]) = \{a_j; 1 \geq j \geq n\} \cup \{b_j; 1 \geq j \geq n\}$ and edge

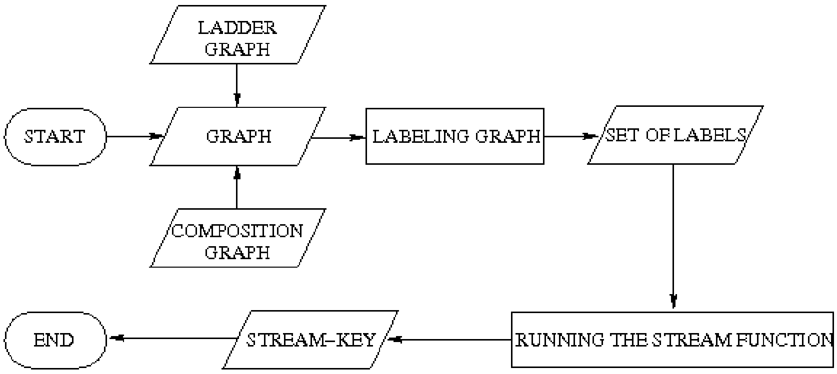

Fig. 1: A model of keystream generation from graph labeling.

Table 1: The Rainbow Vertex of $u-u'$ Path in $P_n[P_2]$.

Case	u	u'	Rainbow Vertex Coloring $u-u'$	Condition
1	a_i	a_j	$a_i,a_{i+1},a_{i+2},\ldots,a_{j-2},a_{j-1},a_j$	$i<j$
2	b_i	b_j	$b_i,b_{i+1},b_{i+2},\ldots,b_{j-2},b_{j-1},b_j$	$i<j$
3	a_i	b_j	$a_i,a_{i+1},a_{i+2},\ldots,a_{j-2},a_{j-1},,b_j$	$i<j$
4	a_i	b_j	a_i,b_j	$i=j$
5	a_i	b_j	$a_i,a_{i-1},a_{i-2},\ldots,a_{j+2},a_{j+1},b_j$	$i>j$

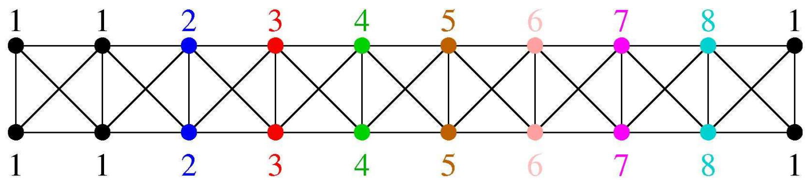

Fig. 2: Rainbow Vertex Coloring $P_{10}[P_2]$ is 8.

set $E(P_n[P_2]) = \{a_ja_{j+1}; 1 \geq j \geq n-1\} \cup \{b_jb_{j+1}; 1 \geq j \geq n-1\} \cup \{a_jb_j; 1 \geq j \geq n\} \cup \{a_jb_{j+1}; 1 \geq j \geq n-1\} \cup \{a_{j+1}b_j; 1 \geq j \geq n-1\}$. The diameter of composition of path graph is $n-1$ and based on Lemma 1, we have $rvac(P_n[P_2]) \geq n-2$ as lower bound. We determine the upper bound of $rvac(P_n[P_2])$ by bijection function of edge labels in two cases.

Case 1. For $n = 3,4$.

Based on the bijection function of edge labels and the function of vertex weight on figure above, we get the vertex weight set $W(P_3[P_2]) = \{16,17,18,32\}$ and $W(P_4[P_2]) = \{21,23,27,42,47\}$. The cardinality of vertex weight set is $|W(P_n[P_2])| = n+1$. Hence, composition of path graph has $n+1$ different weights.

Case 2. For $n \geq 5$.

$f(a_jb_j) = 2n+j-3$; for $1 \geq j \geq n$

$$f(a_ja_{j+1}) = \begin{cases} \frac{9n-7}{2}+j, \text{ for } 1 \leq j \leq \frac{n-1}{2}, \\ \quad n \text{ is odd} \\ \frac{9n-8}{2}+j, \text{ for } 1 \leq j \leq \frac{n}{2}, \\ \quad n \text{ is even} \\ \frac{7n-5}{2}+j, \text{ for } \frac{n+1}{2} \leq j \leq n-1, \\ \quad n \text{ is odd} \\ \frac{7n-6}{2}+j, \text{ for } \frac{n+2}{2} \leq j \leq n-1, \\ \quad n \text{ is even} \end{cases}$$

$$f(b_jb_{j+1}) = \begin{cases} \frac{j}{2}, & \text{for } j \equiv 0 \bmod 2 \\ \frac{n+j}{2}, & \text{for } j \equiv 1 \bmod 2, \\ & n \text{ is odd} \\ \frac{n+j-1}{2}, & \text{for } j \equiv 1 \bmod 2, \\ & n \text{ is even} \end{cases}$$

$f(a_jb_{j+1}) = 4n-j-3$; for $1 \geq j \geq n-1$

$$f(a_{j+1}b_j) = \begin{cases} 4n-3, & \text{for } j=1 \\ 2n-j-1, & \text{for } 2 \leq j \leq n-1 \end{cases}$$

Table 2: The Rainbow Vertex of $u-u'$ Path in L_n.

Case	u	u'	Rainbow Vertex Coloring $u-u'$	Condition
1	a_i	a_j	$a_i, a_{i+1}, a_{i+2}, \ldots, a_{j-2}, a_{j-1}, a_j$	$i<j$
2	b_i	b_j	$b_i, b_{i+1}, b_{i+2}, \ldots, b_{j-2}, b_{j-1}, b_j$	$i<j$
3	a_i	b_j	$a_i, a_{i+1}, a_{i+2}, \ldots, a_{j-2}, a_{j-1}, a_j, b_j$	$i<j$
4	a_i	b_j	a_i, b_j	$i=j$
5	a_i	b_j	$a_i, a_{i-1}, a_{i-2}, \ldots, a_{j+2}, a_{j+1}, a_j, b_j$	$i>j$

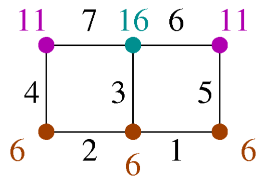

Fig. 3: Rainbow Vertex Antimagic Coloring on L_3

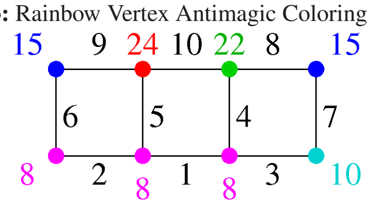

Fig. 4: Rainbow Vertex Antimagic Coloring on L_4

We can determined the vertex weight from the edge label above, such that the function of vertex weight as follows.

$$w(a_j)=\begin{cases}\frac{21n-17}{2}, & \text{for } j=1,\ n \text{ is odd}\\ \frac{21n-18}{2}, & \text{for } j=1,\ n \text{ is even}\\ 19n-13, & \text{for } j=2,\ n \text{ is odd}\\ 19n-14, & \text{for } j=2,\ n \text{ is even}\\ 17n+j-14, & \text{for } 3\le j\le \frac{n-1}{2},\ n \text{ is odd}\\ 17n+j-15, & \text{for } 3\le j\le \frac{n}{2},\ n \text{ is even}\end{cases}$$

$$w(a_j)=\begin{cases}\frac{33n-25}{2}, & \text{for } j=\frac{n+1}{2},\ n \text{ is odd}\\ \frac{33n-26}{2}, & \text{for } j=\frac{n+2}{2},\ n \text{ is even}\\ 15n+j-12, & \text{for } \frac{n+3}{2}\ge j\ge n-1,\ n \text{ is odd}\\ 15n+j-13, & \text{for } \frac{n+4}{2}\ge j\ge n-1,\ n \text{ is even}\end{cases}$$

$$w(a_n)=\begin{cases}\frac{17n-13}{2}, & n \text{ is odd}\\ \frac{17n-14}{2}, & n \text{ is even}\end{cases}$$

$$w(b_1)=\begin{cases}\frac{13n-9}{2}, & n \text{ is odd}\\ \frac{13n-10}{2}, & n \text{ is even}\end{cases}$$

$$w(b_j)=\begin{cases}\frac{17n-13}{2}, & \text{for } 2\le j\le n-1,\ n \text{ is odd}\\ \frac{17n-14}{2}, & \text{for } 2\le j\le n-1\ n \text{ is even}\end{cases}$$

$$w(b_n)=\begin{cases}\frac{13n-11}{2}, & n \text{ is odd}\\ 7n-6, & n \text{ is even}\end{cases}$$

Based on the function of vertex weight, we get the vertex weight set $W(P_n[P_2]) = \{\frac{13n-11}{2}, \frac{13n-9}{2}, \frac{17n-13}{2}, \frac{21n-17}{2}, \frac{31n-21}{2}, \frac{31n-19}{2}, \frac{31n-17}{2}, \ldots, 16n-13, \frac{33n-25}{2}, 17n-11, 17n-10, \ldots, \frac{35n-29}{2}, 19n-13\}$ for n is odd and $W(P_n[P_2]) = \{\frac{13n-10}{2}, 7n-6, \frac{17n-14}{2}, \frac{21n-18}{2}, \frac{31n-22}{2}, \frac{31n-20}{2}, \frac{31n-18}{2}, \ldots, 16n-14, \frac{33n-26}{2}, 17n-10, 17n-11, \ldots, \frac{35n-30}{2}, 19n-14\}$ for n is even. The cardinality of vertex weight set is $|W(P_n[P_2])| = n+2$. Hence, composition of path graph has $n+2$ different weights.

Since every vertex $u \in V(P_n[P_2])$ is assigned with the color $w(u)$, then internal vertices for every two different vertices have different weights. For more detail, it can be seen Table 3. Suppose that $u, u' \in V(P_n[P_2])$, there are five cases of rainbow paths in $P_n[P_2]$. There are as follows.

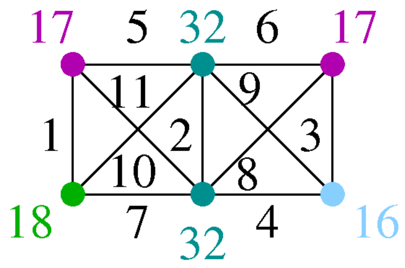

Fig. 5: Rainbow Vertex Antimagic Coloring on $P_3[P_2] = 4$

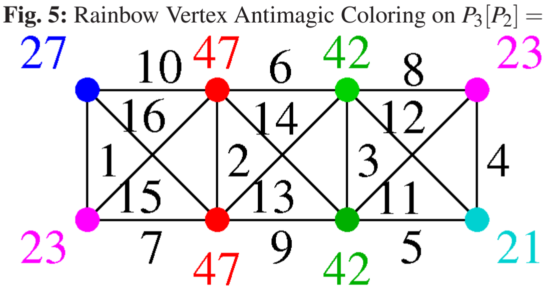

Fig. 6: Rainbow Vertex Antimagic Coloring on $P_4[P_2] = 5$

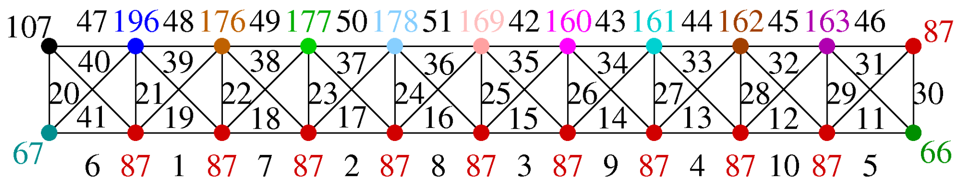

Fig. 7: Rainbow Vertex Antimagic Coloring on $P_{11}[P_2] = 13$

Table 3: The Rainbow Vertex of $u - u'$ Path of $P_n[P_2]$.

Case	u	u'	Rainbow Vertex Coloring $u - u'$	Condition
1	a_i	a_j	$a_i, a_{i+1}, a_{i+2}, \ldots, a_{j-2}, a_{j-1}, a_j$	$i < j$
2	b_i	b_j	$b_i, b_{i+1}, b_{i+2}, \ldots, b_{j-2}, b_{j-1}, b_j$	$i < j$
3	a_i	b_j	$a_i, a_{i+1}, a_{i+2}, \ldots, a_{j-2}, a_{j-1}, b_j$	$i < j$
4	a_i	b_j	a_i, b_j	$i = j$
5	a_i	b_j	$a_i, a_{i-1}, a_{i-2}, \ldots, a_{j+2}, a_{j+1}, b_j$	$i > j$

From the Table 3, we can concludes that the graph $P_n[P_2]$ is rainbow vertex antimagic coloring. Thus, we obtain $rvac(P_n[P_2]) = n+1$ for $n = 3,4$ and $rvac(P_n[P_2]) = n+2$ for $n \geq 5$. □

4 Results and Disscusion

4.1 Constructed Key

In this research, the modification of the affine block cipher lies in the order of the block selection. Illustrations of the encryption process can be seen in Figures 6 and 7.

There are two process that we carried out in building this cryptosystem, namely the encryption process and the decryption process. An illustration of the encryption process is shown in Table 4. In this table we use the plaintext ”CGANTUNEJ”. The plaintext is converted into number representation of each letter based on (mod 26). The key that we use is obtained from the RVAC labeling of a ladder graph with $n = 10$. Then we add P_i to K to produce a cipherext character (C_i). To generate ciphertext we use mod 26 on C_i.

The illustration of the encryption process is shown in Table 4. It shows the result of the encryption process is ”EJGWBZUON”. The chipertext is converted into number representation of each letter based on (mod 26). The key

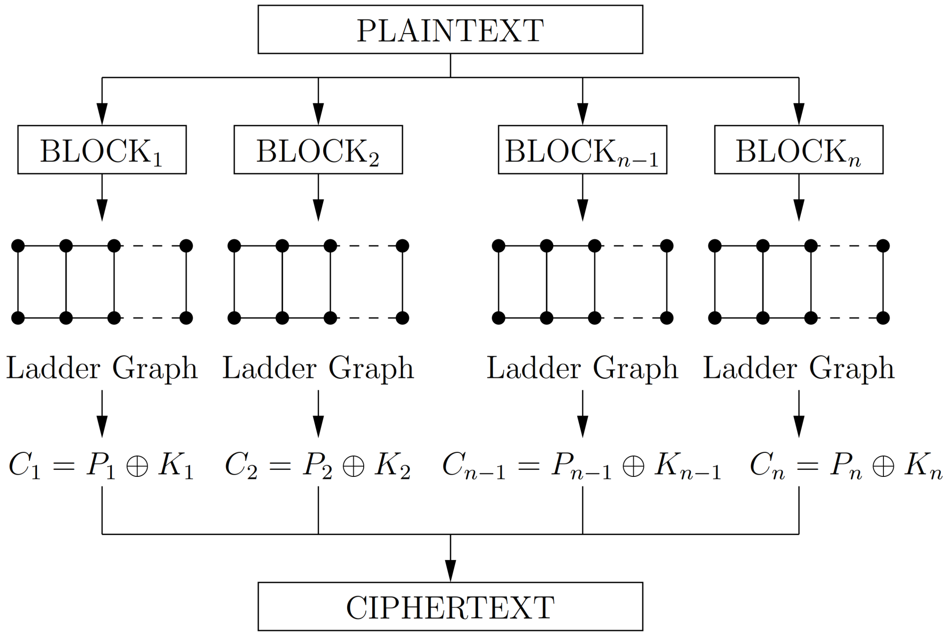

Fig. 8: Encryption Process by using Ladder graph

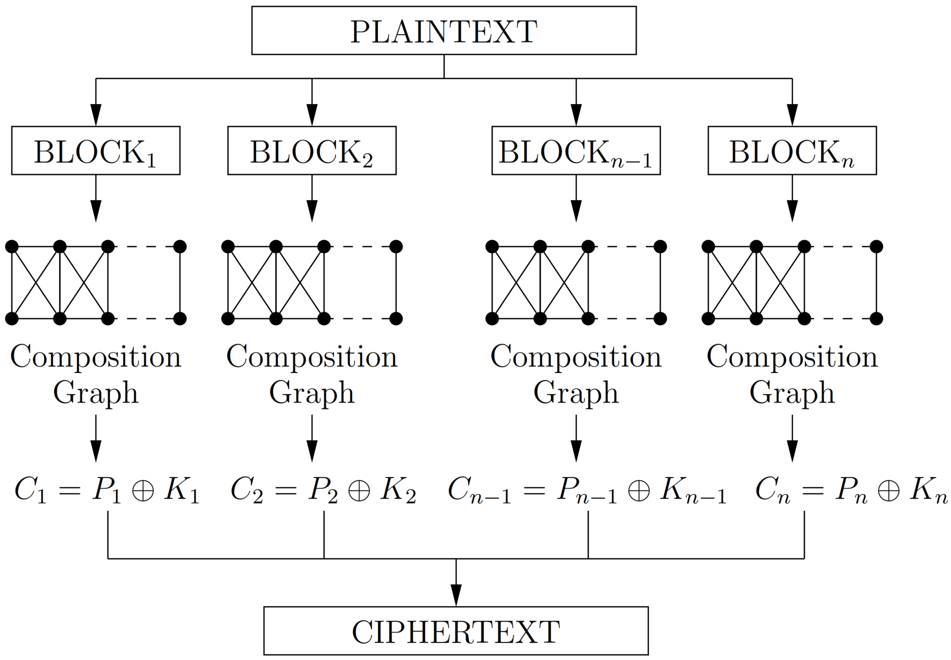

Fig. 9: Encryption Process by using Composition graph

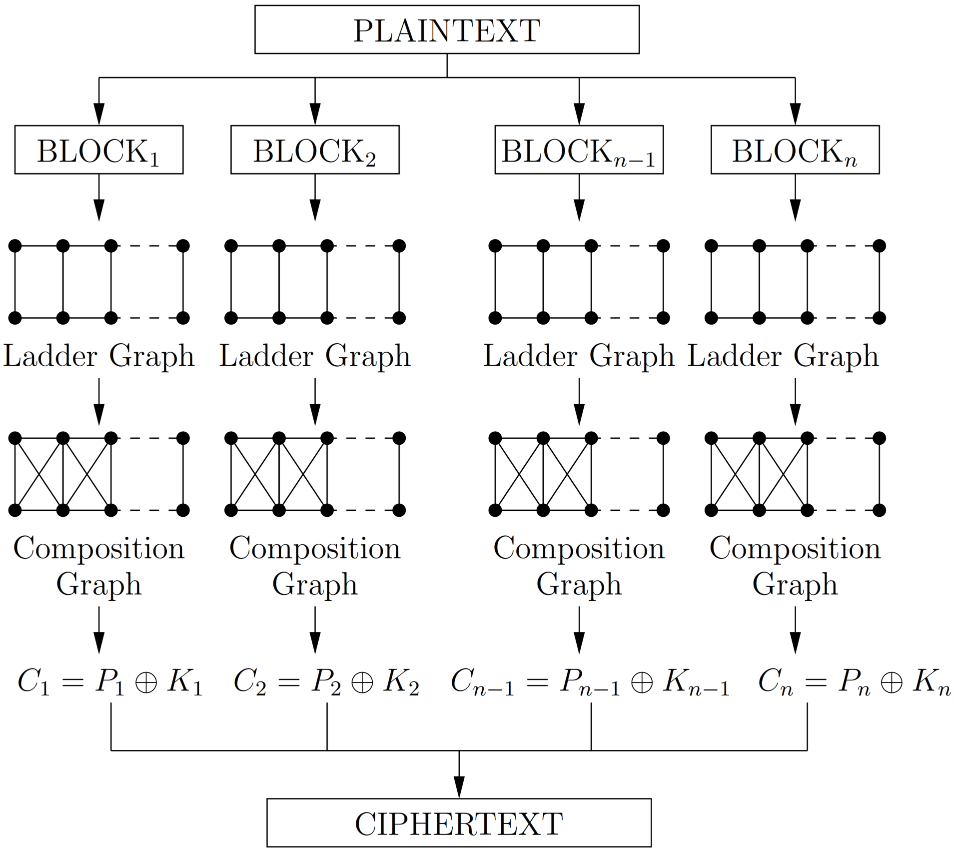

Fig. 10: Encryption Process by using Ladder and Composition graph

Table 4: Illustration of Encryption with Modified Affine Block Cipher Algorithm

P	C	G	A	N	T	U	N	E	J
P_i	2	6	0	13	19	20	13	4	9
K	2	3	6	9	8	5	7	10	4
C_i	4	9	6	22	27	25	20	14	13
C	E	J	G	W	B	Z	U	O	N

Table 5: Illustration of Decryption with Modified Affine Block Cipher Algorithm

C	E	J	G	W	B	Z	U	O	N
C_i	4	9	6	22	27	25	20	14	13
K	2	3	6	9	8	5	7	10	4
P_i	2	6	0	13	19	20	13	4	9
P	C	G	A	N	T	U	N	E	J

that we use is obtained from the RVAC labeling of a ladder graph with $n = 10$. Then we subtract C_i and K to produce a cipher (C_i). To generate ciphertext we use mod 26 on C_i.

4.2 Brute Force Attack

Brute force attacks are aimed at finding key combinations of all possibilities. We assume each key search results in 10^{-5} time. Brute force looks for possible key combinations by generating random numbers ranging from 1 to 76. There are $\frac{n!}{r!(n-r)!}$ possible key combinations that appear. After more than 24 hours and no keystream can be found, the system will automatically lock and the message will be blocked for decryption.

4.3 Applying the Modified Robustness Cryptosystem

We compared the performance of our proposed robust cryptosystem with Advanced Encryption System (AES) and Data Encryption System (DES). The performance

Table 6: Comparison of Encryption Result Size (bytes)

	Ciphertext Length					
Encryption Type	16 bytes	32 bytes	64 bytes	128 bytes	256 bytes	512 bytes
Graph (Ladder and Composition)	191	210	239	342	399	470
AES	48	64	80	192	256	352
DES	32	48	72	176	248	336

Table 7: Comparison of Encryption Process Runtime (seconds)

	Encryption Length					
Encryption Type	16 bytes	32 bytes	64 bytes	128 bytes	256 bytes	512 bytes
Graph (Ladder and Composition)	0.0013	0.0017	0.0025	0.0035	0.0034	0.0040
AES	0.0019	0.0025	0.0029	0.0032	0.0039	0.0040
DES	0.0010	0.0019	0.0022	0.0033	0.0035	0.0039

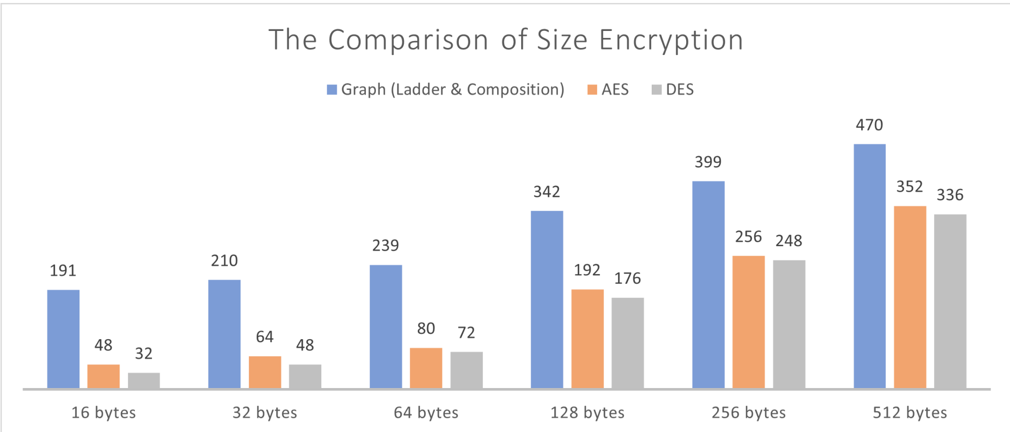

Fig. 11: The Comparison of Size Encryption

comparison that we use is the size of the ciphertext and the runtime of the encryption process. The purpose of this comparison is to examine the complexity of our proposed algorithm when compared to existing cryptosystem methods. Algorithm complexity can be divided into two types, namely storage space complexity and time complexity. We use several test scenarios with plaintext sizes of 16 bytes, 32 bytes, 64 bytes, 256 bytes, and 512 bytes. The purpose of this experiment is to see the effect of encryption when using increasing bytes length.

The comparison of the ciphertext size of the robust cryptosystem algorithm that we propose with other algorithms can be seen in Table 6. Based on Table 6, it can be seen that the size of the encryption results of the algorithm that we propose is larger than AES and DES. In this comparison the DES algorithm has the smallest ciphertext. This is possible because the key size for our proposed robust cryptosystem algorithm follows the length of the plaintext. So that during the encryption process there is a size that exceeds the existing standards. More detail we also show this comparison in Figure 9.

The next comparison is from the time it takes to run the algorithm. We present the results of this comparison in Table 7. Based on the table it can be seen that the robust cryptosystem algorithm that we propose can compete with AES and DES. Even in some conditions the algorithm that we propose can outperform the AES and DES algorithms. These results indicate that in terms of

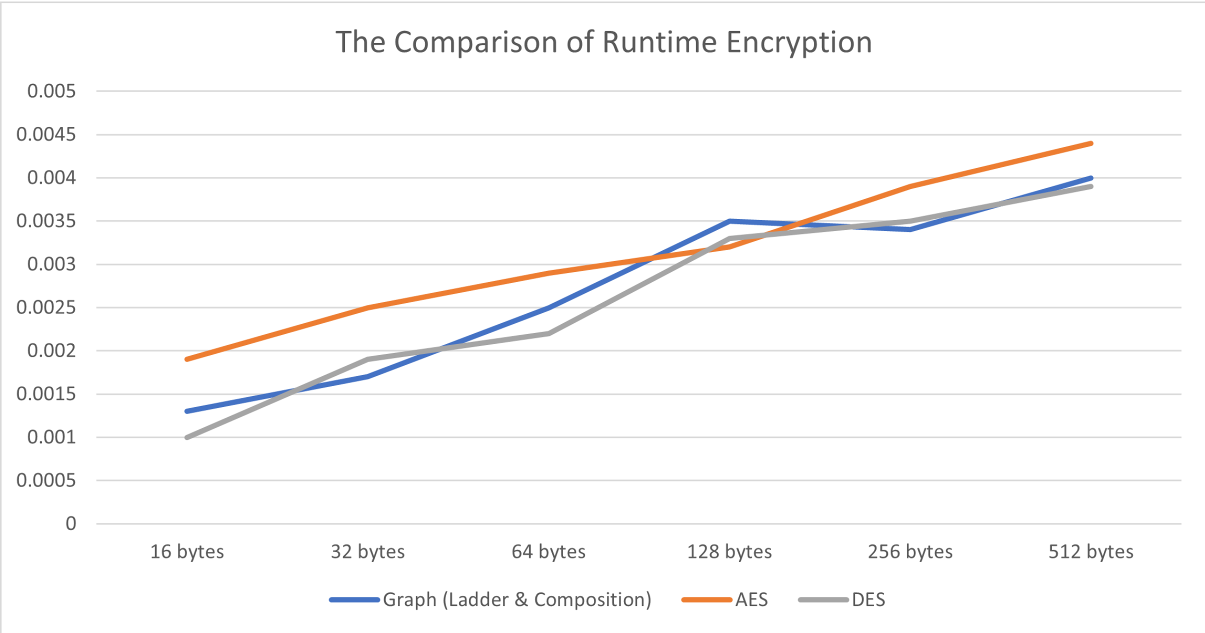

Fig. 12: The Comparison of Runtime Encryption

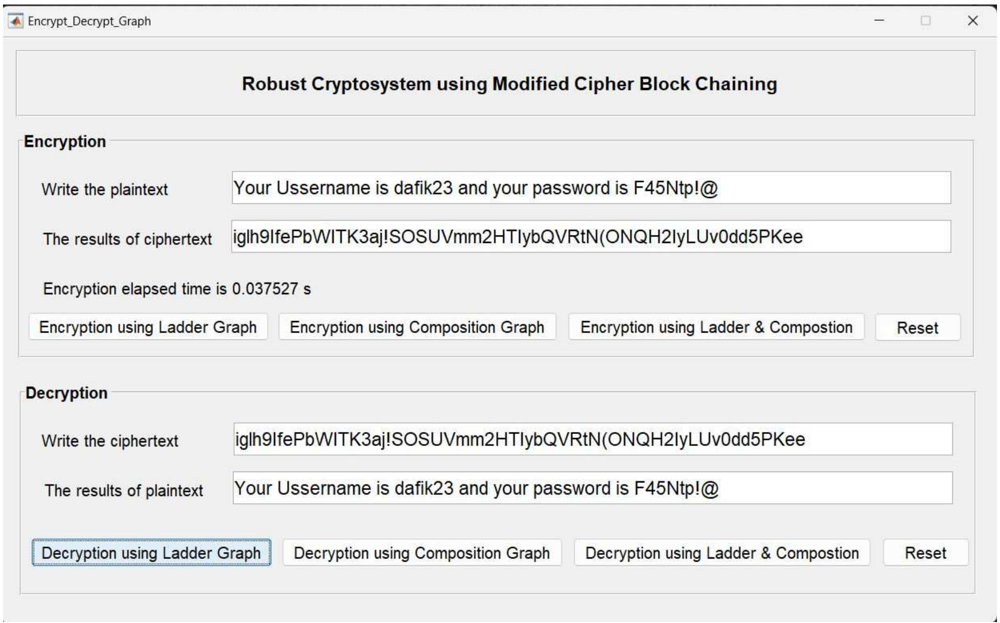

Fig. 13: On MATLAB GUI of the RAC and VC algorithm combination

the required time complexity the algorithm we propose is efficient. In more detail, we also show this comparison in Figure 10. We also design our proposed algorithm using a graphical user interface (GUI) as shown in Figure 11.

5 Conclusion

We have implemented the concept of rainbow vertex antimagic coloring (RVAC) on keystream construction of cryptography. The results show that the combination between rainbow antimagic coloring and vegenere chipper algorithm gives a robust encryption key construction. The advantage of this method is that the length of the keystream can be adjusted by the length of plaintext. We tested several RAC of graphs of any order, the results show that the edge colors of RAC can be used for modified block affine chipper, and this algorithm has competed with the standard symmetric encryption, namely Data Encryption Standard (DES), Advanced Encryption Standard (AES).

The challenging future work of integrating strong cryptography based on graph labeling with established symmetric encryption algorithms such as AES and DES can provide a balanced and comprehensive solution for securing information. This hybrid approach takes advantage of the efficiency and industry acceptance of AES and DES while incorporating the unique security features provided by graph labeling. The result is a more robust and adaptable cryptographic system suitable for a wide range of applications where security and efficiency are important considerations.

Acknowledgement

I gratefully acknowledge from the support of PUI-PT Combinatoric and Graph, CGANT-Universitas Jember, International Collaborative Research Grant, LP2M-Universitas Jember, and Institute for Mathematical Research, Universiti Putra Malaysia, Serdang, Selangor, Malaysia, for the research collaboration of the year 2024.

References

[1] Arputhamary, I. A. and Mercy, M. H. 2015. Rainbow Coloring of Some Ladder Graphs. Global Journal of Pure and Applied Mathematics. Vol 11. No. 3. pp. 1231-1240.

[2] Budi, H. S., Dafik, Tirta, I. M., and Kristiana, A. I. 2021. "On Rainbow Antimagic Coloring of Graphs". *Journal of Physics: Conference Series*. Vol. 1832, No. 1.

[3] Chartrand, G., G. L. Johns, K. A. Mcjeon, dan P. Zhang. 2008. Rainbow Connection in Graphs. Math Bohemia. 133:85-98.

[4] Dafik, Nisviasari, R., Maryati, T. K., I. H. Agustin, and Venkatachalam, M. 2021. "On Local Super Antimagic Total Face Coloring and The Application in Developing a Cipher Block Chaining Key". *International Journal of Electrical and Computer Engineering (IECE)*. Vol. 12. No. 4. pp. 33960-3969.

[5] Hartsfield, N. dan G. Ringel. 1990. Pearls in Graph Theory. London: Academic Press, Inc.

[6] Hikamuddin, A. M., Dafik, Prihandini, R. M. 2022. "Rainbow Vertex Antimagic Coloring 2-Connection pada Keluarga Graf Tangga". *CGANT Journal of Mathematics and Applications*, Vol. 3, No. 2, pp. 58-69.

[7] Joedo, J. C., Kristiana, A. I., Agustin, I. H., and Nisviasari, R. 2022. On The Rainbow Antimagic Coloring of Vertex Amalgamation of Graphs. *Journal of Physics: Conference Series*. Vol. 2157. No. 1.

[8] Kriveleich, M. dan R. Yuster. 2009. The Rainbow Connection of Graph is (at most) Reciprocal to Its Minimum Degree. IWOCA. 5874:432-437.

[9] Lestari, W. Dafik, Susanto, and Wahab, A. Z. 2023. "On The Strong Rainbow Antimagic Coloring of Some Special Graph". *Atlantis Press Series: Advanced in Physics Research*. Vol. 6. pp. 61 - 72.

[10] Marsidi, Agustin, I. H., Dafik, and Kurniawati, E. Y. 2021. "On Rainbow Vertex Antimagic Coloring of Graphs A New Notion". *CAUCHY*, Vol. 7, pp. 64-72.

[11] Mursyidah, I. L., Dafik, Kristiana, A. I., Agustin, I. H., Maylisa, I. N., and Alfarisi, R. 2023. "On Rainbow Antimagic Coloring of Some Classes of Graph". *Atlantis Press Series: Advanced in Physics Research*. Vol. 6. pp. 73 - 93.

[12] Prihandoko, A. C., Dafik, and I. H. Agustin. 2022. "Stream-Keys Generation Based on Graph Labeling for Strengthening Vigenere Encryption". *International Journal of Electrical and Computer Engineering (IECE)*. Vol. 12. No. 4. pp. 33960-3969.

[13] Septory, B. J., Utoyo, M. I., Dafik, Sulistiyono, B., and Agustin, I. H. 2021. "On Rainbow Antimagic Coloring of Special Graphs". *International Journal of Electrical and Computer Engineering (IECE)*. *Journal of Physics: Conference Series*. Vol. 1836, No. 1.

Ika Hesti Agustin completed her doctorate in graph theory at Universitas Airlangga, Indonesia in 2022. She is senior lecturer at Department of Mathematics, Faculty of Mathematics and Science, University of Jember. She is the secretary of PUI-PT Combinatorics and Graph, University of Jember, Indonesia. Her current research include graph theory, mathematics and applied mathematics. She is referee for several local and international journals in the frame of mathematics. She is a member of Indonesian Combinatorial Society (InaCombS).

Dafik Dafik is a professor on combinatorics, graph theory, and combinatorial education from University of Jember in 2013. He completed his doctorate in combinatorics and graph theory at University of Ballarat, Australia in 2007. He is senior lecturer at Department of Postgraduate Mathematics Education, University of Jember. He is the chairman of PUI-PT Combinatorics and Graph, University of Jember, Indonesia. Her current research include graph theory, mathematics education and applied mathematics. He is referee for several local and international journals in the frame of applied mathematics. He is a member of Indonesian Combinatorial Society (InaCombS).

Rosanita Nisviasari is a research assistant in PUI-PT Combinatorics and Graph of University of Jember, Indonesia. She completed her master in combinatorics and graph theory at University of Jember, Indonesia in 2020. Her current research include graph theory, combinatorics and applied mathematics.

Rifki Ilham Baihaki is a research assistant in PUI-PT Combinatorics and Graph of University of Jember, Indonesia. He completed his master in deep learning and computer vision at Sepuluh Nopember of Institute Technology, Surabaya, Indonesia in 2022. Her current research include graph neural network, convolutional neural network, cryptography and applied mathematics.

Elsa Yuli Kurniawati is a research assistant in PUI-PT Combinatorics and Graph of University of Jember, Indonesia. She completed her master in combinatorics and graph theory at University of Jember, Indonesia in 2018. Her current research include graph theory, combinatorics and applied mathematics.

Sharifah Kartini Said Husain completed her doctorate in Algebra at Universiti Putra Malaysia (UPM), Malaysia in 2011. She is senior lecturer at Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia (UPM). She is currently the head of Laboratory Cryptology, Analysis and Structure, Institute For Mathematical Research (INSPEM), UPM. Her current research include algebra (Leibniz algebra), graph theory, mathematics education and etnomathematics. She is Editor of Malaysian Journal of Mathematical Sciences(MJMS) and member of editorial team of Jurnal Sains Indonesia (JSI). She is referee for several local and international journals in the frame of pure mathematics. She is a member of the Malaysian Mathematical Sciences Society (PERSAMA).

Vaishnavi Nagaraja received the B.S. degree in mathematics from Universiti Putra Malaysia, Malaysia, in 2021. She is currently pursuing the Ph.D. degree in mathematical cryptography with the Institute for Mathematical Research, Universiti Putra Malaysia. Her current research interests include post-quantum cryptography, specifically in code-based cryptography, symmetric and asymmetric cryptography, and coding theory. She is a member of the Malaysian Society of Cryptology Research (MSCR).