STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **13**, May 2025, pp 1984–1999.
Published online in International Academic Press (www.IAPress.org)

A Robust Algorithm for Asymmetric Cryptography Using Rainbow Vertex Antimagic Coloring

Kiswara Agung Santoso[1,2,*], Indah Lutfiyatul Mursyidah[1], Ika Hesti Agustin[1,2], Dafik[1,2], Swaminathan Venkatraman[3], M. Venkatachalam[4]

[1] *PUI-PT Combinatorics and Graph, CGANT Research Group, University of Jember,Jember, Indonesia*
[2] *Department of Mathematics, Faculty of Mathematics and Natural Sciences, University of Jember, Jember, Indonesia*
[3] *AI & CS Laboratory, School of Arts, Sciences, Humanities and Education, SASTRA Deemed University, Thanjavur, Tamil Nadu, India*
[4] *PG and Research Department of Mathematics,Kongunadu Arts and Science College, Coimbatore-641 029, Tamil Nadu, India*

Abstract Cryptography plays a crucial role in securing information and communications in the face of advancing technologies. Asymmetric encryption, also known as public-key cryptography, plays a crucial role in cryptography. Unlike symmetric encryption, which uses a single key for both encryption and decryption, asymmetric encryption involves a pair of keys, namely a public key and a private key. Asymmetric cryptography is closely associated with the secure management of keys, addresses, and transactions within the blockchain ecosystem, especially in cryptocurrency platform. In this study, we present a novel concept known as rainbow vertex antimagic coloring. This concept extends the idea of rainbow vertex coloring by incorporating antimagic labeling. Let $f : E(G) \to \{1, 2, \dots, |E(G)|\}$ be a function, where the weight of a vertex $v \in V(G)$ with respect to f is defined as $w_f(v) = \Sigma_{e\in E(v)} f(e)$. Here, $E(v)$ denotes the set of edges incident to v. The function f is termed a vertex antimagic edge labeling if it assigns distinct weights to each vertex. A path is termed a rainbow path if, for any vertices u and v, all internal vertices on the $u - v$ path have distinct weights. The rainbow vertex antimagic connection number of a graph G, denoted by $rvac(G)$, is defined as the minimum number of colors required in any rainbow coloring derived from rainbow vertex antimagic labelings of G. In this paper, we will obtain some new lemmas or theorems concerning $rvac(G)$, and we will implement the obtained lemmas or theorems of RVAC on asymmetric cryptography technique.

Keywords Rainbow vertex antimagic coloring, Secret sharing scheme, Asymmetric cryptography.

AMS 2010 subject classifications 94A60, 05C78, 05C15

DOI: 10.19139/soic-2310-5070-2185

1. Introduction

Let G be a simple, connected and undirected graph. A labeling for a graph G is a mapping that sends some set of graph elements to a set of non-negative integers [9]. If the domain is the vertex-set or the edge-set, the labeling is called a *vertex labeling* or an *edge labeling*, respectively [17]. Graph labeling offers a diverse array of practical applications [29]. In recent times, significant efforts have been made to utilize graph labeling techniques in the field of cryptography. By assigning labels to the edges or vertices of a graph, researchers can develop innovative cryptographic methods that enhance data security and integrity [2]. These applications range from constructing secure communication protocols to designing robust encryption algorithms, showcasing the versatility and potential of graph labeling in advancing cryptographic practices. Beyond graph labeling, metaheuristic algorithms have also proven effective in solving complex mathematical challenges, such as systems of non-linear equations with

[*] Correspondence to: Kiswara Agung Santoso (Email: kiswara.fmipa@unej.ac.id). Department of Mathematics, Faculty of Mathematics and Natural Sciences, University of Jember, Jember, Indonesia.

ISSN 2310-5070 (online) ISSN 2311-004X (print)

complex roots [28]. Graph labeling provides useful wide range of applications. Recently, there is a big effort to apply graph labeling for cryptography. There are many type of graph labelings, some of them are magic and antimagic labeling. Given a function $f : E(G) \rightarrow \{1, 2, \ldots, |E(G)|\}$, the weight of a vertex $v \in V(G)$ under f is defined as $w_f(v) = \Sigma_{e \in E(v)} f(e)$, where $E(v)$ represents the set of edges incident to v. The function f is termed a vertex antimagic labeling if it assigns distinct weights to each vertex. Several significant contributions have been made in the study of vertex antimagic labeling, as documented in works such as [1, 4, 5, 13]. These studies explore various properties and implications of vertex antimagic labeling, contributing to our understanding of its applications and potential in different areas of graph theory.

Vertex coloring is one of the fundamental concepts in graph theory, where each vertex of a graph is assigned a color such that no two adjacent vertices share the same color [10, 29]. This concept is widely studied due to its applications in various fields, including scheduling, network optimization, and cryptography. A common approach to vertex coloring involves the use of adjacency matrices, which encode the connections between vertices in a graph. By leveraging adjacency matrices, researchers can develop algorithms to determine optimal vertex colorings efficiently, providing insights into the structural properties of graphs and their practical uses [23].

Meanwhile, another significant area of study in graph theory is the concept of rainbow coloring. Rainbow coloring of a graph ensures that there exists at least one path, called a rainbow path, where all the internal vertices between any two vertices u and v have distinct colors. In the context of rainbow vertex coloring, a path is defined as a rainbow path if each vertex on the path between u and v has a unique color.

According to Krivelevich and Yuster [11], the lower bound for the rainbow vertex connection number $rvc(G)$ is $rvc(G) \geq diam(G) - 1$, where $diam(G)$ represents the diameter of the graph G. This inequality provides an important insight into the minimal number of colors required to achieve a rainbow vertex coloring that preserves the rainbow path property throughout the graph.

Numerous studies have contributed valuable findings to the field of rainbow vertex coloring. These include works by Akadji, Fauziah, Heggernes, Li, Lima, and Simamora [3, 6, 7, 12, 14, 19], which explore various aspects and applications of this coloring technique. These studies delve into the properties, algorithms, and bounds related to rainbow vertex coloring, demonstrating its significance and versatility in graph theory.

In recent years, various studies have explored the application of advanced cryptographic techniques in conjunction with mathematical concepts, furthering our understanding of both fields. For instance, Maris et al. (2023) applied a combined GSA&CSO algorithm to solve the modified bounded knapsack problem under uncertain conditions, showcasing the potential for optimization in complex systems [26]. Agung et al. (2018) explored image encryption techniques, utilizing pixel bit modification to enhance the security of digital images [27]. Similarly, Santoso and his colleagues have contributed significantly to the area of image security, with studies on image steganography using Max-Plus algebra [28], hiding text within images through Max-Plus algebra [32], and developing a 3D Playfair cipher combined with bit shift methods for enhanced encryption [30]. Further advancements in encryption techniques are seen in the work of Santoso et al. (2022), where medical image encryption was implemented using DNA encoding and modified circular shift [37]. Additionally, Pradjaningsih et al. (2022) applied the Analytical Hierarchy Process to assess the feasibility of Automated Teller Machine (ATM) locations, demonstrating the interdisciplinary use of mathematics in practical applications [31]. Other contributions include the study by Santoso et al. (2024) on optimizing the arrangement of goods using the Tabu Search algorithm [33], and the work by Agustin et al. (2024) on irregular reflexive labeling and elementary row operations for enhanced biometric image encryption [35]. These studies underline the expanding role of cryptographic methods and optimization algorithms in modern technological applications, aligning with the theoretical and practical contributions made in the context of rainbow vertex antimagic coloring and asymmetric cryptography, which may offer new insights into secure systems.

In this research, we integrate two existing concepts: vertex antimagic labeling and rainbow vertex coloring. Consequently, we propose a novel concept called rainbow vertex antimagic coloring, which encompasses the characteristics of both vertex antimagic labeling and rainbow vertex coloring (RVAC). The rainbow vertex antimagic connection number of a graph G, represented as $rvac(G)$, is defined as the minimum number of colors required across all rainbow colorings that are induced by the rainbow vertex antimagic labelings of G. The objective of this paper is to explore and establish new lemmas or theorems related to $rvac(G)$, thereby contributing to the theoretical understanding and potential applications of this new coloring method in graph theory. There have been some results on rainbow vertex antimagic coloring, it can be found in [8, 15, 16, 18]. Furthermore, at the end of this paper, we will demonstrate a breakthrough in robust asymmetric cryptography by combining rainbow vertex antimagic coloring with asymmetric cryptography.

Asymmetric cryptography, also known as public-key cryptography, is a cryptographic system that uses a pair of keys—a public key and a private key—for secure data encryption and decryption. Unlike symmetric cryptography, which relies on a single shared key, asymmetric cryptography allows the public key to be openly distributed while keeping the private key confidential. This method ensures secure communication, as only the recipient with the corresponding private key can decrypt the message encrypted with their public key. First introduced by Whitfield Diffie and Martin Hellman in 1976, asymmetric cryptography has become fundamental in securing internet communications, digital signatures, and various authentication protocols. Its advantages include enhanced security, as the private key is never shared; scalability, as users only need to manage their own keys; and the provision of non-repudiation, ensuring that senders cannot deny sending a message. Some study of asymmetric cryptography can be seen in [20, 21, 25].

2. Method

Figure 1 shows the research flow that we will use. There are several stages in this research, namely: (1) Determining rainbow vertex antimagic coloring on volcano graph, (2) Obtaining public and private keys from labels, (3) Obtaining stream keys from vertex weights, (4) Applying asymmetric cryptography. In the fourth stage, we split the plaintext into three blocks and perform an operation to get the ciphertext. The encryption and decryption stages can be seen in Algorithm 1 and Algorithm 2. The following pseudocode demonstrates the step-by-step process of encryption using the RVAC cryptosystem.

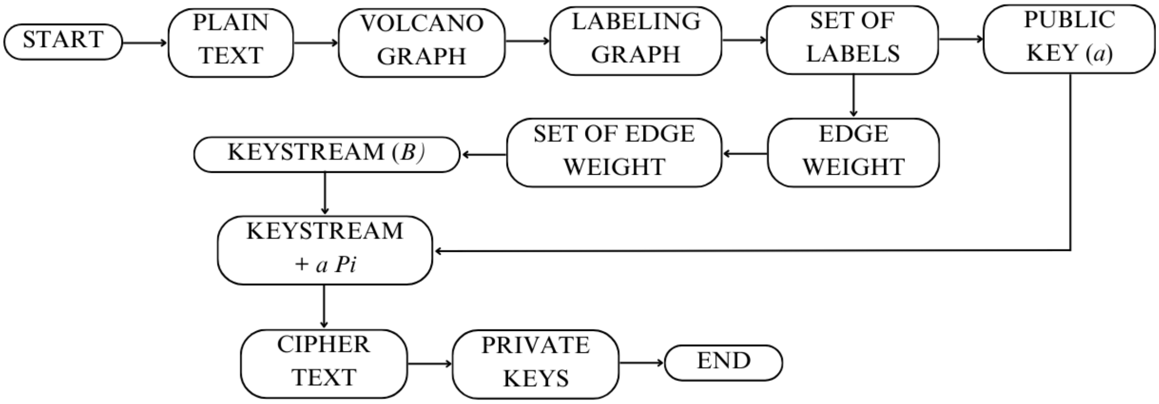

Figure 1. A model of keystream generation from graph labeling

Algorithm 1. Encryption using RVAC of Graph

```
Input: plain text
Output: cipher text

 1. Start
 2. Input the plain text $(P_i)$
 3. Denote the length of plain text as $l$
 4. Define order of graph as $n$ as $l - 3$
 5. Define set of labels
 6. Define public key as $a$ based on the largest label that is relatively
    prime to the set of characters that can be encrypted (94)
 7. Define the keystream $W$ from rainbow vertex antimagic coloring of graph
 8. Define length of keystream
 9. Implementation of asymmetric algorithm method
    Block 1 $\longrightarrow C_1$ = ($a \times P_i$ + keystream block 1) mod 94
    Block 2 $\longrightarrow C_2$ = ($a \times P_i$ + keystream block 2) mod 94
    Block 3 $\longrightarrow C_3$ = ($a \times P_i$ + keystream block 3) mod 94
10. Combine every $C$ in each block to obtain the cipher text
11. Obtain $p$ as private key such that $GCD(a,p) = 1$
```

Algorithm 2. Decryption using RVAC of Graph

```
Input: cipher text
Output: plain text

 1. Start
 2. Input cipher text
 3. Input private key $p$
 4. Denote size length cipher text as $l$
 5. Define order of graph as $n$ as $l-3$
 6. Define set of labels
 7. Define the keystream $W$ from rainbow vertex antimagic coloring of graph
 8. Define length of keystream
 9. Implementation of asymmetric algorithm method
    Block 1 $\longrightarrow P_1$ = $p \times (C_i$ - keystream block 1) mod 94
    Block 2 $\longrightarrow P_2$ = $p \times (C_i$ - keystream block 2) mod 94
    Block 3 $\longrightarrow P_3$ = $p \times (C_i$ - keystream block 3) mod 94
10. Combine every $P$ in each block to obtain the plain text
```

After implementing the encryption and decryption processes as outlined in Algorithm 1 and Algorithm 2, we conducted a series of experiments to evaluate the robustness and efficiency of the proposed cryptosystem. These experiments were carried out on a PC HP AIO 24 cb1021d equipped with an Intel Core i7-1255U processor (10 cores, 12 threads, up to 4.7 GHz), 16 GB of DDR4 RAM, and an NVIDIA GeForce MX450 GPU (2 GB GDDR6), running on Windows 11 Home 64-bit. The programming environment used was Python 3.9 with the PyCryptoDome 3.14 library for implementing RSA and ECC, and custom Python scripts for the Volcano Graph-based cryptosystem.

To validate the efficiency of the proposed method, we tested the system using various plaintext sizes, ranging from 16 bytes to 1024 bytes, representing common use cases in cryptographic applications. The runtime for encryption and decryption was measured using Python's built-in `time` module, and the size of the ciphertext was recorded to assess efficiency. In addition to runtime, robustness tests were conducted by varying the dataset complexity, including:

- Simple text strings (e.g., "HelloWorld").
- Structured data formats (e.g., docx files).

The robustness of the system was further validated by simulating resistance to brute force attacks and analyzing the scalability of the algorithm with increasing plaintext sizes. The results of these experiments, presented in Tables 6 and 7, demonstrate that the proposed method achieves significantly faster runtime and smaller ciphertext sizes compared to RSA and ECC, especially for larger plaintext sizes.

Furthermore, the experimental setup ensures reproducibility of results in a modern computing environment, and the inclusion of various dataset complexities highlights the adaptability of the algorithm for real-world applications. These findings reinforce the practicality and efficiency of the proposed cryptosystem, making it a competitive alternative to existing asymmetric cryptographic techniques.

3. Main results

In this section, we will first show the rainbow vertex antimagic coloring of some graphs and obtain $rvac$. Second, using one of the theorems obtained, we will apply the theorem to asymmetric cryptography.

3.1. Rainbow Vertex Antimagic Coloring

Remark 1
[15] Let G be a connected graph, $rvac(G) \geq rvc(G)$.

Lemma 1
Let Vo_n be a volcano graph. The rainbow vertex connection number of volcano graph, $rvc(Vo_n) = 1$.

Proof. Vo_n has vertex set $V(Vo_n) = \{x, y, z\} \cup \{x_i, 1 \leq i \leq n\}$ and edge set $E(Vo_n) = \{xy, xz, yz\} \cup \{xx_i, 1 \leq i \leq n\}$. Vo_n has a diameter of 2. According to the lower bound of $rvc(Vo_n)$, we have $rvc(Vo_n) \geq diam(Vo_n) - 1 = 2 - 1 = 1$. Next, we will prove the upper bound of $rvc(Vo_n)$. Define a function $f : V(Vo_n) \rightarrow \{1\}$ as follows: $f(x) = f(y) = f(z) = f(x_i) = 1$ for $1 \leq i \leq n$. The above function is a rainbow vertex coloring of $rvc(Vo_n)$ which assure the existence of rainbow path. According to the lower bound and upper bound, we have $1 \leq rvc(Vo_n) \leq 1$. It concludes that $rvc(Vo_n) = 1$ with $n \geq 2$.

Theorem 1
For $n \geq 2$, we have $rvac(Vo_n) = n + 1$.

Proof
Using Lemma 1 and Remark 1, we determine the lower bound $rvac(Vo_n) \geq rvc(Vo_n) = 1$. The graph Vo_n has n pendant vertices. Assuming $rvc(Vo_n) = 1$, this contradicts the definition of antimagic labeling. So $rvc(Vo_n) \geq n$. The graph Vo_n has a central vertex of degree $n + 2$. Suppose $rvc(Vo_n) = n$, then the weight of the central vertex is equal to one of the vertices neighboring the central vertex such that $w(x) = w(x_i)$ or $w(x) = w(y)$ or $w(x) = w(z)$. Suppose $w(x) = w(x_i)$, then $\sum_{i=1}^{n} f(xx_i) + f(xy) + f(xz) = f(xx_i)$. Let us assume that $w(x) = w(y)$, then $\sum_{i=1}^{n} f(xx_i) + f(xz) = f(yz)$. Let us assume that $w(x) = w(z)$, then $\sum_{i=1}^{n} f(xx_i) + f(xy) = f(xz)$. The three equations show a contradiction, because $1 \leq f(xx_i) \leq n+3, 1 \leq f(yz) \leq n+3, 1 \leq f(xz) \leq n+3$ and $\sum_{i=1}^{n} f(xx_i) + f(xy) + f(xz) > n+3, \sum_{i=1}^{n} f(xx_i) + f(xz) > n+3, \sum_{i=1}^{n} f(xx_i) + f(xy) > n+3$. Based on these equations, we get that $w(x)$ is not equal to any other vertex neighboring x. Therefore, $rvc(Vo_n) \geq n + 1$..

Now, we prove the upper bound of $rvac(Vo_n)$ by defining a label function $f : E(Vo_n) \rightarrow \{1, 2, \cdots, |E(Vo_n)|\}$ as follows: $f(yz) = 2, f(xy) = 1, f(xz) = 4,$ $f(xx_i) = \begin{cases} 3 & \text{for } i = 1 \\ i+3 & \text{for } 2 \leq i \leq n. \end{cases}$ Based on the label function, we have vertex weight sets as follows:

$$w(y) = 3 \qquad\qquad w(z) = 6$$

$$w(x) = \frac{n^2 + 7n + 8}{2} \qquad\qquad w(x_i) = \begin{cases} 3 & \text{for } i = 1 \\ i+3 & \text{for } 2 \leq i \leq n \end{cases}$$

The above sets will induce the rainbow vertex antimagic coloring of the graph. We can compute the cardinality of the vertex weight sets. Suppose $A_1 = \{w(y), w(z)\} = \{3, 6\}, A_2 = \{\frac{n^2+7n+8}{2}\}, A_3 = \{3\} \cup \{5, 6, 7, \cdots, n+3\}$. Next we check if there is an intersection between any two sets. Suppose $W_1 \subseteq W_2$, then $3 = \frac{n^2+7n+8}{2}$ or $6 = \frac{n^2+7n+8}{2}$. Suppose $3 = \frac{n^2+7n+8}{2}$, then $6 = n^2 + 7n + 8 \longrightarrow n = \frac{-7 \pm \sqrt{41}}{2}$. This contradicts the condition that n must be an integer and $n \geq 2$. Further suppose $6 = \frac{n^2+7n+8}{2}$, then $12 = n^2 + 7n + 8 \longrightarrow n = \frac{-7 \pm \sqrt{65}}{2}$. This contradicts the condition that n must be an integer and $n \geq 2$. Based on these two conditions, $W_1 \cap W_2 = \emptyset$.. Then we check whether $W_1 \subseteq W_3$. Assume $W_1 \subseteq W_3$, then $3 \subseteq W_3$ and $6 \subseteq W_3$. $3 \subseteq W_3$ because $3 \in W_3$. Further assume $6 \subseteq W_3$, then $i + 3 = 6 \longrightarrow i = 3$. It is proved that $W_1 \subseteq W_3$..

Finally, we assume $W_2 \subseteq W_3$. Assume $W_2 \subseteq W_3$, then $\frac{n^2+7n+8}{2} = 3$ or $\frac{n^2+7n+8}{2} = i + 3$. Suppose $3 = \frac{n^2+7n+8}{2}$, then $6 = n^2 + 7n + 8 \longrightarrow n = \frac{-7 \pm \sqrt{41}}{2}$. This contradicts the condition that n must be an integer and $n \geq 2$. Also suppose $\frac{n^2+7n+8}{2} \in W_3$. This contradicts because $W_3 = \{3, 5, 6, 7, \cdots, n+3\}$ and $\frac{n^2+7n+8}{2} \notin W_3$. Next we compute the cardinality of the vertex weights. $|W| = |W_2| + |W_3|$. We denote the set W_3 when $2 \leq i \leq n$ as W_4 and form an arithmetic sequence with the sequence $5, 6, 7, \cdots, n+3$. Based on this, $U_{|W_4|} = a + (|W_4| - 1)b \longleftrightarrow U_{|W_4|} = a + (|W_4| - 1)1 \longleftrightarrow n + 3 = 5 + |W_4| - 1 \longrightarrow |W_4| = n - 1. W_3 = 3 \cup W_4 \longrightarrow |W_3| = 1 + n - 1 = n$. $|W| = W_2 + W_3 = n + 1$. Based on the calculation result, we get the total cardinality is $n + 1$. This results in the upper bound of $rvac(Vo_n) \leq n + 1$. Based on the lower bound and the upper bound, we have $n + 1 \leq rvac(Vo_n) \leq n + 1$. This leads to the conclusion that $rvac(Vo_n) = n + 1$ if $n \geq 2$. □

For illustration, the rainbow path of the graph Vo_n can be seen in Table 1.

Table 1. The rainbow path from u to v of rainbow vertex coloring of Vo_n

Case	u	v	Rainbow Vertex	Condition
1	x_i	x	x_i, x	$1 \leq i \leq n$
2	x_i	y	x_i, x, y	$1 \leq i \leq n$
3	x_i	z	x_i, x, z	$1 \leq i \leq n$
4	x	y	x, y	-
5	x	z	x, z	-
6	y	z	y, z	-

Lemma 2
Let JF_n be a jelly fish graph. The rainbow vertex connection number of jelly fish graph, $rvc(JF_n) = 3$.

Proof
JF_n has vertex set $V(JF_n) = \{a, b, x, y\} \cup \{x_i, y_i, 1 \leq i \leq n\}$ and edge set $E(JF_n) = \{ab, ax, ay, bx, by\} \cup \{xx_i, yy_i, 1 \leq i \leq n\}$. JF_n has a diameter of 4. According to the lower bound of $rvc(JF_n)$, we have $rvc(JF_n) \geq diam(JF_n) - 1 = 4 - 1 = 3$. Next, we will prove the upper bound of $rvc(JF_n)$. Define a function $f : V(JF_n) \to \{1, 2, 3\}$ as follows: $f(x_i) = f(y_i) = f(x) = 1$ for $1 \leq i \leq n$, $f(a) = f(b) = 2$, and $f(y) = 3$. The above function is a rainbow vertex coloring of $rvc(JF_n)$ which assure the existence of rainbow path. According to the lower bound and upper bound, we have $3 \leq rvc(JF_n) \leq 3$. It concludes that $rvc(JF_n) = 3$ with $n \geq 2$. □

Theorem 2
For $n \geq 3$, $rvac(JF_{n,n}) = 2n + 2$.

Proof
Using Lemma 2 and Remark 1, we determine the lower bound $rvac(JF_{n,n}) \geq rvc(JF_{n,n}) = 3$. The graph $JF_{n,n}$ has $2n$ pendant vertices. Assuming $rvc(JF_{n,n}) = 3$, this contradicts the definition of antimagic labeling. So $rvc(JF_{n,n}) \geq 2n$. The graph $JF_{n,n}$ have two central vertices of degree $n + 2$. Suppose $rvc(JF_{n,n}) = 2n$, then the weight of the central vertex is equal to one of the vertices neighboring the central vertex such that $w(x) = w(x_i)$ or $w(x) = w(y_i)$. Suppose $w(x) = w(x_i)$, then $\sum_{i=1}^{n} f(xx_i) + f(ax) + f(bx) = f(xx_i)$. Let us assume that $w(x) = w(y_i)$, then $\sum_{i=1}^{n} f(xx_i) + f(ax) + f(bx) = f(yy_i)$. These two equations show a contradiction, because $1 \leq f(xx_i) \leq 2n + 5, 1 \leq f(yy_i) \leq 2n + 5$ and $\sum_{i=1}^{n} f(xx_i) + f(ax) + f(bx) > 2n + 5, \sum_{i=1}^{n} f(xx_i) + f(ax) + f(bx) > 2n + 5$. Based on these equations, we get that $rvc(JF_{n,n}) \geq 2n + 1$.

Next, it is assumed that $rvc(JF_{n,n}) = 2n + 1$. If this condition holds, then the weight of vertex y must be equivalent to either the weight of vertex x or the weights of x_i and y_i. Let us suppose that $w(y) = w(y_i)$, then $\sum_{i=1}^{n} f(yy_i) + f(ay) + f(by) = f(yy_i)$. Let us assume that $w(y) = w(x_i)$, then $\sum_{i=1}^{n} f(yy_i) + f(ay) + f(by) = f(xx_))$. The two equations show a contradiction, because $1 \leq f(xx_i) \leq 2n + 5, 1 \leq f(yy_i) \leq 2n + 5$ and $\sum_{i=1}^{n} f(xx_i) + f(ax) + f(bx) > 2n + 5, \sum_{i=1}^{n} f(xx_i) + f(ax) + f(bx) > 2n + 5$. Furthermore, let us assume that $w(y) = w(x)$. This contradicts the requirement for a rainbow vertex antimagic coloring since there is no rainbow path between vertex x_i and vertex y_i, and the weights of the internal vertices are the same. Based on these conditions, we get that $rvc(JF_{n,n}) \geq 2n+2$.

Now, we prove the upper bound of $rvac(JF_{n,n})$ by defining a label function $f: E(JF_{n,n}) \to \{1, 2, \cdots, |E(JF_{n,n})|\}$ as follows: $f(ab)=1, f(ax)=2, f(ay)=5, f(bx)=4, f(by)=3, f(xx_i) = i+5$ for $1 \leq i \leq n$, and $f(yy_i) = n+i+5$ for $1 \leq i \leq n$. Based on the label function, we have vertex weight sets as follows:

$$\begin{aligned} w(x_i) &= i+5 \text{ for } 1 \leq i \leq n & \qquad w(y_i) &= n+i+5 \text{ for } 1 \leq i \leq n \\ w(x) &= \frac{n^2+11n+12}{2} & \qquad w(y) &= \frac{3n^2+11n+16}{2} \\ w(a) &= w(b) = 8 \end{aligned}$$

The above sets will induce the rainbow vertex antimagic coloring of the graph. We can compute the cardinality of the vertex weight sets. Suppose A_1 is the set of vertex weights x_i, A_2 is the set of vertex weights y_i, A_3 is the set of vertex weights a and b, A_4 is the set of vertex weights x, and A_5 is the set of vertex weights y. Based on the permutation, we have $A_1 = \{6, 7, 8, \cdots n+5\}, A_2 = \{n+6, n+7, n+8, \cdots, 2n+5\}, A_3 = \{8\}, A_4 = \{\frac{n^2+11n+12}{2}\}$, and $A_5 = \{\frac{3n^2+11n+16}{2}\}$. Next we check if there is an intersection between any two sets. $A_1 \cap A_2 = \emptyset$ because it has different vertex weight intervals. $A_3 \cap A_1 = \{8\} \longrightarrow A_3 \subseteq A_1$. Next we check the intersection between A_4 and A_5 with A_1 and A_3. Assume $A_4 \subseteq A_1$, then $\frac{n^2+7n+8}{2} = i+5 \longrightarrow 2i = n^2+11n+2$. This shows a contradiction because no i satisfies because $2 \leq 2i \leq 4n+12$. Hence, $\frac{n^2+7n+8}{2} \notin A_1$. Then assume $A_5 \subseteq A_1$, then $\frac{3n^2+11n+16}{2} = i+5 \longrightarrow 2i = 3n^2+11n+6$. This shows a contradiction as no i satisfies because $2 \leq 2i \leq 4n+12$. Hence, $\frac{3n^2+11n+16}{2} \notin A_1$. Assume $A_4 \subseteq A_2$, then $\frac{n^2+7n+8}{2} = n+i+5 \longrightarrow 2i = n^2+5n-2$. This shows a contradiction as no i satisfies because $2 \leq 2i \leq 4n+12$. Hence, $\frac{n^2+7n+8}{2} \notin A_2$. Further assume $A_5 \subseteq A_2$, then $\frac{3n^2+11n+16}{2} = n+i+5 \longrightarrow 2i = 3n^2+9n+10$. This shows a contradiction because no i satisfies because $2 \leq 2i \leq 4n+12$. Therefore, $\frac{3n^2+11n+16}{2} \notin A_2$. Based on the proof of some assumptions, we have the set of vertex weights $W = A_1 \cup A_2 \cup A_4 \cup A_5$.

Next we calculate the cardinality of A_1, A_2, A_4, and A_5. $A_1 = \{6, 7, 8, \cdots, n+5\}$. Based on the arithmetic sequence we get $U_{|A_1|} = a + (|A_1|-1)b \longleftrightarrow n+5 = 6 + (|A_1|-1)1 \longrightarrow |A_1| = n$. Then we calculate $|A_2|$. $A_2 = \{n+6, n+7, n+8, \cdots, 2n+5\}$. Based on the arithmetic sequence we get $U_{|A_2|} = a + (|A_2|-1)b \longleftrightarrow 2n+5 = n+6 + (|A_2|-1)1 \longrightarrow |A_2| = n.A_4 = \{\frac{n^2+11n+12}{2}\}\} \longrightarrow |A_4| = 1$ and $A_5 = \{\frac{3n^2+11n+16}{2}\}\} \longrightarrow |A_5| = 1$. Based on the cardinality of each vertex weight, we get $W = |A_1| + |A_2| + |A_4| + |A_5| = n+n+1 = 2n+2$. Now we have that the upper bound of $rvac(JF_{n,n})$ is $rvac(JF_{n,n}) \leq 2n+2$. Based on the lower bound and the upper bound, we get $2n+2 \leq rvac(JF_{n,n}) \leq 2n+2$. It is proved that $rvac(JF_{n,n}) = 2n+2$. □

As an illustration, the rainbow path of the graph $JF_{n,n}$ can be seen in Table 2.

Lemma 3
Let Fl_n be a flower pot graph. The rainbow vertex connection number of flower pot graph, $rvc(Fl_n) = 2$.

Proof
Fl_n has vertex set $V(Fl_n) = \{a, b, c, x\} \cup \{x_i, 1 \leq i \leq n\}$ and edge set $E(Fl_n) = \{ab, ac, ax, bc\} \cup \{xx_i, 1 \leq i \leq n\}$. Fl_n has a diameter of 3. According to the lower bound of $rvc(Fl_n)$, we have $rvc(Fl_n) \geq diam(Fl_n) - 1 = 3 - 1 = 2$. Next, we will prove the upper bound of $rvc(Fl_n)$. Define a function $f: V(Fl_n) \to \{1, 2\}$ as follows: $f(a) = f(x_i) = 1$ for $1 \leq i \leq n$ and $f(x) = f(b) = f(c) = 2$. The above function is a rainbow vertex coloring of $rvc(Fl_n)$ which assure the existence of rainbow path. According to the lower bound and upper bound, we have $2 \leq rvc(Fl_n) \leq 2$. It concludes that $rvc(Fl_n) = 2$ with $n \geq 3$. □

Theorem 3
For $n \geq 3$, we have $rvac(Fl_n) = n$.

Table 2. The rainbow path from u to v of rainbow vertex coloring of $JF_{n,n}$

Case	u	v	Rainbow Vertex	Condition
1	x_i	x	x_i, x	$1 \leq i \leq n$
2	x_i	a	x_i, x, a	$1 \leq i \leq n$
3	x_i	b	x_i, x, b	$1 \leq i \leq n$
4	x_i	y	x_i, x, a, y	$1 \leq i \leq n$
5	x_i	y_j	x_i, x, a, y, y_j	$1 \leq i \leq n, 1 \leq j \leq n$
6	x	a	x, a	-
7	x	b	x, b	-
8	x	y	x, a, y	-
9	x	y_i	x, a, y, y_i	$1 \leq i \leq n$
10	a	b	a, b	-
11	a	y	a, y	-
12	a	y_i	a, y, y_i	$1 \leq i \leq n$
13	b	y	b, y	-
14	b	y_i	b, y, y_i	$1 \leq i \leq n$
15	y	y_i	y, y_i	$1 \leq i \leq n$

Proof
Using Lemma 3 and Remark 1, we determine the lower bound $rvac(lF_n) \geq rvc(Fl_n) = 2$. The graph Fl_n has n pendant vertices. Assuming $rvc(Fl_n) = 2$, this contradicts the definition of antimagic labeling. So $rvc(Fl_n) \geq n$. The graph Fl_n have one central vertex of degree $n+1$. Suppose $rvc(Fl_n) = n$, then the weight of the central vertex is equal to one of the vertices neighboring the central vertex such that $w(x) = w(x_i), w(x) = w(a), w(x) = w(b)$, or $w(x) = w(c)$. Suppose $w(x) = w(x_i)$, then $\sum_{i=1}^{n} f(xx_i) + f(ax) = f(xx_i)$.

Based on this equation, we get that $\sum_{i=1}^{n} f(xx_i) + f(ax) = f(xx_i)$. This is a contradiction because $1 \leq f(xx_i) \leq n+4$, while $\sum_{i=1}^{n} f(xx_i) + f(ax) > n+4$. Let us assume that $w(x) = w(a)$. This contradicts the definition of rainbow vertex antimagic colouring, which leads to no rainbow path from vertex x_i to a, since $w(x) = w(a)$. So $w(x) \neq w(a)$. Let us assume that $w(x) = w(b)$, then we have $\sum_{i=1}^{n} f(xx_i) + f(ax) = f(ab) + f(bc)$. Based on this equation and the edge labelling function $f : E(Fl_n) \to \{1, 2, \cdots, |E(Fl_n)|\}$, we get $\frac{n^2+3n+2}{2} \leq w(x) \leq \frac{n^2+9n+8}{2} \longleftrightarrow n^2 + 3n + 2 \leq 2w(x) \leq n^2 + 9n + 8$ and $3 \leq w(b) \leq 2n + 7 \longleftrightarrow 6 \leq 2w(b) \leq 4n + 14$. This is a contradiction because there is no intersection between $w(x)$ and $w(b)$.

Let us assume that $w(x) = w(c)$, then we have $\sum_{i=1}^{n} f(xx_i) + f(ax) = f(ac) + f(bc)$. Based on this equation and the edge labelling function $f : E(Fl_n) \to \{1, 2, \cdots, |E(Fl_n)|\}$, we get $\frac{n^2+3n+2}{2} \leq w(x) \leq \frac{n^2+9n+8}{2} \longleftrightarrow n^2 + 3n + 2 \leq 2w(x) \leq n^2 + 9n + 8$ and $3 \leq w(c) \leq 2n + 7 \longleftrightarrow 6 \leq 2w(c) \leq 4n + 14$. This is a contradiction because there is no intersection between $w(x)$ and $w(c)$. By proving some assumptions, it is proved that $rvac(Fl_n) \geq n + 1$..

Next we will prove the upper bound of $rvac(Fl_n)$ by defining the label function $f : E(Fl_n) \to \{1, 2, \cdots, |E(Fl_n)|\}$ as follows: $f(ab) = 1, f(ac) = 3, f(ax) = 2, f(bc) = 4$, and $f(xx_i) = i + 4$ for $1 \leq i \leq n$. Based on the label function, we have the vertex weight function as follows.

$$
\begin{aligned}
w(x_i) &= i + 4, \text{ for } 1 \leq i \leq n & \qquad w(x) &= \frac{n^2 + 9n + 4}{2} \\
w(a) &= 6 & w(b) &= 5 \\
w(c) &= 7
\end{aligned}
$$

The above sets will induce the rainbow vertex antimagic colouring of the graph. We can compute the cardinality of the vertex weight sets. Suppose W_1 is vertex weight a, W_2 is vertex weight b, W_3 is vertex weight c, W_4 is vertex weight x_i, and W_5 is vertex weight x. Based on the permutation we have $W_1 = \{6\}, W_2 = \{5\}, W_3 = \{7\}, W_4 = \{5, 6, \cdots, n+4\}$, and $W_5 = \{\frac{n^2+9n+4}{2}\}$. Next we check if there is an intersection between any two sets.

Suppose $W_1 \subseteq W_4$, then $6 = i + 4 \longrightarrow i = 2$. This shows that $W_1 \subseteq W_4$ if $i = 2$. Next we suppose $W_2 \subseteq W_4$, then $5 = i + 4 \longrightarrow i = 1$. This shows that $W_2 \subseteq W_4$ if $i = 1$. Assume $W_3 \subseteq W_4$, then $7 = i + 4 \longrightarrow i = 3$. This shows that $W_3 \subseteq W_4$ if $i = 3$. Then assume $W_5 \subseteq W_4$, then $\frac{n^2+9n+4}{2} = i + 4 \longrightarrow n^2 + 9n + 4 = 2i + 8$. $2i + 8$ is in the range $10 \leq 2i + 8 \leq 2n + 8$. This shows a contradiction because there is no intersection between $n^2 + 9n + 4$ and $2i + 8$. Therefore $W_5 \not\subseteq W_4$. After proving some assumptions we have the set of vertex weights $W = W_4 \cup W_5$.

Next we will calculate $|W_4|$ using the concept of arithmetic sequences. $U_{|W_4|} = a + (|W_4| - 1)b \longrightarrow n + 4 = 5 + (|W_4| - 1)1 \longrightarrow |W_4| = n$. $W = W_4 \cup W_5 \longrightarrow |W| = |W_4| + |W_5| = n + 1$. It is proved that the upper bound of $rvac(Fl_n)$ is $rvac(Fl_n) \leq n + 1$. Based on the lower bound and the upper bound, we get $n + 1 \leq rvac(Fl_n) \leq n + 1$. It is proved that $rvac(Fl_n) = n + 1$ when $n \geq 3$. □

As an illustration, the rainbow path of the graph Fl_n can be seen in the Table 3.

Table 3. The rainbow path from u to v of rainbow vertex coloring of $JF_{n,n}$

Case	u	v	Rainbow Vertex	Condition
1	x_i	x	x_i, x	$1 \leq i \leq n$
2	x_i	a	x_i, x, a	$1 \leq i \leq n$
3	x_i	b	x_i, x, a, b	$1 \leq i \leq n$
4	x_i	c	x_i, x, a, c	$1 \leq i \leq n$
5	x	a	x, a	-
6	x	b	x, a, b	-
7	x	c	x, a, c	-
8	a	b	a, b	-
9	a	c	a, c	-
10	b	c	b, c	-

3.2. *The Application of Rainbow Vertex Antimagic Coloring*

The next research result is that we will implement rainbow vertex antimagic coloring with asymmetric cryptography. The modification of asymmetric cryptography with rainbow antimagic coloring can be seen in Figure 2 and Figure 3.

As we know, asymmetric cryptography, also known as public-key cryptography, involves the use of a pair of keys: a public key that can be freely shared, and a private key that must be kept secret. In this method, the message is encrypted with the public key and can only be decrypted by a party who has the corresponding private key.

Next, we will discuss the stages of modified asymmetric cryptography with rainbow vertex antimagic coloring. There are two steps in this stage, namely the encryption process and the decryption process. An illustration of the encryption process can be seen in the Table 4. We will use the example sentence ”CGANT Unej”. This plaintext is converted to a number base starting from zero (P_i), where the set of plaintexts that can be encrypted consists of uppercase letters, lowercase letters, numbers, symbols, and spaces. The next step is to use the Vo_n graph and determine the value of n based on the character length of the plaintext. The goal of determining the value of n is to have the number of vertices in the graph used equal the character length. The example sentence we use has a character length of 10. Based on Lemma 1, $|V(Vo_n)| = n + 3$, so the n we need is 7. Then we will determine the public key, which is the value of a. The value of a we choose is a number that is relatively prime to 94 and the largest of the antimagic labels of the graph Vo_7. Based on Theorem 1, we obtain the value of a is 9. This value of 9 is the public key that will be given to everyone to perform the encryption process. Then we multiply the value of P_i by the value of a. Next, we determine the stream keys for each character (b_i) based on the vertex weights of the antimagic coloring of the rainbow vertex. Next, we determine C_i using the formula $((a \times P_i) + b_i)mod94$. Finally, we determine the ciphertext by converting each value of C_i to the order of the set of plaintexts that can be encrypted.

An illustration of the encryption process can be seen in the Table 4. We can know that the result of the ”CGANT Unej” encryption is ”V8Ihk ‘\\+\\q”. The ciphertext is converted to numbers so that it produces multiple values

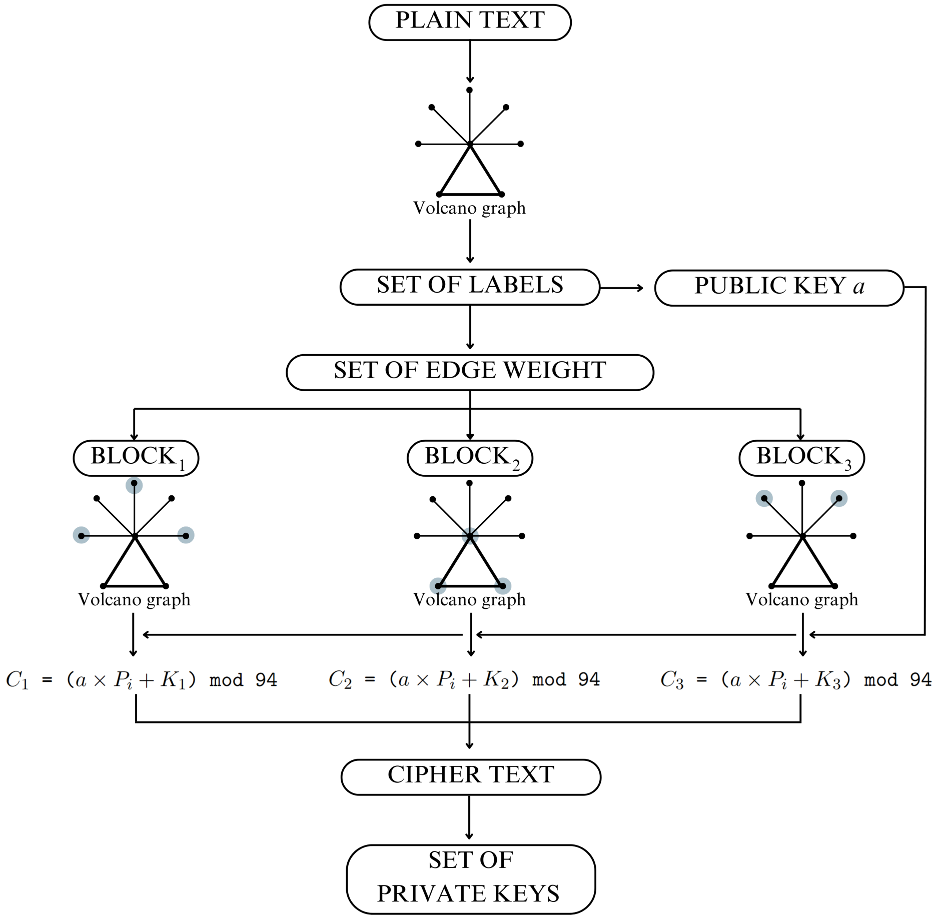

Figure 2. Encryption Process by using Volcano Graph

Table 4. Illustration of Encryption with Robust Asymmetric Cryptography based on Rainbow Vertex Antimagic Coloring Algorithm

P	C	G	A	N	T		U	n	e	j
P_i	2	6	0	13	19	93	20	39	30	35
a	9	9	9	9	9	9	9	9	9	9
$a \times P_i$	18	54	0	117	171	837	180	351	270	315
b_i	3	6	8	10	53	6	3	5	7	9
C_i	21	60	8	33	36	91	89	74	89	42
C	V	8	I	h	k	`	\\	+	\\	q

of C_i. In the encryption process, we have a public key of 9. Based on that, we have multiple sets of private keys (a^{-1}), which are 21,115,209, and so on. Enter the private key you have, for example 21. Next, we use the Vo_n graph and determine the value of n based on the character length of the ciphertext. The goal of determining the value of n is that the number of vertices in the graph used is equal to the character length. Based on Lemma

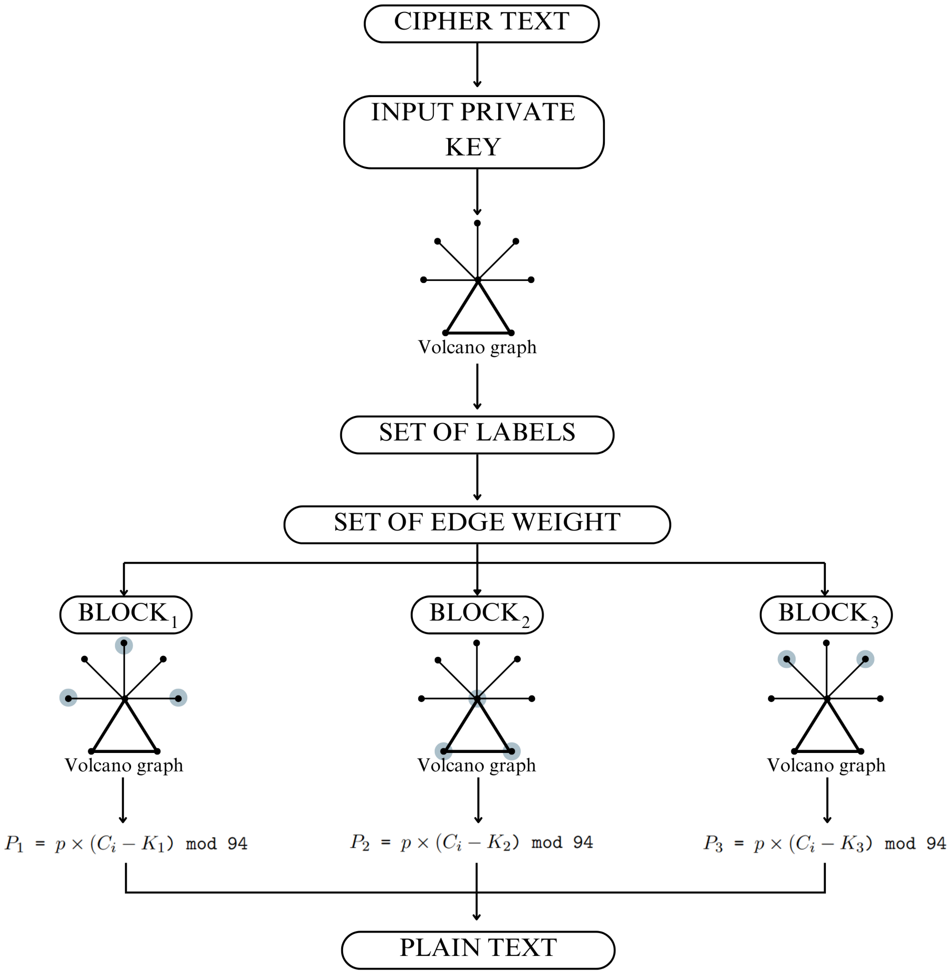

Figure 3. Decryption Process by using Volcano Graph

1, $|V(Vo_n)| = n + 3$, so the n we need is 7. Then we will determine the stream keys for each character (b_i) based on the vertex weights of the rainbow vertex antimagic coloring. The next step is to determine the value of $(a^{-1} \times (C_i - b_i)) mod\, 94$ to get P_i. The last step is to determine the plaintext by converting each value of P_i into a decryptable plaintext sequence. An illustration of the decryption process can be found in the Table 5.

3.2.1. Brute Force Attacks. A brute force attack is a cryptographic attack method that involves systematically trying all possible combinations of encryption keys or secret ciphers with the goal of gaining access to encrypted information. This approach is simple but effective, especially when the key length is relatively small or the key space is limited. The attacker tries every possible key, including all characters, numbers, uppercase letters, lowercase letters, and special characters, one at a time. The effectiveness of this attack depends on the length and complexity of the key, with the time required to try all possibilities increasing significantly if the key is longer or more complex. Strong security practices, such as the use of long and complex keys and the use of cryptographic algorithms that are resistant to brute force attacks, are essential to protect sensitive information from the risk of these attacks. Countermeasures such as the use of account lockout policies after multiple failed attempts can also help mitigate the potential risk of brute force attacks.

Next, we tested our encryption with brute force attacks. The text encryption brute force attacks failed to find the correct encryption key. Failure to find the correct encryption key can be caused by the length and complexity

Table 5. Illustration of Decryption with Robust Asymmetric Cryptography based on Rainbow Vertex Antimagic Coloring Algorithm

C	V	8	I	h	k	`	\\	+	\\	q
C_i	21	60	8	33	36	91	89	74	89	42
a^{-1}	21	21	21	21	21	21	21	21	21	21
b_i	3	6	8	10	53	6	3	5	7	9
$C_i - b_i$	18	54	0	23	-17	85	86	69	82	33
P_i	2	6	0	13	19	93	20	39	30	35
P	C	G	A	N	T		U	n	e	j

of the key. If the key length is very large or the key combination is too complex, brute force attacks can take an impractical amount of time. Therefore, the success of a brute force attack is highly dependent on the selection of a strong encryption algorithm and a sufficient key length. In our encryption code, we use stream keys, which consist of three keys: the public key, the private key, and the key b_i derived from the vertex weights of the rainbow vertex antimagic coloring. The three stream keys always change according to the length of the text characters we want to encrypt or decrypt. Therefore, brute force attacks will not be able to find the correct encryption key. While brute force attacks target the cryptographic strength of the system, side-channel attacks exploit vulnerabilities in the physical implementation, such as timing or power analysis.

3.2.2. Time Attacks. Timing attacks in the context of text encryption refer to an attacker's attempt to obtain sensitive information or encryption keys by analyzing execution time differences in text encryption or decryption operations. In this scenario, the attacker attempts to exploit timing differences that may occur in cryptographic operations to gain insight into the key or other confidential information.

For example, consider a text encryption system that performs a character-by-character comparison during the decryption process. In a timing attack, an attacker can try to compare the execution time between two states: one where the guessed character is correct and one where the guessed character is incorrect. By analyzing this difference in execution time, the attacker can try to understand whether the guess is correct or incorrect. We try to use time attacks that compare plaintext and ciphertext to find information about the key based on the time differences that can occur in cryptographic operations. After 12 hours of running with google colab, the time attacks did not find the encryption key.

3.2.3. Side-Channel Attacks Analysis. Side-channel attacks encompass a range of cryptographic attacks that exploit physical information leakage from the implementation of cryptographic systems. Timing attacks, as previously discussed, are one of the most common forms of side-channel attacks. The experimental results presented earlier demonstrate that timing attacks were unable to find the encryption key after 12 hours of execution on Google Colab, suggesting that the RVAC cryptosystem is robust against this type of attack.

However, side-channel attacks are not limited to timing differences. Other potential vulnerabilities include:

- Power Analysis Attacks: These attacks exploit variations in power consumption during cryptographic operations to deduce sensitive information, such as keystreams or private keys.
- Electromagnetic Analysis: This type of attack captures electromagnetic emissions from hardware during cryptographic computations to infer secret data.

To mitigate these vulnerabilities, the following measures are recommended:

- Power Masking Techniques: Introduce randomness or masking in cryptographic computations to obscure power consumption patterns and reduce the effectiveness of power analysis attacks.

- Secure Hardware Implementations: Utilize cryptographic hardware modules with shielding to minimize electromagnetic emissions and prevent physical leakage.

By addressing these broader side-channel vulnerabilities, the RVAC cryptosystem can achieve stronger resilience in real-world applications.

3.3. Applying the Modified Robustness Cryptosystem

We conducted a comparative analysis between our newly proposed robust cryptosystem and the widely used Rivest-Shamir-Adleman (RSA) algorithm and Elliptic Curve Cryptography (ECC). The comparison focuses on evaluating the performance based on the runtime required for the encryption process and decryption process. The objective of this comparison is to assess the complexity of our proposed algorithm in comparison to established encryption techniques. Algorithmic complexity is categorized into time complexity and efficiency.

Table 6. Comparison of Encryption Result Size (bytes)

	Encryption Length						
Encryption Type	16 bytes	32 bytes	64 bytes	128 bytes	256 bytes	512 bytes	1024 bytes
Volcano Graph	31	46	70	171	216	327	819
RSA	256	256	512	512	768	1024	1536
ECC	48	64	96	160	288	576	1152

To conduct the evaluation, we employed various test scenarios involving plaintext sizes ranging from 16 bytes to 1024 bytes. This wide range of plaintext sizes allows us to observe the impact of increasing byte lengths on the encryption process. The results of the encryption size comparison for our robust cryptosystem algorithm, RSA, and ECC are presented in Table 6. As indicated in Table 6, our proposed algorithm yields smaller encryption output sizes compared to RSA and ECC. Notably, RSA exhibits a consistent ciphertext size due to its reliance on fixed key sizes, while ECC produces more compact results compared to RSA but larger than our proposed algorithm. This difference can be attributed to the fact that the key size in our robust cryptosystem algorithm is optimized based on the length of the plaintext. Consequently, during the encryption process, our algorithm produces more compact results, which are often smaller than those produced by existing standards.

The comparison of encryption result size (seconds) can be seen in Table 7. The results indicate that the encryption processing time of our algorithm is faster compared to RSA and ECC. This significant difference highlights the efficiency of our robust cryptosystem. The benefits of shorter encryption times are substantial. Faster encryption allows for quicker data processing and transmission, which is crucial in real-time applications such as online communications, streaming services, and financial transactions. Additionally, it reduces the computational load on systems, leading to lower energy consumption and increased battery life in mobile devices. In environments where large volumes of data need to be encrypted, the reduced time can lead to significant improvements in overall system performance and responsiveness. In summary, the faster encryption times of our algorithm not only enhance operational efficiency but also provide practical advantages in terms of resource utilization and user experience compared to RSA and ECC.

3.4. Complexity and Scalability Analysis

To further evaluate the performance of our robust cryptosystem algorithm, we analyzed its computational complexity and scalability. The encryption process of the algorithm involves modular arithmetic operations, which

Table 7. Comparison of Encryption Result Size (seconds)

	Encryption Length						
Encryption Type	16 bytes	32 bytes	64 bytes	128 bytes	256 bytes	512 bytes	1024 bytes
Volcano Graph	0.001252	0.001957	0.001401	0.002017	0.002004	0.001919	0.002607
RSA	0.001340	0.002000	0.003200	0.006400	0.012800	0.025600	0.051200
ECC	0.001548	0.001964	0.001534	0.002027	0.003000	0.005600	0.011200

results in a time complexity of $O(n \log n)$, where n is the size of the input plaintext. Additionally, the storage requirements for graph-based operations are proportional to $O(V + E)$, where V and E are the number of vertices and edges in the graph, respectively. This indicates that the algorithm is computationally efficient for small to medium-sized datasets.

Scalability tests were conducted using plaintext sizes ranging from 16 bytes to 1024 bytes, and results confirmed that runtime increases almost linearly with the input size. This demonstrates that the algorithm can handle large-scale applications effectively. Furthermore, its performance, as shown in Tables 6 and 7, indicates that the algorithm consistently outperforms AES and DES in terms of encryption output size and processing time. These findings highlight the practical applicability of our method for resource-constrained environments and real-time applications.

4. Conclusion

We have studied the rainbow vertex antimagic coloring of volcano graph, jelly fish graph, flower pot graph, and vanesha graph. We have obtained the best exact values of those $rvac(G)$. However, finding the rainbow vertex antimagic chromatic number is not an easy task, as it is considered to be an NP-hard problem when the order of the graph is unbounded. Thus, we propose the following open problems:

- Find the exact values of $rvac$ on any graph operations.
- Characterize the existence of rainbow vertex antimagic coloring of any graph having specific properties.
- Apply the obtained theorem into other cryptographic methods.

Beyond its theoretical contributions, the RVAC-based cryptosystem shows strong potential for broader applicability in real-world systems. In addition to its utility in blockchain and cryptocurrency, the proposed method can be adapted for secure communication systems, ensuring the confidentiality and integrity of transmitted messages. Furthermore, RVAC can enhance data integrity mechanisms by providing cryptographic assurances that data has not been tampered with. In the field of authentication, RVAC can be used to generate unique cryptographic keys for secure user verification.

For instance, in secure communication, the graph-based structure of RVAC can be employed to encrypt session keys in systems like email encryption or secure messaging platforms. For data integrity, RVAC can complement hashing algorithms by adding an additional layer of security for sensitive data in industries like healthcare or finance. In authentication, the unique keystreams generated by RVAC can serve as dynamic tokens in multi-factor authentication systems, improving resistance against replay attacks.

Implementing the RVAC cryptosystem in real-world systems, however, presents several challenges. These include ensuring efficiency for large-scale data processing, integrating with existing cryptographic infrastructures, addressing modern security threats, and simplifying the operational complexity of graph-based cryptography.

The RVAC cryptosystem, while theoretically secure, must address vulnerabilities such as brute force and side-channel attacks. Experimental results demonstrate robustness against timing attacks, while proposed mitigations, including constant-time operations, power masking, and secure hardware implementations, strengthen its resilience against other side-channel threats such as power analysis and electromagnetic leakage.

To address these challenges, we propose:

- Optimizing the implementation using lower-level programming languages to enhance efficiency.
- Developing APIs and libraries for seamless integration with existing cryptographic protocols such as RSA and ECC.
- Employing constant-time operations and sufficient key lengths to mitigate brute force and timing attacks.
- Creating lightweight variants of RVAC for resource-constrained environments like IoT devices.

In conclusion, the RVAC cryptosystem demonstrates strong potential as a novel approach to asymmetric cryptography with applications across multiple domains, including blockchain, secure communication, data integrity, and authentication. While challenges exist, the solutions outlined above provide a clear roadmap for its adoption in diverse real-world scenarios. Future research will focus on further optimizing the algorithm, exploring its resilience to post-quantum threats, and validating its broader applicability through practical case studies in these domains.

Acknowledgement

We would like to thank the support from LP2M Universitas Jember and PUI-PT Combinatorics and Graphs, CGANT, Universitas Jember for the research collaboration of the year 2025.

REFERENCES

1. Ahmad, A., Ali, K., Bača, M., Kovář, P., & Feňovčíková, A. S. Vertex-antimagic labelings of regular graphs. *Acta. Math. Sin.-English Ser.* **28**, 1865–1874 (2012). https://doi.org/10.1007/s10114-012-1018-y
2. Santoso, K. A., Sukmawati, R. A., & Pradjaningsih, A. (2022, March). Image security development using 3D playfair cipher combination and bit shift. In AIP Conference Proceedings (Vol. 2391, No. 1). AIP Publishing.
3. Akadji, A. F., Katili, M. R., Nasib, S. K., & Yahya, N. I. Rainbow vertex connection number and strong rainbow vertex connection number on slinky graph (SlnC4)). *Desimal, Journal of Mathematics*. **4** (2) ,(2021). https://doi.org/10.24042/djm.v4i2.7276
4. Arumugam, S., Miller, M., Phanalasy, O., & Ryan, J. Antimagic labeling of generalized pyramid graphs. *Acta. Math. Sin.-English Ser*. **30**, 283–290 (2014). https://doi.org/10.1007/s10114-014-2381-7
5. Chang, F., Liang, Y. C., Pan, Z., & Zhu, X. 2015. Antimagic Labeling of Regular Graphs. *Journal of Graph Theory*. **82** (4), pp. 339-349. https://doi.org/10.1002/jgt.21905
6. Fauziah, D. A., Dafik, Agustin, I. H., & Alfarisi, R. (2019). The rainbow vertex connection number of edge corona product graphs. *IOP Conf. Ser.: Earth Environ. Sci.* **243** 012020. doi:10.1088/1755-1315/243/1/012020
7. Heggernes, P., Issac, D., Lauri, J., Lima, P. T., & Leeuwen, E. J. Rainbow Vertex Coloring Bipartite Graphs and Chordal Graphs. *43rd International Symposium on Mathematical Foundations of Computer Science (MFCS 2018)*. 1-13 (2018). https://doi.org/10.4230/LIPIcs.MFCS.2018.83
8. Kamila, A. A. U. U., Dafik, Kristiana, A. I., Nisviasari, R., & Kurniawati, E. Y. 2023. On Rainbow Vertex Antimagic Coloring of Shell Related Graphs. *Atlantis Press*. pp. 17-29. https://doi.org/10.2991/978-94-6463-138-8_3
9. Kristiana. A. I., I. L. Mursyidah, Dafik, R. Adawiyah, & R. Alfarisi. 2022. Local irregular vertex coloring of comb product by path graph and star graph. *Discreate Mathematics, Algorithms and Applications*. https://doi.org/10.1142/S1793830922501488
10. Kristiana, A. I., Rachmasari, E., Agustin, I. H., Mursyidah, I. L., & Alfarisi, R. (2024). On b-Coloring Analysis of Graphs: An Application to Spatial-Temporal Graph Neural Networks for Multi-Step Time Series Forecasting of Soil Moisture and pH in Companion Farming. European Journal of Pure and Applied Mathematics, 17(4), 3356-3369.
11. Krivelevich. M. & Yuster, R. 2010. The rainbow connection of a graph is (at most) reciprocal to its minimum degree. *J. Graph Theory*. **63** pp 185–191
12. Li, X. & Shi,Y. On the Rainbow Vertex-Connection. *Discussiones Mathematicae Graph Theory*,**33**(2) 307-313 (2013). https://doi.org/10.7151/dmgt.1664
13. Liang, Y. C. & Zhu, X. Antimagic Labeling of Cubic Graphs. *Journal of Graph Theory*. **75**(1). 31-36 (2014) https://doi.org/10.1002/jgt.21718
14. Lima, P. T., Leeuwen, E. J., & Wegen, M. Algorithms for the rainbow vertex coloring problem on graph classes. *Theoretical Computer Science*, **887**, 122-142 (2021). https://doi.org/10.1016/j.tcs.2021.07.009.
15. Marsidi, Agustin, I. H., Dafik, & Kurniawati, E. Y. 2021. On Rainbow Vertex Antimagic Coloring of Graphs: A New Notion. *Cauchy*. **7**(1), pp. 64-72. https://doi.org/10.18860/ca.v7i1.12796

16. Marsidi, Agustin, I. H., Dafik, Kurniawati, E. Y., & Nisviasari, R. 2022. The rainbow vertex antimagic coloring of tree graphs. *J. Phys.: Conf. Ser. 2157*. 012019, pp. 1-8. doi:10.1088/1742-6596/2157/1/012019
17. Mursyidah I. L., Dafik, & A. I. Kristiana. 2023. On Rainbow Antimagic Coloring of Some Classes of Graphs. *Advances in Physics Research Proceedings of the 6th International Conference of Combinatorics, Graph Theory, and Network Topology (ICCGANT 2022)*. pp. 73-93. https://doi.org/10.2991/978-94-6463-138-8_8
18. Dafik, Mursyidah, I. L., Agustin, I. H., Baihaki, R. I., Febrinanto, F. G., Husain, S., Binti, S. K., & Sunder, R. 2024. On Rainbow Vertex Antimagic Coloring and Its Application on STGNN Time Series Forecasting on Subsidized Diesel Consumption. *IAENG International Journal of Applied Mathematics*, **54**(5).
19. Simamora, D. N. S.& Salman, A. N. M. The Rainbow (Vertex) Connection Number of Pencil Graphs. *Procedia Computer Science*. **74** 138-142 (2015). https://doi.org/10.1016/j.procs.2015.12.089
20. Mohamad, M. S. A., Din, R., & Ahmad, J. I. (2021). Research trends review on RSA scheme of asymmetric cryptography techniques. *Bulletin of Electrical Engineering and Informatics*, **10**(1), 487-492.
21. Hammad, B. T., Sagheer, A. M., Ahmed, I. T., & Jamil, N. (2020). A comparative review on symmetric and asymmetric DNA-based cryptography. *Bulletin of Electrical Engineering and Informatics*, **9**(6), 2484-2491.
22. Santoso, K. A., Cristyanto, F. G., Halikin, I., & Alfarisi, R. (2024). Advancing Graph Theory with Genetic Algorithms: AFocus on Non-Inclusive Vertex Irregular Labeling. European Journal of Pure and Applied Mathematics, 17(4), 3994-4002.
23. Santoso, K. A., Agustin, I. H., Prihandini, R. M., & Alfarisi, R. (2019, April). Vertex colouring using the adjacency matrix. In Journal of Physics: Conference Series (Vol. 1211, No. 1, p. 012019). IOP Publishing.
24. Kamsyakawuni, A., Sari, M. P., Riski, A., & Santoso, K. A. (2020, March). Metaheuristic algorithm approach to solve non-linear equations system with complex roots. In Journal of Physics: Conference Series (Vol. 1494, No. 1, p. 012001). IOP Publishing.
25. Abroshan, H. (2021). A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms. *International Journal of Advanced Computer Science and Applications*, **12**(6), 31-37.
26. Maris, I., Pradjaningsih, A., Santoso, K. A. (2023). Application of combined GSA&CSO algorithm to modified bounded knapsack with multiple constraints problem against uncertain coefficient. 080011. https://doi.org/10.1063/5.0107520
27. Agung, K., Fatmawati, Suprajitno, H. (2018). Image encryption based on pixel bit modification. Journal of Physics: Conference Series, 1008, 012016. https://doi.org/10.1088/1742-6596/1008/1/012016
28. Santoso, K. A., Fatmawati, Suprajitno, H. (2018). On Max-Plus Algebra and Its Application on Image Steganography. Scientific World Journal, 2018. https://doi.org/10.1155/2018/6718653
29. Santoso, K. A., Dafik, Agustin, I. H., Prihandini, R. M., Alfarisi, R. (2019). Vertex colouring using the adjacency matrix. Journal of Physics: Conference Series, 1211(1). https://doi.org/10.1088/1742-6596/1211/1/012019
30. Santoso, K. A., Sukmawati, R. A., Pradjaningsih, A. (2022). Image security development using 3D playfair cipher combination and bit shift. AIP Conference Proceeding, 020013. https://doi.org/10.1063/5.0079220
31. Pradjaningsih, A., Anggraeni, D. M., Santoso, K. A. (2022). ANALYTICAL HIERARCHY PROCESS IN DETERMINING LEVEL THE FEASIBILITY OF THE AUTOMATED TELLER MACHINE LOCATION (CASE STUDY BANK SYARIAH INDONESIA JEMBER). BAREKENG: Jurnal Ilmu Matematika Dan Terapan, 16(3), 1115–1122. https://doi.org/10.30598/barekengvol16iss3pp1115-1122
32. Santoso, K. A., Kamsyakawuni, A; Riski, A. (2019). Hiding the Text into An Image by Max-Plus Algebra. Proceedings - 2019 International Conference on Computer Science, Information Technology, and Electrical Engineering, ICOMITEE 2019. https://doi.org/10.1109/ICOMITEE.2019.8921210
33. Santoso, K. A., Ilmiyah, I. M., Pradjaningsih, A. (2024). Optimizing the Arrangement of Goods in Box Van Using the Tabu Search Algorithm. Statistics, Optimization Information Computing, 13(4), 1472–1479. https://doi.org/10.19139/soic-2310-5070-2151
34. Santoso, K. A., Yusnita, A. R., Pradjaningsih, A. (2024). SCHEDULING ANALYSIS BEDUGUL VILLA CONSTRUCTION PROJECT USING PERT AND CPM METHODS. BAREKENG: Jurnal Ilmu Matematika Dan Terapan, 18(1), 0105–0116. https://doi.org/10.30598/barekengvol18iss1pp0105-0116
35. Agustin, I. H., Dafik, Baihaki, R. I., Marsidi, Santoso, K. A. (2024). Irregular Reflexive Labeling and Elementary Row Operations for Enhanced Biometric Image Encryption. Journal of Computer Science, 20(12), 1766–1777. https://doi.org/10.3844/jcssp.2024.1766.1777
36. Pradjaningsih, A., Rozi, M. F., Santoso, K. A. (2024). Strategical level assessment of bank offices location using analytical hierarchy process method. 020010. https://doi.org/10.1063/5.0211372
37. Santoso, K. A., Kamsyakawuni, A., Seggaf, M. (2022). MEDICAL IMAGE ENCRYPTION USING DNA ENCODING AND MODIFIED CIRCULAR SHIFT. BAREKENG: Jurnal Ilmu Matematika Dan Terapan, 16(1), 235–242. https://doi.org/10.30598/barekengvol16iss1pp233-240