JTAM (Jurnal Teori dan Aplikasi Matematika)
http://journal.ummat.ac.id/index.php/jtam
p-ISSN 2597-7512 | e-ISSN 2614-1175
Vol. 9, No. 1, January 2025, pp. 314-330

Analysis of Rainbow Vertex Antimagic Coloring and its Application to Cryptographic Secret Sharing with Affine Cipher Technique

Dafik[1,3*], Iftitahul Firdausiyah[2], Robiatul Adawiyah[2,3], Ika Hesti Agustin[1,3], Indah Lutfiyatul Mursyidah[3], Marsidi[4]
[1]Department of Mathematics, University of Jember, Indonesia
[2]Department of Mathematics Education, University of Jember, Indonesia
[3]Department PUI-PT Combinatorics and Graph, CGANT, University of Jember, Indonesia
[4]Department of Mathematics Education, Universitas PGRI Argopuro Jember, Indonesia
d.dafik@unej.ac.id

Article History:
Received : 23-11-2024
Revised : 10-01-2025
Accepted : 11-01-2025
Online : 31-01-2025

Keywords:
Rainbow Vertex Antimagic Coloring;
Secret Sharing;
Affine Cipher.

ABSTRACT

Rainbow vertex antimagic coloring is a novel concept in graph theory that combines rainbow vertex connection with antimagic labeling. Rainbow vertex connection is a vertex coloring where each vertex in a simple connected graph $G = (V, E)$ is connected by a path such that all interior vertices have distinct colors. The antimagic labeling assigns a bijective function $f: E(G) \rightarrow \{1, 2, 3, \dots, |E(G)|\}$ to the edges, and the vertex weight $w_{f(v)} = \sum_{e \in E(v)} f(e)$, where $E(v)$ is the set of edges adjacent to vertex v. A graph G achieves rainbow vertex antimagic coloring if all its internal vertices have unique vertex weights. This research investigates the application of rainbow vertex antimagic coloring to Shadow $D_2(S_n)$ graphs and $Amal(V_n, v, m)$ graphs in cryptographic secret sharing and encryption using the affine cipher technique. The study employs mathematical modeling, graph visualization tools, and cryptographic software to ensure methodological rigor. The encryption and decryption processes are evaluated based on effectiveness, including brute force test resistance, encryption time, and encryption size. The results demonstrate that rainbow vertex antimagic coloring is an effective method for dividing cryptographic keys into segments during the secret sharing stage and serves as a robust key in the affine cipher technique. The method offers significant advantages, including faster encryption times for Shadow $D_2(S_n)$ graphs compared to $Amal(V_n, v, m)$ graphs and reduced encryption size for $Amal(V_n, v, m)$ graphs. Both graphs exhibited strong resistance to brute force attacks. In conclusion, this study highlights the relevance of rainbow vertex antimagic coloring in advancing graph theory applications and its utility in developing secure and efficient cryptographic systems. These findings contribute to bridging theoretical graph concepts with practical cryptographic implementations.

https://doi.org/10.31764/jtam.v9i1.28037

A. INTRODUCTION

A graph G is defined as a pair of sets $(V(G), E(G))$, where $V(G)$ is a finite nonempty set of elements called vertices, and $E(G)$ is a (possibly empty) set of unordered pairs (u, v) of elements in $V(G)$, called edges (Alfarisi et al., 2019; Gembong et al., 2017). In graph theory, two fundamental concepts describe the structure of a graph: order and size. The order of a graph G, denoted by $|V(G)|$, refers to the number of vertices, while the size, denoted by $|E(G)|$, represents the number of edges (Dafik et al., 2017, 2018; Kristiana et al., 2023; Mursyidah et al., 2021).

Rainbow vertex antimagic coloring is a recently developed concept that integrates two key ideas: rainbow vertex coloring and antimagic labeling (Marsidi et al., 2021). Rainbow vertex coloring assigns colors to vertices so that every pair of vertices is connected by a path where all internal vertices have different colors. The minimal number of colors required for such an assignment is called the rainbow vertex connection number $rvc(G)$. Various studies have investigated rainbow vertex connection, including those by (Akadji et al., 2021; Fauziah et al., 2019; Heggernes et al., 2018; Li & Shi, 2013; Mursyidah et al., n.d.; Simamora & Salman, 2015), exploring its properties, algorithms, and practical applications.

On the other hand, antimagic labeling of graphs involves assigning labels from $\{1,2,\cdots,|E(G)|\}$ to the edges of a graph G such that the sum of edge labels incident to any two vertices is distinct (Mursyidah et al., 2023; Septory et al., 2021; Wulandari & Simanjuntak, 2023). For instance, Wulandari & Simanjuntak (2023) studied the distance antimagic labeling of product graphs, while Cesati (2023) explored its applications in RSA cryptographic systems, emphasizing the intersection of graph theory and cryptography.

Rainbow vertex antimagic coloring combines these two concepts. For a simple connected graph $G = (V, E)$, a bijective function $f: E(G) \rightarrow \{1, 2, 3, \cdots, E(G)\}$ is defined, and the edge weight $w(v)$ of a vertex $v \in V(G)$ is given by $w(v) = \sum_{e \in E(v)} f(e)$, where $E(v)$ represents the set of edges incident to v. A graph G is said to have a rainbow vertex antimagic coloring if all its internal vertices have distinct edge weights (Marsidi et al., 2021). The smallest number of colors required for such a coloring is denoted by $rvac(G)$. This concept has been further developed in recent studies (Agustin et al., 2024; Dafik et al., 2024; Kamila et al., 2023; Marsidi et al., 2022).

Despite its growing significance, the integration of rainbow vertex antimagic coloring (RVAC) with cryptographic techniques has been explored in constructing encryption keystreams (Agustin et al., 2024; Nisviasari et al., 2022). However, prior studies have not addressed the potential of RVAC in advanced cryptographic frameworks, particularly in asymmetric cryptography and secure secret sharing schemes. This research seeks to bridge this gap by investigating the application of RVAC to enhance the robustness and security of these cryptographic methods.

Cryptography, originating from the Greek words cryptos (secret) and graphein (writing), involves the processes of encryption and decryption (Khan et al., 2020). Two primary types of cryptography exist: symmetric and asymmetric. Symmetric cryptography uses the same key for encryption and decryption, while asymmetric cryptography employs a pair of keys: a public key for encryption and a private key for decryption (Mohan et al., 2022; Panahi et al., 2021). In symmetric algorithms, a conversion table is often required to map characters to numeric values for encryption and decryption. Figure 1 shows the character-to-number conversion table, essential for implementing the affine cipher, a classical cryptographic algorithm that employs keys a and b in its encryption and decryption processes. The mathematical operations are as follows:

$$\text{Encryption: } C_i = (ax + b) mod\ m$$
$$\text{Decryption: } P_i = \left(a^{-1}(x - b)\right) mod\ m$$

Where a is relatively prime to m, a^{-1} is the modular inverse of a, m is the size of the character set, and x represents the plaintext letters converted to numeric values. Secret sharing is another cryptographic technique developed by Shamir and Blakley in 1979 to divide a secret into multiple shares distributed among entities, enabling reconstruction only when a sufficient subset of shares is combined. Recent studies have focused on enhancing the efficiency and security of secret sharing in distributed systems (Krenn & Lorünser, 2023; Phalakarn et al., 2020). This study investigates the application of rainbow vertex antimagic coloring in cryptography by combining it with secret sharing schemes and affine cipher techniques. The research aims to contribute to the development of secure and efficient cryptographic systems by addressing existing gaps in the integration of advanced graph theory concepts with cryptographic methods, as shown in Figure 1.

$A \rightleftarrows 0$	$B \rightleftarrows 1$	$C \rightleftarrows 2$	$D \rightleftarrows 3$	$E \rightleftarrows 4$	$F \rightleftarrows 5$	$G \rightleftarrows 6$	$H \rightleftarrows 7$	$I \rightleftarrows 8$	$J \rightleftarrows 9$
$K \rightleftarrows 10$	$L \rightleftarrows 11$	$M \rightleftarrows 12$	$N \rightleftarrows 13$	$O \rightleftarrows 14$	$P \rightleftarrows 15$	$Q \rightleftarrows 16$	$R \rightleftarrows 17$	$S \rightleftarrows 18$	$T \rightleftarrows 19$
$U \rightleftarrows 20$	$V \rightleftarrows 21$	$W \rightleftarrows 22$	$X \rightleftarrows 23$	$Y \rightleftarrows 24$	$Z \rightleftarrows 25$	$a \rightleftarrows 26$	$b \rightleftarrows 27$	$c \rightleftarrows 28$	$d \rightleftarrows 29$
$e \rightleftarrows 30$	$f \rightleftarrows 31$	$g \rightleftarrows 32$	$h \rightleftarrows 33$	$i \rightleftarrows 34$	$j \rightleftarrows 35$	$k \rightleftarrows 36$	$l \rightleftarrows 37$	$m \rightleftarrows 38$	$n \rightleftarrows 39$
$o \rightleftarrows 40$	$p \rightleftarrows 41$	$q \rightleftarrows 42$	$r \rightleftarrows 43$	$s \rightleftarrows 44$	$t \rightleftarrows 45$	$u \rightleftarrows 46$	$v \rightleftarrows 47$	$w \rightleftarrows 48$	$x \rightleftarrows 49$
$y \rightleftarrows 50$	$z \rightleftarrows 51$	$0 \rightleftarrows 52$	$1 \rightleftarrows 53$	$2 \rightleftarrows 54$	$3 \rightleftarrows 55$	$4 \rightleftarrows 56$	$5 \rightleftarrows 57$	$6 \rightleftarrows 58$	$7 \rightleftarrows 59$
$8 \rightleftarrows 60$	$9 \rightleftarrows 61$	$! \rightleftarrows 62$	$@ \rightleftarrows 63$	$\# \rightleftarrows 64$	$\$ \rightleftarrows 65$	$\% \rightleftarrows 66$	$\hat{} \rightleftarrows 67$	$\& \rightleftarrows 68$	$* \rightleftarrows 69$
$(\rightleftarrows 70$	$) \rightleftarrows 71$	$- \rightleftarrows 72$	$\rightleftarrows 73$	$+ \rightleftarrows 74$	$= \rightleftarrows 75$	$: \rightleftarrows 76$	$; \rightleftarrows 77$	$" \rightleftarrows 78$	$< \rightleftarrows 79$
$, \rightleftarrows 80$	$> \rightleftarrows 81$	$. \rightleftarrows 82$	$? \rightleftarrows 83$	$/ \rightleftarrows 84$	$\{ \rightleftarrows 85$	$[\rightleftarrows 86$	$] \rightleftarrows 87$	$\} \rightleftarrows 88$	$// \rightleftarrows 89$
$\vert \rightleftarrows 90$	$` \rightleftarrows 91$	$\tilde{} \rightleftarrows 92$	$\rightleftarrows 93$						

Figure 1. Character to number conversion table

B. METHODS

1. Research Methods

This research utilized a combination of methods designed to achieve the objectives of analyzing and applying rainbow vertex antimagic coloring in cryptography using the affine cipher technique. The methods used include:

a. Pattern Detection Method
This method was employed to identify and construct antimagic labeling patterns that facilitate rainbow vertex antimagic coloring on predefined graphs. Specifically, it involves analyzing edge-labeling patterns and verifying that they satisfy the properties of antimagic coloring. By systematically detecting patterns, this method directly contributes to solving the research problem by ensuring that each graph adheres to the defined antimagic coloring criteria.

b. Axiomatic Deductive Method
The axiomatic deductive method involves applying established theorems and logical reasoning to prove new theorems related to rainbow vertex antimagic coloring. This method ensures mathematical rigor by utilizing previously validated results, such as Lemma 1 and Lemma 2, as foundational tools to derive new results. The relevance of the lemmas lies in their ability to establish bounds and constraints, which are crucial for proving the properties of rainbow vertex connection and antimagic coloring on the

selected graphs.

Lemma 1 Suppose G is a connected graph with $diam(G)$, then $rvc(G) \geq diam(G) - 1$ (Marsidi et al., 2022).

Lemma 2 Suppose G is a connected graph, $rvac(G) \geq rvc(G)$ (Marsidi et al., 2021).

c. Applicative Method

The applicative method was used to address practical problems in cryptography, specifically the encryption and decryption processes using affine cipher techniques. This method leverages the findings from the pattern detection and axiomatic deductive methods to develop encryption keys and implement the cryptographic algorithm. By translating theoretical results into practical applications, this method demonstrates the utility of the research in real-world contexts, particularly in secure data communication.

2. Research Subjects

The subjects of this research were two types of graphs: Shadow graphs and Volcano amalgamation graphs. These graphs were chosen due to their structural properties, which make them suitable for demonstrating and testing the concepts of rainbow vertex antimagic coloring.

3. Research Instruments

The primary instruments used in this research include:

a. Mathematical models and equations: To represent and analyze the properties of the graphs.
b. Graph visualization tools: To illustrate the rainbow vertex antimagic coloring and its application in encryption.
c. Cryptographic tools: Software applications to implement and test the affine cipher technique.

4. Data Analysis Technique

The data analysis involved:

a. Verification of Coloring Properties: Ensuring that the generated patterns satisfy the rainbow vertex antimagic coloring criteria.
b. Theorem Proofs: Using logical and mathematical reasoning to establish new results related to the rainbow vertex connection and antimagic coloring.
c. Performance Evaluation: Assessing the effectiveness of the cryptographic application through brute force analysis, encryption time measurement, and byte size comparison. The security level of the encryption was also analyzed to validate the robustness of the method.

By integrating these methods and analysis techniques, the study establishes a robust framework for exploring the theoretical and practical aspects of rainbow vertex antimagic coloring and its cryptographic applications.

C. RESULT AND DISCUSSION

This research produces two theorems related to rainbow vertex connection numbers on the Shadow $D_2(S_n)$ and $Amal(V_n, a, m)$ graphs, as well as two theorems on rainbow vertex antimagic connection numbers for the same graphs. These theorems are further applied to cryptographic secret sharing utilizing the affine cipher technique. In this section, we first discuss the mathematical properties of the graphs, including the proofs for rainbow vertex connection and antimagic connection numbers. Subsequently, the practical applications of these concepts in cryptographic secret sharing are elaborated, emphasizing key sharing mechanisms and their integration with encryption and decryption processes. Finally, we provide a detailed analysis of the security, efficiency, and effectiveness of the proposed method, including comparisons of encryption time and size between the graph types. This comprehensive discussion bridges the theoretical findings with their real-world applications in secure data systems.

1. Rainbow Vertex Connection Number and Rainbow Vertex Antimagic Connection Number

Theorem 1 Rainbow vertex connection number on Shadow graph $D_2(S_n)$ for $n \geq 3$ is 1.

Proof. $D_2(S_n)$ is a shadow graph with vertex set $V(D_2(S_n)) = \{x_i;\ 1 \leq i \leq n\} \cup \{y_i;\ 1 \leq i \leq n\} \cup \{x\} \cup \{y\}$ and edge set $E(D_2(S_n)) = \{xx_i;\ 1 \leq i \leq n\} \cup \{xy_i;\ 1 \leq i \leq n\} \cup \{yx_i;\ 1 \leq i \leq n\} \cup \{yy_i;\ 1 \leq i \leq n\}$. The cardinality of the edge set and vertex set of the shadow graph $D_2(S_n)$ are $|V(D_2(S_n))| = 2n + 2$ and $|E(D_2(S_n))| = 4n$ respectively. First, we will show the lower bound of $rvc(D_2(S_n))$. $D_2(S_n)$ has a diameter which is $diam(D_2(S_n)) = 2$. Based on Lemma 1, it follows that $rvc(D_2(S_n)) \geq 1$. Secondly, we will show the upper bound of $rvc(D_2(S_n))$ by define the vertex function as follows:

$$f(x) = f(y) = f(x_i) = f(y_i) = 1; i = n \quad (1)$$

The rainbow path of $u - v$ can be seen in Table 1. Based on Table 1, it is known that every path $u - v$ has a rainbow path or in other words, every path in the Shadow graph has an interior vertex with a different color, thus fulfilling the concept of rainbow vertex coloring. Based on the vertex function above, it is proven that $rvc(D_2(S_n)) \leq 1$. Based on the lower bound and upper bound, we have $1 \leq rvc(D_2(S_n)) \leq 1$. Therefore, it is proven that $rvc(D_2(S_n)) = 1$.

Table 1. Rainbow Path on Shadow graph $D_2(S_n)$

Case	*u*	*v*	Rainbow path	Condition
1	x	y	x, x_i, y	$1 \leq i \leq n$
2	y	x	y, y_i, x	$1 \leq i \leq n$
3	x_i	y_i	x_i, x, y_i	$1 \leq i \leq n$
4	y_i	x_i	y_i, y, x_i	$1 \leq i \leq n$

An illustration of rainbow vertex coloring can be seen in Figure 2 which is an example of rainbow vertex coloring on Shadow graph $D_2(S_3)$. In Figure 2, $rvc(D_2(S_3)) = 1$ is also obtained.

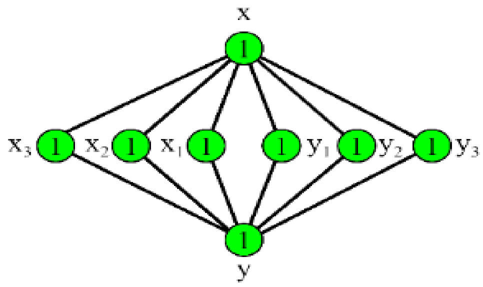

Figure 2. Rainbow Vertex Coloring of $D_2(S_3)$

Theorem 2 Rainbow vertex antimagic connection number on Shadow graph $D_2(S_n)$ for $n \geq 3$ is 2.

Proof. $D_2(S_n)$ is a shadow graph with vertex set $V(D_2(S_n)) = \{x_i;\ 1 \leq i \leq n\} \cup \{y_i;\ 1 \leq i \leq n\} \cup \{x\} \cup \{y\}$ and edge set $E(D_2(S_n)) = \{xx_i;\ 1 \leq i \leq n\} \cup \{xy_i;\ 1 \leq i \leq n\} \cup \{yx_i;\ 1 \leq i \leq n\} \cup \{yy_i;\ 1 \leq i \leq n\}$. The cardinality of the edge set and vertex set in Shadow graph $D_2(S_n)$ are $|V(D_2(S_n))| = 2n + 2$ and $|E(D_2(S_n))| = 4n$, respectively. First, we will show the lower bound of $rvac(D_2(S_n))$. Based on Lemma 2, we have $rvac(D_2(S_n)) \geq rvc(D_2(S_n)) = 1.\}$ Next, we assume $rvac(D_2(S_n)) = 1$, then $w(x) = w(x_i) = w(y_i) = w(y)$. Assume $w(x) = w(x_i)$, then $\sum_{i=1}^{n} f(xx_i) + \sum_{i=1}^{n} f(xy_i) = \sum_{i=1}^{n} f(xx_i) + \sum_{i=1}^{n} f(yx_i)$. Assume $w(y) = w(y_i)$, then $\sum_{i=1}^{n} f(yx_i) + \sum_{i=1}^{n} f(yy_i) = \sum_{i=1}^{n} f(xy_i) + \sum_{i=1}^{n} f(yy_i)$. Both equations show a contradiction, because $2n^2 + n \leq f(xx_i) + f(xy_i) \leq 6n^2 + n, 2n^2 + n \leq f(yx_i) + f(yy_i) \leq 6n^2 + n$ and $3 \leq f(xx_i) + f(yx_i) \leq 8n - 1, 3 \leq f(xy_i) + f(yy_i) \leq 8n - 1$. Based on Eqs. $w(x) = w(y)$ and $w(x_i) = w(y_i)$. Therefore, it can be concluded that $rvac(D_2(S_n)) \geq 2$. Next, we will show the upper bound of rainbow vertex antimagic coloring. The proof of upper bound of rainbow vertex antimagic coloring on $D_2(S_n)$ is divided into 2 cases as follows.

Case 1: For $n \equiv 1(mod\ 2)$

We will show the upper bound of rainbow vertex antimagic coloring on Shadow graphs by define the bijective function of edge labels in $D_2(S_n)$ as follows:

$$f(x_i x) = \begin{cases} 4n - i + 1, & i \equiv 1(mod\ 2) \\ i, & i \equiv 0(mod\ 2) \end{cases}$$
$$f(x_i y) = \begin{cases} i, & i \equiv 1(mod\ 2) \\ 4n - i + 1, & i \equiv 0(mod\ 2) \end{cases}$$
$$f(y_i x) = \begin{cases} 2n - i + 1, & i = 1\ or\ i \equiv 0(mod\ 2) \\ 2n + i, & i \equiv 1(mod\ 2), 1 < i < n\ or\ i = n \end{cases}$$
$$f(y_i y) = \begin{cases} 2n + i, & i = 1\ or\ i = n\ or\ i \equiv 0(mod\ 2) \\ 2n - i + 1, & i \equiv 1(mod\ 2), 1 < i < n \end{cases} \quad (2)$$

Based on the label function, we have the vertex weight function as follows:

$$w(x) = w(y) = 4n^2 + n$$
$$w(x_i) = w(y_i) = 4n + 1, 1 \leq i \leq n \quad (3)$$

Based on the vertex weight, we get $|w(V(D_2(S_n)))| = 2$. The rainbow path of $u - v$, derived from the vertex weight function above, can be seen in Table 1. As shown in Table 1, each distinct vertex in the Shadow graph is connected by a rainbow path, consistent with the definition of rainbow vertex antimagic coloring. From the lower and upper bounds, it can be concluded that $2 \leq rvac\big(D_2(S_n)\big) \leq 2$. Thus, it is proven that $rvac(D_2(S_n)) = 2$. An illustration of rainbow vertex antimagic coloring in Shadow graph can be seen in Figure 3. Figure 3 is an example of rainbow vertex antimagic coloring in Shadow graph $D_2(S_3)$ and also obtained rainbow vertex antimagic connection number which is $rvac(D_2(S_3)) = 2$.

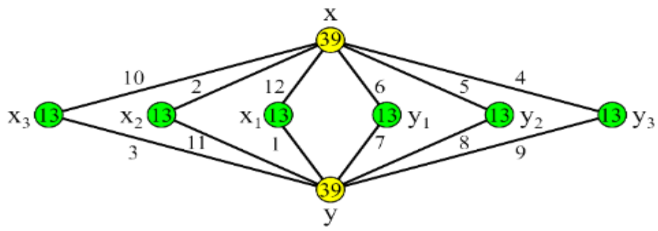

Figure 3. Rainbow Vertex Antimagic Coloring of $D_2(S_3)$

Case 2: For $n \equiv 0(mod\ 2)$
We will show the upper bound of rainbow vertex antimagic coloring on Shadow graphs by define the bijective function of edge labels in $D_2(S_n)$ as follows:

$$f(x_ix) = \begin{cases} 4n - i + 1, & i \equiv 1(mod\ 2) \\ i, & i \equiv 0(mod\ 2) \end{cases}$$
$$f(x_iy) = \begin{cases} i, & i \equiv 1(mod\ 2) \\ 4n - i + 1, & i \equiv 0(mod\ 2) \end{cases}$$
$$f(y_ix) = \begin{cases} 2n - i + 1, & i \equiv 0(mod\ 2) \\ 2n + i, & i \equiv 1(mod\ 2) \end{cases} \quad (4)$$
$$f(y_iy) = \begin{cases} 2n + i, & i \equiv 0(mod\ 2) \\ 2n - i + 1, & i \equiv 1(mod\ 2) \end{cases}$$

Based on the label function, we have the vertex weight function as follows:

$$w(x) = w(y) = 4n^2 + n$$
$$w(x_i) = w(y_i) = 4n + 1 \quad (5)$$

Based on the vertex weight, we get $|w(V(D_2(S_n)))| = 2$. The rainbow path of $u - v$, derived from the vertex weight function above, can be seen in Table 2. As shown in Table 2, each distinct vertex in the Shadow graph is connected by a rainbow path, consistent with the definition of rainbow vertex antimagic coloring. From the lower and upper bounds, it can be concluded that $2 \leq rvac\big(D_2(S_n)\big) \leq 2$. Thus, it is proven that $rvac(D_2(S_n)) = 2$. An illustration of rainbow vertex antimagic coloring in Shadow graph can be seen in Figure 4. Figure 4 is an example of rainbow vertex antimagic coloring in Shadow graph $D_2(S_4)$ and also obtained rainbow vertex antimagic connection number which is $rvac(D_2(S_4)) = 2$.

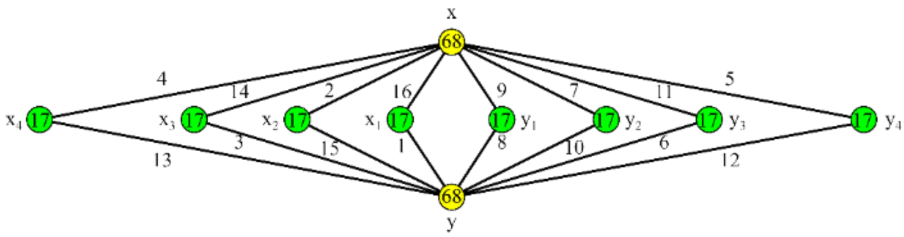

Figure 4. Rainbow Vertex Antimagic Coloring of $D_2(S_4)$

Theorem 3 Rainbow vertex connection number on the $Amal(V_n, a, m)$ graph for $n \geq 3$ and $m \geq 2$ is 1.

Proof. $Amal(V_n, a, m)$ is a volcano amalgamation graph with vertex set $V\big(Amal(V_n, a, m)\big) = \{x_i;\ 1 \leq\ i \leq\ m\} \cup \{y_i;\ 1 \leq\ i \leq\ m\} \cup \{z_{i,j};\ 1 \leq\ i \leq\ m, 1 \leq\ j \leq\ n\} \cup \{a\}$ and the edge set $E\big(Amal(V_n, a, m)\big) = \{x_i y_i;\ 1 \leq\ i \leq\ m\} \cup \{x_i a\ ;\ 1 \leq\ i \leq\ m\} \cup \{y_i a;\ 1 \leq\ i \leq\ m\} \cup \{z_{i,j} a;\ 1 \leq\ i \leq\ m, 1 \leq\ j \leq\ n\}$. Cardinality of the vertex set and edge set of the graph $Amal(V_n, a, m)\ are\ |V(Amal(V_n, a, m))| = 2m + mn + 1\ and\ |E(Amal(V_n, a, m))| = 3m + mn$ respectively. First, we will show the lower bound of $Amal(V_n, a, m)$. $Amal(V_n, a, m)$ has a diameter which is $diam(Amal(V_n, a, m)) = 2$. Based on Lemma 1, it follows that $rvc\big(Amal(V_n, a, m)\big) \geq\ 1$. Secondly, we will show the upper bound of $rvc(Amal(V_n, a, m))$ by define the vertex function as follows:

$$f(x_i) =\ f(y_i) = f(a) = f\big(z_{i,j}\big) = 1; 1 \leq\ i \leq\ m, 1 \leq\ j \leq\ n \qquad (6)$$

The rainbow path of $u - v$ can be seen in Table 2. Based on Table 2, it is known that every path $u - v$ has a rainbow path or in other words, every path in the $Amal(V_n, a, m)$ has an interior vertex with a different color, thus fulfilling the concept of rainbow vertex coloring. Based on the vertex function above, it is proven that $rvc\big(Amal(V_n, a, m)\big) \leq 1$. Based on the lower bound and upper bound, we have $1 \leq rvc\big(Amal(V_n, a, m)\big) \leq 1$. Therefore, it is proven that $rvc(Amal(V_n, a, m)) = 1$.

Table 2. Rainbow Path on the $Amal(V_n, a, m)$ for $n \geq 3$ and $m \geq 2$

Case	u	v	Rainbow path	Condition
1	x_i	x_k	x_i, a, x_k	$1 \leq i \leq m, 1 \leq k \leq m$
2	x_i	y_i	x_i, a, y_i	$1 \leq i \leq m$
3	x_i	$z_{i,j}$	$x_i, a, z_{i,j}$	$1 \leq i \leq m, 1 \leq j \leq n$
4	a	x_i	a, x_i	$1 \leq i \leq m$
5	a	y_i	a, y_i	$1 \leq i \leq m$
6	a	$z_{i,j}$	$a, z_{i,j}$	$1 \leq i \leq m, 1 \leq j \leq n$

An illustration related to rainbow vertex coloring can be seen in Figure 5. which is an example of rainbow vertex coloring on the graph $Amal(V_3, a, 2)$. In Figure 5. it is also obtained that $rvc(Amal(V_3, a, 2)) = 1$.

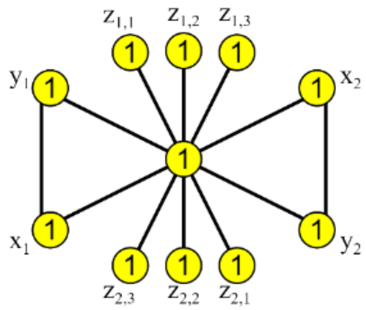

Figure 5. Rainbow Vertex Coloring of $Amal(V_3, a, 2)$

Theorem 4 Rainbow vertex antimagic connection number on the $Amal(V_n, a, m)$ graph for $n \geq 3$ and $m \geq 2$ is mn +1.

Proof. $Amal(V_n, a, m)$ is a volcano amalgamation graph with vertex set $V(Amal(V_n, a, m)) = \{x_i;\ 1 \leq i \leq m\} \cup \{y_i;\ 1 \leq i \leq m\} \cup \{z_{i,j};\ 1 \leq i \leq m, 1 \leq j \leq n\} \cup \{a\}$ and the edge set $E(Amal(V_n, a, m)) = \{x_i y_i;\ 1 \leq i \leq m\} \cup \{x_i a\ ;\ 1 \leq i \leq m\} \cup \{y_i a;\ 1 \leq i \leq m\} \cup \{z_{i,j} a;\ 1 \leq i \leq m, 1 \leq j \leq n\}$. Cardinality of the vertex set and edge set of the graph $Amal(V_n, a, m)\ are\ |V(Amal(V_n, a, m))| = 2m + mn + 1\ and\ |E(Amal(V_n, a, m))| = 3m + mn$ respectively. First, we will show the lower bound of $rvac(Amal(V_n, a, m))$. Based on Lemma 2, we have $rvac(Amal(V_n, a, m)) \geq rvc(Amal(V_n, a, m)) = 1$. The graph $Amal(V_n, a, m)$ has mn star vertices. Assuming $rvac(Amal(V_n, a, m)) = 1$, it contradicts the definition of antimagic labeling. Hence, $rvac(Amal(V_n, a, m)) \geq mn$. The graph $Amal(V_n, a, m)$ has a central vertex of degree $mn + 2m$. Suppose $rvac(Amal(V\_n, a, m)) = mn$, then the weight of the central vertex is equal to one of the weights of the vertices neighboring the central vertex such that $w(a) = w(x_i)$ or $w(a) = w(y_i)$ or $w(a) = w(z_{i,j})$. Assume $w(a) = w(x_i)$, then $\sum_{i=1}^{m} f(x_i a) + \sum_{i=1}^{m} f(y_i a) + \sum_{i=1}^{m} \sum_{j=1}^{n} f(z_{i,j} a) = \sum_{i=1}^{m} f(x_i a) + \sum_{i=1}^{m} f(x_i y_i)$. Then assume $w(a) = w(y_i)$, then $\sum_{i=1}^{m} f(x_i a) + \sum_{i=1}^{m} f(y_i a) + \sum_{i=1}^{m} \sum_{j=1}^{n} f(z_{i,j} a) = \sum_{i=1}^{m} f(y_i a) + \sum_{i=1}^{m} f(x_i y_i)$. Next assume $w(a) = w(z_{i,j})$, then $\sum_{i=1}^{m} f(x_i a) + \sum_{i=1}^{m} f(y_i a) + \sum_{i=1}^{m} f(x_i a) + \sum_{i=1}^{m} \sum_{j=1}^{n} f(z_{i,j} a) = \sum_{i=1}^{m} \sum_{j=1}^{n} f(z_{i,j} a)$. The three equations show a contradiction, because $w(a) = 2m^2 + m + \frac{4m^2 n + mn + m^2 n^2}{2}$, $3 \leq w(x_i) \leq 4m - 1, 3 \leq w(y_i) \leq 4m - 1, 1 \leq w(z_{i,j}) \leq mn$. Based on this condition, it is found that $w(a)$ is not equal to $w(x_i), w(y_i)$, and $w(z_{i,j})$. Therefore, $rvac(Amal(V_n, a, m)) \geq mn + 1$. Second, we will show the upper bound of rainbow vertex antimagic coloring in the graph $Amal(V_n, a, m)$. We will show the upper bound by define the bijective function of edge labels in $Amal(V_n, a, m)$ as follows:

$$
\begin{gathered}
f(x_i a) = 2i - 1; 1 \leq i \leq m \\
f(y_i a) = 2i; 1 \leq i \leq m \\
f(x_i y_i) = 3m - i + 1; 1 \leq i \leq m \\
f(z_{i,j} a) = 3m + n(i - 1) + j; 1 \leq i \leq m, 1 \leq j \leq n
\end{gathered} \tag{7}
$$

Based on the label function, we have the vertex weight function as follows:

$$\begin{aligned} w(x_i) &= 3m + i; 1 \leq i \leq m \\ w(y_i) &= 3m + i + 1; 1 \leq i \leq m \\ w(z_{i,j}) &= 3m + n(i-1) + j; 1 \leq i \leq m, 1 \leq j \leq n \\ w(a) &= 2m^2 + m + \frac{m^2n^2 + 6m^2n + mn}{2} \end{aligned} \tag{8}$$

Based on the vertex weights, we conclude that the number of different colors in the graph $Amal(V_n, a, m)$ is determined by the set of weights $W(z_{i,j}) = \{mn+1, mn+2, mn+3, \dots, 2mn\}$. From this set, we can determine the number of different weights on $w(z_{i,j})$. To find the number of vertex weights, we use the arithmetic sequence formula $U_s = a + (s-1)b$. The solution using this formula is shown below:

$$\begin{aligned} U_s &= a + (s-1)b \\ 2mn &= mn + 1 + (s-1)1 \\ s &= mn \end{aligned} \tag{9}$$

If each vertex weight corresponds to a single color, then it is equal to 1, specifically when $w(a) = 2m^2 + m + \frac{m^2n^2+6m^2n+mn}{2}$. Therefore, when combined with the sum of the edge weights $w(z_{i,j}) = mn + i; 1 \leq i \leq m, 1 \leq j \leq n$, it results in a total number of colors $1 + mn = mn + 1$, proving that there are $mn + 1$ colors in the graph $Amal(V_n, a, m)$. From the lower and upper bounds, it can be concluded that $mn + 1 \leq rvac(Amal(V_n, a, m)) \leq mn + 1$. Thus, it is proven that $rvac(Amal(V_n, a, m)) = mn + 1$. To show that every two distinct vertices on the graph $Amal(V_n, a, m)$ are connected by a rainbow path can be seen in Table 4. An illustration of rainbow vertex antimagic coloring on the graph $Amal(V_n, a, m)$ can be seen in **Figure 6**. Figure 6 is an example of rainbow vertex antimagic coloring on the graph $Amal(V_3, a, 3)$ and also obtained rainbow vertex antimagic connection number which is $rvac(Amal(V_3, a, 3)) = 10$.

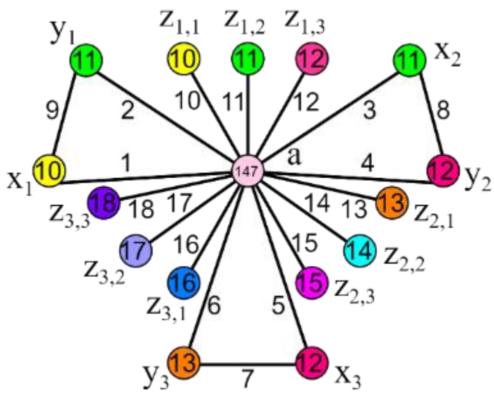

Figure 6. Rainbow Vertex Antimagic Coloring of $Amal(V_3, a, 3)$

2. Application of Rainbow Vertex Antimagic Coloring in Cryptography with Affine Cipher Technique

The application of rainbow vertex antimagic coloring in secret sharing cryptography is used to back up a message by dividing the cryptographic key into several parts. rainbow vertex antimagic coloring has an edge label that is used as secret sharing. The graphs used as secret sharing are shadow graphs $D_2(S_3)$ and $D_2(S_4)$ with $D_2(S_3)$ can reconstruct the edge label pattern with $n \equiv 1 \ (mod\ 2)\ and\ D_2(S_4)$ can reconstruct the edge label pattern with $n \equiv 0 \ (mod\ 2)$ and the graph $Amal(V_3, a, 2)$ can reconstruct the edge label pattern on the graph $Amal(V_n, a, m)$.

To find out the edge labeling pattern of the Shadow graph $D_2(S_n)$, we have to share 2 edge labeling patterns i.e. at least to 12 people using the Shadow graph $D_2(S_3)$ and share the edge labeling pattern at least to 16 people using from the Shadow graph $D_2(S_4)$. Therefore, 12 people get 2 edge label functions namely from Shadow graph $D_2(S_3)$ and from Shadow graph $D_2(S_4)$ and 4 people get 1 edge label function from Shadow graph $D_2(S_4)$. Meanwhile, to find out the edge labeling pattern of the graph $Amal(V_n, a, m)$ by sharing the edge labeling pattern which is at least 12 people using the graph $Amal(V_3, a, 2)$. The key sharing or edge label pattern sharing can be seen in Table 3.

Table 3. Key division or edge label pattern sharing

Key Division	**Shadow Graph $D_2(S_3)$**	**Shadow Graph $D_2(S_4)$**	**Graph $Amal(V_3, a, 2)$**
First person	$f(yx_1) = 1$	$f(yx_1) = 1$	$f(ax_1) = 1$
Second person	$f(xx_2) = 2$	$f(xx_2) = 2$	$f(ay_1) = 2$
Third person	$f(yx_3) = 3$	$f(yx_3) = 3$	$f(ax_2) = 3$
Fourth person	$f(xy_3) = 4$	$f(xx_4) = 4$	$f(ay_2) = 4$
Fifth person	$f(xy_2) = 5$	$f(xy_4) = 5$	$f(x_2y_2) = 5$
Sixth person	$f(xy_1) = 6$	$f(yy_3) = 6$	$f(x_1y_1) = 6$
Seventh person	$f(yy_1) = 7$	$f(xy_2) = 7$	$f(az_{1,1}) = 7$
Eighth person	$f(yy_2) = 8$	$f(yy_1) = 8$	$f(az_{1,2}) = 8$
Ninth person	$f(yy_3) = 9$	$f(xy_1) = 9$	$f(az_{1,3}) = 9$
Tenth person	$f(xx_3) = 10$	$f(yy_2) = 10$	$f(az_{2,1}) = 10$
Eleventh person	$f(yx_2) = 11$	$f(xy_3) = 11$	$f(az_{2,2}) = 11$
Twelfth person	$f(xx_1) = 12$	$f(yy_4) = 12$	$f(az_{2,3}) = 12$
Thirteenth person		$f(yx_4) = 13$	
Fourteenth person		$f(xx_3) = 14$	
Fifteenth person		$f(yx_2) = 15$	
Sixteenth person		$f(xx_1) = 16$	

The division of the edge label above is used to create a general function of the edge label so as to get the vertex weight function when the minimum number is gathered. The vertex weight is used for the key in Cryptography with affine cipher technique.

a. Encryption Process

Encryption using Shadow graph $D_2(S_n)$ as follows:

1) The plaintext to be encrypted is **UNEJ, 29!**. The cardinality of the Plaintext is 9 or $|P| = 9$.
2) The values of x_i in the above Plaintext are $\{20, 13, 4, 9, 80, 93, 54, 61, 62\}$ respectively.

3) Determine n in the Shadow graph $D_2(S_n)$ according to the length of the Plaintext with the formula $\lceil\frac{|P|-2}{2}\rceil$. Then the required n is $n = \lceil\frac{|P|-2}{2}\rceil = 4$ or the required graph is Shadow graph $D_2(S_4)$. The Shadow graph $D_2(S_4)$ can be seen in Figure 7.

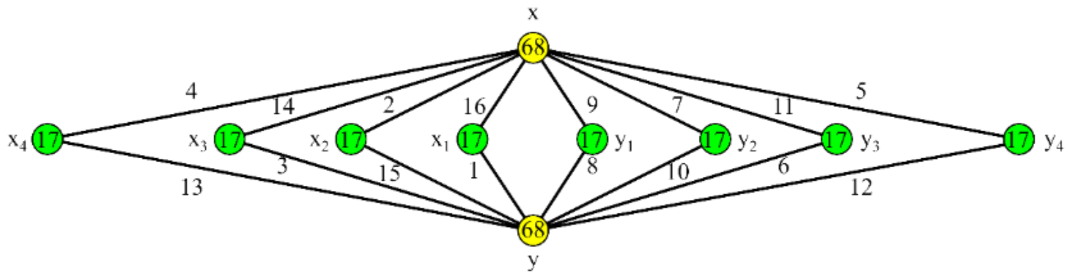

Figure 7. Shadow graph $D_2(S_4)$ in the encryption process

4) The set of edge labels in the Shadow graph $D_2(S_4)$ is $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$. The largest edge label that is relatively prime to $m = 94$ is 15. Hence, the key $a = 15$. The key sequence b, i.e. $\{x, y, x_i, y_i\}$. The cardinality of the vertex weight of the Shadow graph $D_2(S_4)$ is 10, but the one used as key b is as many as the Plaintext which is 9. Hence, key b is $\{68, 68, 17, 17, 17, 17, 17, 17, 17\}$. The placement of plaintext in the encryption process of Shadow graph $D_2(S_4)$ can be seen in **Figure 8**.

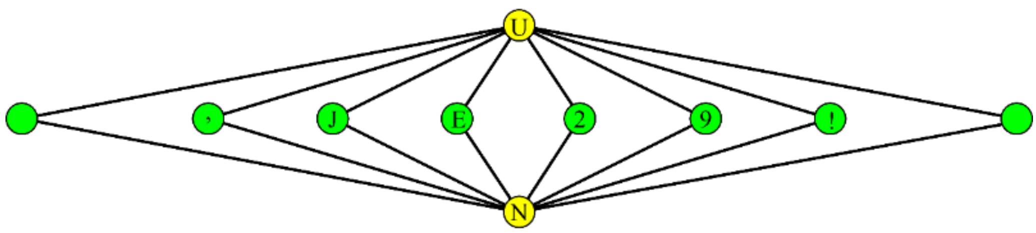

Figure 8. Placement of plaintext in Shadow graph encryption process $D_2(S_4)$

5) Find C_i with formula $C_i = (ax_i + b_i) mod\ 94$
   "U" : $(ax_1 + b_1) mod\ 94 = (15 \times 20 + 68) mod\ 94 = 368\ mod\ 94 = 86$
   "N" : $(ax_2 + b_2) mod\ 94 = (15 \times 13 + 68) mod\ 94 = 263\ mod\ 94 = 75$
   "E" : $(ax_3 + b_3) mod\ 94 = (15 \times 4 + 17) mod\ 94 = 77\ mod\ 94 = 77$
   "J" : $(ax_4 + b_4) mod\ 94 = (15 \times 19 + 17) mod\ 94 = 152\ mod\ 94 = 58$
   "," : $(ax_5 + b_5) mod\ 94 = (15 \times 80 + 17) mod\ 94 = 1217\ mod\ 94 = 89$
   " " : $(ax_6 + b_6) mod\ 94 = (15 \times 93 + 17) mod\ 94 = 1412\ mod\ 94 = 2$
   "2" : $(ax_7 + b_7) mod\ 94 = (15 \times 54 + 17) mod\ 94 = 827\ mod\ 94 = 75$
   "9" : $(ax_8 + b_8) mod\ 94 = (15 \times 61 + 17) mod\ 94 = 932\ mod\ 94 = 86$
   "!" : $(ax_9 + b_9) mod\ 94 = (15 \times 62 + 17) mod\ 94 = 947\ mod\ 94 = 7$
6) Convert the result C_i to characters, i.e. {86,75,77,58,89,2,75,86,7} to {[, =, ; ,6,// ,C, =,[, H}. Then the ciphertext of **UNEJ, 29!** is **[=;6/C=[H**. An illustrative example of graph encryption $Amal(V_n, a, m)$ can be seen in Table 4.

Table 4. Key division or edge label pattern sharing

P	U	N	E	J	,		2	9	!
x_i	20	13	4	9	80	93	54	61	62
a	9	9	9	9	9	9	9	9	9
ax_i	180	117	36	81	720	837	486	549	558
b_i	7	8	9	10	7	8	44	8	9
$ax_i + b_i$	187	125	45	91	727	745	530	557	567
C_i	93	31	45	91	69	93	60	87	3
C		f	t	‘	*		8	]	D

b. Decryption Process

The decryption key used is the same as the key used in the encryption process. The decryption key in affine cipher is the modular inverse of the encryption key. In other words, if the encryption keys are a and b, then the decryption keys are a^{-1} and $-b$, where a^{-1} is the modular inverse of a. Next, an example of decryption using Shadow graph $D_2(S_n)$ is given as follows:

1) The ciphertext to be decrypted is [=;6//C=[H. The cardinality of the ciphertext is 9 or |P|=9.
2) The values of y_i in the Plaintext above are consecutively {86,75,77,58,89,2, 75,86,7}.
3) Determine n in the Shadow graph $D_2(S_n)$ according to the length of the Plaintext with the formula $\lceil\frac{|P|-2}{2}\rceil$. Then the required n is $n = \lceil\frac{|P|-2}{2}\rceil = 4$ or the required graph is Shadow graph $D_2(S_4)$. The Shadow graph $D_2(S_4)$ can be seen in Figure 9.

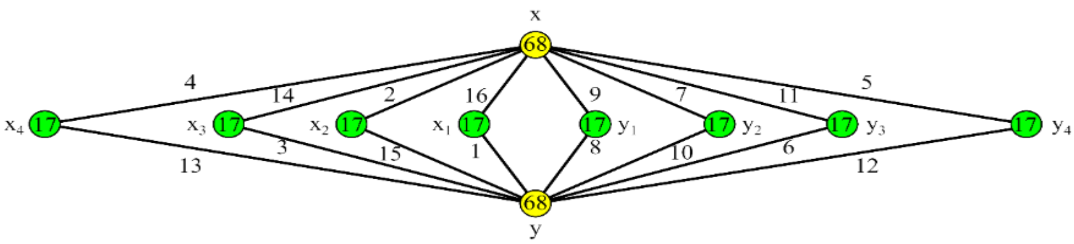

Figure 9. Shadow Graph $D_2(S_4)$ in the decryption process

4) The set of edge labels in the Shadow graph $D_2(S_4)$ is {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16}. The largest edge label relatively prime to 94 is 15. The inverse of 15 mod (94) is $a^{-1} = 69$. Hence, the key $a^{-1} = 69$. The key sequence b, i.e. $\{x, y, x_i, y_i\}$. The cardinality of the vertex weight of the Shadow graph $D_2(S_4)$ is 10, but the one used as key b is as many as the Plaintext which is 9. Hence, the key b is {68, 68, 17, 17, 17, 17, 17, 17, 17}. The placement of plaintext in the decryption process of Shadow graph $D_2(S_4)$ can be seen in Figure 10.

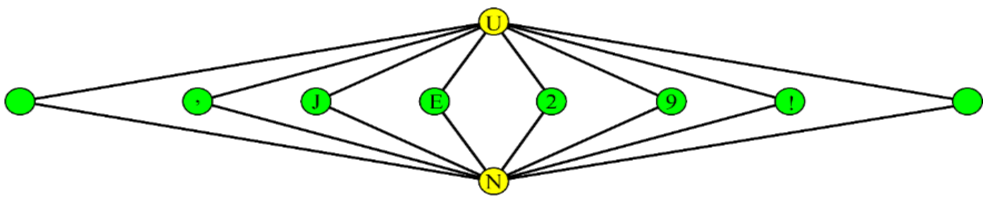

Figure 10. Placement of plaintext in Shadow graph decryption process $D_2(S_4)$

5) Find P_i with formula $P_i = a^{-1}(y_i - b_i) \ mod \ 94$
   "[" : $a^{-1}(y_1 - b_1) mod \ 94 = 69(86 - 68) mod \ 94 = 1242 \ mod \ 94 = 20$
   "=" : $a^{-1}(y_2 - b_2) mod \ 94 = 69(75 - 68) mod \ 94 = 483 \ mod \ 94 = 13$
   ";" : $a^{-1}(y_3 - b_3) mod \ 94 = 69(77 - 17) mod \ 94 = 4140 \ mod \ 94 = 4$
   "6" : $a^{-1}(y_4 - b_4) mod \ 94 = 69(58 - 17) mod \ 94 = 2829 \ mod \ 94 = 9$
   "//" : $a^{-1}(y_5 - b_5) mod \ 94 = 69(89 - 17) mod \ 94 = 4968 \ mod \ 94 = 80$
   "C" : $a^{-1}(y_6 - b_6) mod \ 94 = 69(2 - 17) mod \ 94 = -1035 \ mod \ 94 = 93$
   "=" : $a^{-1}(y_7 - b_7) mod \ 94 = 69(54 - 17) mod \ 94 = 4002 \ mod \ 94 = 54$
   "[" : $a^{-1}(y_8 - b_8) mod \ 94 = 69(61 - 17) mod \ 94 = 4761 \ mod \ 94 = 61$
   "H" : $a^{-1}(y_9 - b_9) mod \ 94 = 69(7 - 17) mod \ 94 = -690 \ mod \ 94 = 62$
6) Convert the result P_i to characters, i.e. {20, 13, 4, 9, 80, 93, 54, 61, 62}. Then the plaintext of **[=;6//C=[H** is **UNEJ, 29!**. An illustrative example of graph decryption of $Amal(V_n, a, m)$ can be seen in Table 5.

Table 5. Illustration of decryption process on graph $Amal(V_n, a, m)$

C		**f**	**t**	**'**	*****		**8**	**]**	**D**
y_i	93	31	45	91	69	93	60	87	3
a^{-1}	21	21	21	21	21	21	21	21	21
b_i	7	8	9	10	7	8	44	8	9
$y_i - b_i$	86	23	36	81	62	85	16	79	-6
$a^{-1}(y_i - b_i)$	1806	483	756	1701	1302	1785	336	1659	-126
P_i	20	13	4	9	80	93	54	61	62
P	U	N	E	J	,		2	9	!

c. Security Analysis

This subsection provides a comprehensive analysis of the encryption and decryption processes using Shadow graph $D_2(S_n)$ and $Amal(V_n, a, m)$ graphs, focusing on their resistance to attacks, efficiency in terms of encryption time, and storage requirements for encrypted data. The results are categorized into three main aspects:

1) Resistance to Brute Force Attacks

   The use of rainbow vertex antimagic coloring in cryptography significantly enhances security. By assigning unique antimagic labels to the edges of Shadow graph $D_2(S_n)$ and $Amal(V_n, a, m)$, the encryption keys become highly unpredictable, making brute force attacks infeasible. Tests conducted using Python-based brute force algorithms demonstrate that no feasible attack could successfully decode the ciphertext without the correct keys. This underscores the robustness of the method in securing sensitive information against unauthorized access.

2) Encryption Time Analysis

   The efficiency of the encryption process is a critical factor for practical applications. Table 6 shows the comparison of encryption times for different message lengths using $D_2(S_n)$ and $Amal(V_n, a, m)$.

Table 6. Comparison of encryption time (seconds)

Length encryption	16 bytes	32 bytes	64 bytes	128 bytes
Graph Shadow $D_2(S_n)$	0.042342	0.050505	0.057054	0.059752
Graph $Amal(V_n, a, m)$	0.079908	0.093868	0.096844	0.099150

From the results, it is evident that the encryption time for Shadow graph $D_2(S_n)$ is consistently faster than that of $Amal(V_n, a, m)$. This difference arises due to the simpler structure and fewer edge interactions in $D_2(S_n)$, making it more computationally efficient for encryption tasks.

3) Encryption Byte Size Analysis
In addition to encryption time, the size of encrypted data is another critical factor, especially in environments with limited storage or bandwidth. Table 7 compares the encryption size for $D_2(S_n)$ and $Amal(V_n, a, m)$.

Table 7. Comparison of encryption time (seconds)

Length encryption	16 bytes	32 bytes	64 bytes	128 bytes
Graph Shadow $D_2(S_n)$	36599	36619	36649	36723
Graph $Amal(V_n, a, m)$	36593	36615	36647	36712

The results show that the encryption size for $Amal(V_n, a, m)$ is slightly smaller than that for $D_2(S_n)$. This can be attributed to the more compact labeling structure of $Amal(V_n, a, m)$, which minimizes redundancy in key distribution. However, the difference is minimal, suggesting that both graphs are efficient in terms of storage requirements. In summary, both $D_2(S_n)$ and $Amal(V_n, a, m)$ graphs demonstrate strong resistance to brute force attacks, ensuring the security of the proposed cryptographic method. While $D_2(S_n)$ excels in encryption speed, $Amal(V_n, a, m)$ offers slightly better storage efficiency. These results highlight the flexibility of using different graph structures to balance efficiency and security based on specific application needs.

D. CONCLUSION AND SUGGESTIONS

Based on the results and discussion, several conclusions can be drawn. The rainbow vertex antimagic connection number for the Shadow graph $D_2(S_n)$ with $n \geq 3$ is 2, demonstrating unique edge-weight properties that enhance its suitability for cryptographic applications. For the $Amal(V_n, a, m)$ graph, the rainbow vertex antimagic connection number is $mn + 1$, reflecting its ability to generate highly complex and secure key configurations. This research also successfully demonstrates the application of rainbow vertex antimagic coloring in cryptographic secret sharing. In $D_2(S_n)$, $n \equiv 1 (\text{mod } 2)$ (e.g., $D_2(S_3)$) requires at least 12 participants, whereas $n \equiv 0 (\text{mod } 2)$ (e.g., $D_2(S_4)$) necessitates 16 participants to reconstruct edge label patterns. For the $Amal(V_3, a, 2)$ graph, at least 12 participants are needed to securely distribute the edge label patterns. These findings confirm the effectiveness of dividing cryptographic keys into secure segments, ensuring the keys can only be reconstructed with sufficient shares.

Additionally, the Shadow graph $D_2(S_n)$ offers faster encryption times, making it suitable for real-time applications, whereas the $Amal(V_n, a, m)$ graph provides lighter encryption sizes, which are advantageous for systems with storage or bandwidth constraints. Both graph-based methods exhibit strong resistance to brute force attacks, affirming their reliability in securing sensitive data. For future research, several directions are proposed. First, further exploration is needed to determine the precise values of $rvac$ for a broader range of graph operations and additional graph structures. Second, it is crucial to identify specific conditions under which rainbow vertex antimagic coloring can be achieved for specialized graph classes. Finally, the application of these graph-theoretical concepts should be extended to advanced cryptographic systems, such as blockchain technologies, secure communication protocols, and distributed data storage solutions. These recommendations aim to bridge the gap between theoretical advancements and practical implementations, paving the way for innovations in secure data management.

ACKNOWLEDGEMENT

We sincerely thank LP2M Universitas Jember and PUI-PT Combinatorics and Graphs (CGANT) at Universitas Jember for their invaluable support and collaboration in our 2025 research initiatives. Special gratitude is extended to the lecturers and members of the CGANT Research Group, whose dedication and expertise have significantly contributed to the success of our endeavors.

REFERENCES

Agustin, I. H., Dafik, D., Nisviasari, R., Baihaki, R. I., Kurniawati, E. Y., Husain, S. K. S., & Nagaraja, V. (2024). On Rainbow Vertex Antimagic Coloring and Its Application to the Encryption Keystream Construction. *Applied Mathematics and Information Sciences*, *18*(4), 783–794. https://doi.org/10.18576/amis/180411

Akadji, A. F., Katili, M. R., Nasib, S. K., & Yahya, N. I. (2021). *Desimal: jurnal matematika*. *4*(2), 123–132. https://doi.org/10.24042/djm

Alfarisi, R., Dafik, Prihandini, R. M., Adawiyah, R., Albirri, E. R., & Agustin, I. H. (2019). Graceful Chromatic Number of Unicyclic Graphs. *Journal of Physics: Conference Series*, *1306*(1), 012039. https://doi.org/10.1088/1742-6596/1306/1/012039

Cesati, M. (2023). A New Idea for RSA Backdoors. *Cryptography*, *7*(3). https://doi.org/10.3390/cryptography7030045

Dafik, Agustin, I. H., Hasan, M., Adawiyah, R., Alfarisi, R., & Wardani, D. A. R. (2018). On the Locating Edge Domination Number of Comb Product of Graphs. *Journal of Physics: Conference Series*, *1022*(1). https://doi.org/10.1088/1742-6596/1022/1/012003

Dafik, Agustin, I. H., Surahmat, Alfarisi, R., & Sy, S. (2017). On Non-Isolated Resolving Number Of Special Graphs And Their Operations. *Far East Journal of Mathematical Sciences (FJMS)*, *102*(10), 2473–2492. https://doi.org/10.17654/MS102102473

Dafik, Mursyidah, I. L., Agustin, I. H., Baihaki, R. I., Febrinanto, F. G., Husain, S. K. B. S., & 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), 984–996.

Fauziah, D. A., Dafik, Agustin, I. H., & Alfarisi, R. (2019). The rainbow vertex connection number of edge corona product graphs. *IOP Conference Series: Earth and Environmental Science*, *243*(1). https://doi.org/10.1088/1755-1315/243/1/012020

Gembong, A. W., Slamin, Dafik, & Agustin, I. H. (2017). Bound of Distance Domination Number of Graph and Edge Comb Product Graph. *Journal of Physics: Conference Series*, *855*(1). https://doi.org/10.1088/1742-6596/855/1/012014

Heggernes, P., Issac, D., Lauri, J., Lima, P. T., & Van Leeuwen, E. J. (2018). Rainbow vertex coloring bipartite graphs and chordal graphs. *Leibniz International Proceedings in Informatics, LIPIcs*, *117*(83), 1–13. https://doi.org/10.4230/LIPIcs.MFCS.2018.83

Kamila, A. A. U. U., Dafik, Kristiana, A. I., Nisviasari, R., & Kurniawati, E. Y. (2023). *On Rainbow Vertex Antimagic Coloring of Shell Related Graphs* (Vol. 2). Atlantis Press International BV. https://doi.org/10.2991/978-94-6463-138-8_3

Khan, M. A., Quasim, M. T., Alghamdi, N. S., & Khan, M. Y. (2020). A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data. *IEEE Access*, *8*, 52018–52027. https://doi.org/10.1109/ACCESS.2020.2980739

Krenn, S., & Lorünser, T. (2023). *Verifiable Secret Sharing*. 45–54. https://doi.org/10.1007/978-3-031-28161-7_7

Kristiana, A. I., Mursyidah, I. L., Dafik, D., Adawiyah, R., & Alfarisi, R. (2023). Local irregular vertex coloring of comb product by path graph and star graph. *Discrete Mathematics, Algorithms and Applications*, *15*(6). https://doi.org/10.1142/S1793830922501488

Li, X. L., & Shi, Y. (2013). On the rainbow vertex-connection. *Discussiones Mathematicae Graph Theory*, *33*(2), 307. https://doi.org/10.7151/dmgt.1664

Marsidi, Agustin, I. H., Dafik, Kurniawati, E. Y., & Nisviasari, R. (2022). The rainbow vertex antimagic coloring of tree graphs. *Journal of Physics: Conference Series*, *2157*(1), 012019. https://doi.org/10.1088/1742-6596/2157/1/012019

Marsidi, M., Agustin, I. H., Dafik, D., & Kurniawati, E. Y. (2021). On Rainbow Vertex Antimagic Coloring of Graphs: A New Notion. *CAUCHY: Jurnal Matematika Murni Dan Aplikasi*, *7*(1), 64–72. https://doi.org/10.18860/ca.v7i1.12796

Mohan, K. R., Rasappan, S., Murugesan, R., Kumaravel, S. K., & Elngar, A. A. (2022). *Secret Information Sharing Using Probability and Bilinear Transformation* (pp. 115–122). https://doi.org/10.1007/978-981-19-0182-9_12

Mursyidah, I. L., Ayu, A., Ulya, U., & Baihaki, I. (n.d.). *Rainbow Vertex Connection Number on Some Special Graphs*. 27–34.

Mursyidah, I. L., Dafik, Adawiyah, R., Kristiana, A. I., & Agustin, I. H. (2021). On local irregularity vertex coloring of comb product on star graphs. *Journal of Physics: Conference Series*, *1836*(1), 012023. https://doi.org/10.1088/1742-6596/1836/1/012023

Mursyidah, I. L., Dafik, Kristiana, A. I., Agustin, I. H., Maylisa, I. N., & Alfarisi, R. (2023). *On Rainbow Antimagic Coloring of Some Classes of Graphs* (pp. 73–93). https://doi.org/10.2991/978-94-6463-138-8_8

Nisviasari, R., Dafik, Agustin, I. H., Kurniawati, E. Y., Maylisa, I. N., & Septory, B. J. (2022). Improving the robustness of the affine cipher by using a rainbow antimagic coloring. *Journal of Physics: Conference Series*, *2157*(1), 012017. https://doi.org/10.1088/1742-6596/2157/1/012017

Panahi, P., Bayılmış, C., Çavuşoğlu, U., & Kaçar, S. (2021). Performance Evaluation of Lightweight Encryption Algorithms for IoT-Based Applications. *Arabian Journal for Science and Engineering*, *46*(4), 4015–4037. https://doi.org/10.1007/s13369-021-05358-4

Phalakarn, K., Suppakitpaisarn, V., Attrapadung, N., & Matsuura, K. (2020). *Constructive t-secure Homomorphic Secret Sharing for Low Degree Polynomials* (pp. 763–785). https://doi.org/10.1007/978-3-030-65277-7_34

Septory, B. J., Utoyo, M. I., Dafik, Sulistiyono, B., & Agustin, I. H. (2021). On rainbow antimagic coloring of special graphs. *Journal of Physics: Conference Series*, *1836*(1), 012016. https://doi.org/10.1088/1742-6596/1836/1/012016

Simamora, D. N. S., & Salman, A. N. M. (2015). The Rainbow (Vertex) Connection Number of Pencil Graphs. *Procedia Computer Science*, *74*, 138–142. https://doi.org/10.1016/j.procs.2015.12.089

Wulandari, R. Y., & Simanjuntak, R. (2023). Distance antimagic labelings of product graphs. *Electronic Journal of Graph Theory and Applications*, *11*(1), 111. https://doi.org/10.5614/ejgta.2023.11.1.9