Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 4** : 1–8.
ISSN-0037-8712
doi:10.5269/bspm.79975

Applications of Rainbow Antimagic Coloring of Flower Snark Graphs in Secure Cryptographic Protocol Design

Sangeetha B., Srinivasa Rao K., Sunil S., Manjunath N. K., Madhu N. R.

ABSTRACT: Graph theory and cryptography maintain a profound theoretical relationship, especially concerning structural complexity and computational difficulty. This paper investigates a new intersection by utilizing Rainbow Antimagic Edge Coloring on Flower Snark graphs, which are a type of non-Hamiltonian, non-3-edge-colorable cubic graphs for creating secure Cryptographic protocols. Rainbow Antimagic Coloring assigns distinct edge weights such that each vertex sums are unique, resulting in a one-way encoding system well-suited for encryption and hashing purposes. We illustrate how the challenge of computing valid Rainbow Antimagic Colorings for Flower Snark graphs can be leveraged to develop secure public key systems by encryption algorithm. The fundamental structural complexity of the Flower Snark graph allows for the establishment of Cryptographic primitives that are provably secure and resilient to both classical and quantum attacks.

Keywords: Rainbow antimagic coloring, flower snark graph, cryptography, encryption algorithm.

Contents

1 Introduction 1

2 Definitions 2

3 Results 3

4 Encryption Algorithm 4

5 Proposed Uses 6

6 Conclusion 6

1. Introduction

Cryptography has evolved from traditional ciphers to complex mathematical frameworks that form the backbone of contemporary information security [1]. Historically, number-theoretic methods like RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) has prevalent in this area [4]. Nevertheless, the rising need for unconventional cryptographic frameworks, especially in the age of quantum computing, has spurred the investigation into different mathematical fields such as graph theory [1]. Graphs, with their intricate structural characteristics and combinatorial challenges, offer an encouraging basis for encoding information in innovative manners. A key area of graph theory pertinent to cryptography is graph labeling, wherein numerical values are assigned to vertices or edges according to specified criteria [3]. Among the various types, antimagic labeling has garnered interest because it ensures that the weights of vertices or edges are distinct, thus generating unique and unpredictable setups [7]. This characteristic directly reflects the fundamentals of secure encryption, where distinctiveness and complexity are critical for safeguarding messages. Expansions of this idea have been utilized to create encryption methods utilizing star, bipartite, and corona graphs. Building on this, the concept of Rainbow Antimagic Coloring (RAC) merges antimagic labeling with rainbow path coloring, ensuring both distinct weights and diversity in paths. This integration adds two layers of cryptographic intricacy: every shortest path must possess a rainbow color while also upholding antimagic uniqueness [7] [8]. This combination significantly enhances the strength of the encoded framework against attempts at reconstruction by adversaries. In this context, Flower Snark graphs hold a unique significance. Snark graphs are recognized for their cubic nature, lack of bridges, and non-3-edge-colorable properties, making them some of the most structurally

2020 *Mathematics Subject Classification:* 05C15.
Submitted November 08, 2025. Published February 26, 2026

intricate classes of graphs [6]. The Flower Snark family notably adds levels of irregularity and complex connectivity patterns, which makes them highly suitable for cryptographic uses. Utilizing rainbow antimagic coloring on Flower Snark graphs not only heightens the irregularity of labeling schemes but also greatly expands the potential key space, thus contributing to more robust cryptographic primitives. As a result, the combination of rainbow antimagic coloring with Flower Snark graphs offers a groundbreaking approach for graph-based cryptography, presenting opportunities for progress in encryption design, secure key generation, and resistance to both structural and computational attacks, particularly in light of forthcoming post-quantum security demands.

2. Definitions

2.1 Rainbow Coloring: Is a type of coloring of graph where the path between the two distinct vertices so that no two edges in that path has same colors, denoted by $rc(G)$.

2.2 Rainbow Antimagic Coloring: It is the rainbow coloring of graph such that $\exists$: a bijection $g : E(G) \to 1, 2, 3, \cdots, |E|$ so that the vertex sums for distinct vertices are different, i.e the edge weight $w(e) = g(u) + g(v)$ obtain a color for its edges, ensuring a rainbow path between distinct pair of vertices with distinct value, denoted by $rac(G)$.

2.3 Flower Snark Graph: Flower Snarks are a connected, bridgeless cubic graphs. The Flower Snarks are non-Hamiltonian and non-planar. The Flower Snark J_n can be constructed with the following process:

- Build n copies of the star $K_{1,3}$. Denote the central vertex of each star by q_i and the outer vertices p_i, r_i *and* s_i. This results in a disconnected graph on $4n$ vertices with $3n$ edges (q_ip_i, q_ir_i *and* q_is_i $for\ 1 \leq i \leq n$).
- Construct the $n - cycle$ $(p_1, p_2 \cdots, p_n, p_1)$. This adds n edges.
- Finally construct the $2n - cycle$ $(r_1, r_2, \cdots, r_n, s_1, s_2, \cdots, s_n, r_1)$. Thus adds $2n$ edges.

2.4 Cryptography: Cryptography is the science of securing information through the use of mathematical techniques and algorithms that convert readable data into an encoded format, assuring that only authorized parties can access and understand the information. It encompasses methods for confidentiality, integrity, authentication, and non-rejection of data in communication and storage.

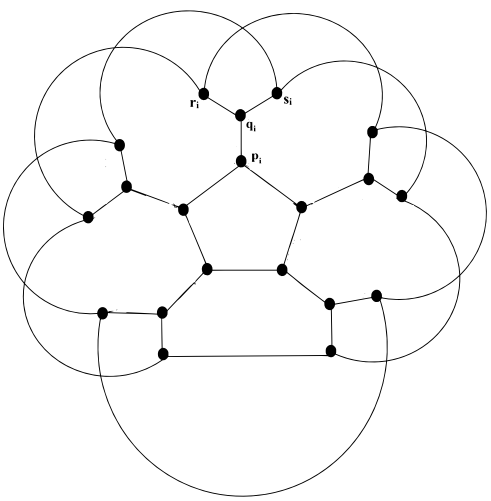

Figure 1: Flower Snark J_5

3. Results

Here we discuss the results of Rainbow Antimagic Coloring of Flower Snark graph.

Theorem 3.1 *: let $G = J_n$. Then for odd $n \geq 5$, $rc(G) = \lceil \frac{n}{2} \rceil + 3$. [6]*

Theorem 3.2 *: Let G be a connected graph. Let $rc(G)$ be the rainbow connection number of G and the maximum degree of G is $\Delta(G)$. Then, $rac(G) \geq max\{\mathrm{rc(G)}, \Delta(G)\}$. [9]*

Theorem 3.3 *: Let $G = J_n$ be the flower snark graph for $n \geq 5$ (odd). The Rainbow Antimagic connection number of G is $3n$.*

Proof: *: Let V be the vertex set and E be the edge set of G. The vertex set of G is $V(G) = \{p_1, p_2, \cdots, p_n\} \cup \{q_1, q_2, \cdots, q_n\} \cup \{r_1, r_2, \cdots, r_n\} \cup \{s_1, s_2, \cdots, s_n\}$ where q_i is the central vertex forming star graph and p_i, r_i and s_i denotes the other vertices. The cardinality of vertex set is $|V(G)| = 4n$ and edges $|E(G)| = 6n$. The flower snark graph has a maximum degree $\Delta(J_n) = 3$ and the rainbow connection number $rc(J_n) = \lceil \frac{n}{2} \rceil + 3$. Define vertex function $f : V(G) = \{1, 2, 3, \cdots, 4n\}$ defined by*

$$f(v) = \begin{cases} f(p_i) = i & for\ 1 \leq i \leq n, \\ f(q_i) = n + i & for\ 1 \leq i \leq n, \\ f(r_i) = 4n + 1 - i & for\, i\ even,\ 1 \leq i \leq 2n, \\ f(s_i) = 4n + 1 - i & for\, i\ odd,\ 1 \leq i \leq 2n - 1. \end{cases}$$

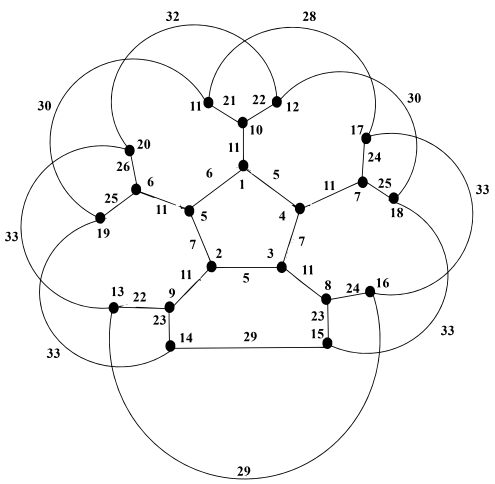

Figure 2: RAC of J_5

The edge weight of G as follows. Define $w : E(G) \to \{1, 2, 3, \cdots, 6n\}$ such that

$$w(e) = \begin{cases} w(p_i p_{i+1}) = n - 1 + i & for\ 1 \leq i \leq n-2, \\ w(p_i q_i) = 2n + 1 & for\ 1 \leq i \leq n, \\ w(q_i r_i) = 4n + i & for\ 1 \leq i \leq n, \\ w(q_i s_i) = 4n + i & for\ 2 \leq i \leq n, \\ w(r_i r_{i+3}) = 5n + 2 + i & for\ 1 \leq i \leq n, \\ w(s_i s_{i+3}) = 5n + 4 + i & for\ 1 \leq i \leq n, \\ w(r_i s_{i+2}) = 5n + 4i & for\ 1 \leq i \leq n, \\ w(s_i r_{i+2}) = 5n + 4i & for\ 2 \leq i \leq n. \end{cases}$$

From the weight function, the Flower Snark graph has $3n$ *colors. Thus the Rainbow Antimagic connection number is*

$$\text{rac}(G) \leq 3n. \tag{1}$$

Since G *has maximum degree of* $\Delta(G) = 3$ *and rainbow connection number of* G *is* $\lceil \frac{n}{3} \rceil + 3$ *. Using theorem* 2*, it may not be sufficient to get rainbow path according to antimagic property. In Flower Snark graph the degree of each vertex is* 3 *and it contains* n *star-like structures centered at the central vertices, where each structure consists of* 3 *edges that must be colored differently to maintain rainbow connection. Since there are* n *star-like structures which require* 3 *different colors, this requirement propagates the use of atleast* $3n$ *colors. Hence we have*

$$\text{rac}(G) \geq 3n. \tag{2}$$

By (1) and (2), we prove that $rac(G) = 3n$ *.* □

4. Encryption Algorithm

4.1 Graph Preparation

Step (i): Create the flower snark graph ($J_5 or J_7$), making sure every edge is assigned a distinct weight and that each path can be colored in a 'rainbow' style (no two edges on a path should have the same color or label).

Step (ii): Systematically document the correspondence between edges and their respective colors or weights.

4.2 Key Generation

Step (iii): Select a private key that includes: The coloring/labeling scheme (the mapping of edge numbers to labels/colors). A group of uniquely colored antimagic paths or cycles designated as valid "routes" for encoding messages.

4.3 Message Encoding

Step (iv): Transform the plaintext message M into a series of numerical blocks using ASCII or another standardized scheme.

Step (v): For each block:

- **Assign a path:** Relate the numerical value to a distinct path between node pairs or a uniquely identified cycle based on the edge labels/weights from the Flower Snark graph presented.
- **Path selection:** For a specified plaintext block, locate a path in the graph whose total of edge labels (weights) corresponds to or uniquely encodes the block. The total is antimagic, ensuring each block has a different path sum.
- **Edge sequence:** Document the precise order of edge labels (and their associated coloring if color is used for an additional layer of security).

4.4 Ciphertext Generation

Step (vi): The ciphertext for each block is represented as a tuple: The array of edge labels (or colors) utilized in the encoding path.
If desired, the starting and ending vertices may be included for extra ambiguity.

Step (vii): The complete ciphertext is created by concatenating these tuples for all blocks within the message.

4.5 Transmission

Step (viii): Send the series of encrypted tuples (ciphertext), along with the identifier specifying which Flower Snark graph configuration is employed ($e.g., J_n$), to the intended recipient.

Example: (Applying Steps to Diagram)
Assuming the plaintext is **"CAT"**. **"C"** (ASCII 67), **"A"** (ASCII 65), **"T"** (ASCII 84).

- For **"67"**, identify a path or subgraph where the edge labels (from the diagram, such as 33, 23, 11, etc.) total 67, adhering to Antimagic uniqueness.
- Let's choose edges labeled 33, 23, and 11 in a path (since $33 + 23 + 11 = 67$) as the encoding for **"C"**.
- Record and transmit the path as.
- Repeat for **"A"** (65) and **"T"** (84) using different disjoint antimagic paths.

Table 1: Summary Table

Plain Textbox	*Path(Edge Lables)*	*Ciphertext Output*
"C" (67)	33-23-11	$[33 + 23 + 11]$
"A" (65)	32-22-11	$[32 + 22 + 11]$
"T" (84)	24-28-21-11	$[24 + 28 + 21 + 11]$

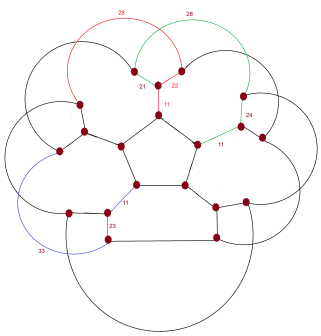

Figure 3: RAC path

Decryption Method (for Completeness)
The receiver, aware of the labeling/coloring scheme and the Snark graph, reconstructs each block of plaintext by:

- Locating the communicated path within the graph.
- Computing the total of its edge labels (or applying color mappings if color encoding is utilized).
- Obtaining the referenced plaintext block (e.g., ASCII value).

5. Proposed Uses

The Flower Snark graph shows promising potential in cryptography when combined with Rainbow Antimagic Coloring due to its distinct structural and coloring characteristics that can bolster security and resilience in Cryptographic methods.

Structural Benefits of Flower Snark Graphs:
Flower Snark graphs are intricate, cubic structures that lack a Hamiltonian cycle, noted for their complexity and extensive automorphism group, making it ideal for Cryptographic modeling where unpredictability and protection against typical attacks are crucial. The intricate interconnections and non-planarity heighten the challenge for adversaries trying to analyze or navigate the network, which is utilized to create secure communication methods.

Function of Rainbow Antimagic Coloring:
In Rainbow Antimagic Coloring, edges or vertices receive colors or labels in a way that makes specific paths (e.g., communication routes) within the graph both rainbow (with all distinct colors) and antimagic (where vertex or edge sums are unique), ensuring every route is identifiable and lacks repetitions. These coloring strategies provides a way to encode distinctive cryptographic keys or session tokens, assuring that if multiple nodes or edges are compromised, the security is maintained due to the constraints of the coloring.

Design of Cryptographic Protocols:
Key Distribution and Secret Sharing: The distinct colorings can facilitate the division of cryptographic keys into segments, distributed across different paths in the graph. Only certain validated combinations (Rainbow Antimagic paths) can reconstruct the key, improving secret sharing and threshold schemes.

Intrusion Resistance: With each connection (edge or path) uniquely colored, it becomes remarkably more complex for attackers to predict or brute-force valid communication paths, thereby enhancing the system's defense against eavesdropping and replay assaults.

Firewall Simulation and Channel Security: Rainbow Antimagic coloring can function as multiple, separate firewalls between nodes. Communication is permitted solely through appropriately colored (rainbow) paths, acting as a Cryptographic shield against intruders.

Graph-based Encryption: The distinctive color sums or labels can function as cryptographic keys or inputs for encryption algorithms (such as affine ciphers or key schedule generation), rendering the encryption process robust and adaptable.

6. Conclusion

Graphs with elevated Rainbow Antimagic connection numbers, like the Flower Snark, offer an extensive parameter space for key generation, diminishing the likelihood of collisions and making brute-force attacks computationally unfeasible. Practical research indicates quicker encryption and reduced ciphertext sizes using Rainbow Antimagic Coloring compared to alternative methods, further endorsing its applicability in cryptographic system development. In this context, we have proposed an encryption algorithm for the RAC of Flower Snark graph with Antimagic coloring $rac(G) = 3n$. Thus, Flower

Snark graphs adorned with Rainbow Antimagic Colorings enhance Cryptographic protocol design by providing strong key diversification, secure key-sharing solutions, and robust defenses against a variety of attacks—utilizing their complexity and coloring constraints for effective security implementations.

Acknowledgments

The authors would like to thank the administration and the Research and Development centre, Sri Venkateshwara College Of Engineering, Vidyanagar, Bengaluru and BGS Science Academy and Research Centre, Agalagurki, Chikkaballapur, Dept of Mathematics.

References

1. M. Tarawneh,*Cryptography: Recent Advances and Research Perspectives,*. IntechOpen.(2023).

2. M. Lalitha and S. Vasu., *A study on graph theory in cryptography using Python*. Journal of Emerging Technologies and Innovative Research, vol. 10, no. 4, (2023).

3. R. Nandhini, V. Maheswari, and V. Balaji,*A graph theory approach on cryptography*. Journal of Computational Mathematics, vol. 2, no. 1,(2018), pp. 97–104.

4. Nasir. Ali, Ayesha Sadiqa, Muhammad Amir Shahzad, Muhammad Imran Qureshi, Hafiz Muhammad Afzal Siddiqui, Suhad Ali Osman Abdallah, and Nashaat S. Abd El-Gawaad, *Secure communication in the digital age: A new paradigm with graph-based encryption algorithms*. Frontiers in Computer Science, vol. 6, 1454094, (2024).

5. R. Jegan, P. Vijayakumar, V. D. Ambethkumar, and P. Vijay, *Encryption and decryption of a word into weighted graph using super-edge anti-magic total labeling of Bi-star graph*. Journal of Discrete Mathematical Science and Cryptography, vol. 26, no. 5, (2023), pp. 1355–1365.

6. K. Srinivasa Rao, U. Vijaya Chandra Kumar, A. Mekala, *Rainbow Connection Number Of Flower Snark Graph*. International Journal of Applied Mathematics, vol. 33, no. 4,(2020).

7. G. Chartrand, G. L. Johns, K. A. McKeon, P. Zhang, *Rainbow Connection in graphs*. Mathematica Bohemia, **133**, no. 1 (2008), 85-98.

8. B. Sulistiyono, Slamin, Dafik, I H Agustin, R Alfasari, *On Rainbow antimagic coloring of some graphs*. Journal of Physics: Conference Series 1465(2020) 012029.

9. H. S. Budi, Dafik, I M Tirta, I H Agustin and A I Kristina, *On Rainbow antimagic coloring of graphs*. Journal of physics: conference series 1832(2021)012016.

10. Wahaya Lestari, Dafik, Susanto and Abd. Aziz Wahab, *On the strong rainbow antimagic coloring of some special graphs*. ICCGANT (2022),(2023), Apr 6 pp. 61-72.

11. K. Srinivasa Rao, R. Murali, *Rainbow critical graphs*. Int. Journal of computer application, 4, no. 4 (2014), 252-259.

12. K. Srinivasa Rao, R. Murali, S. K. Rajendra, *Rainbow and strong rainbow criticalness of some standard graphs*. Int. Journal of Mathematics and computer Research, **3**, no. 1, (2015), 829-836.

13. H. Anwar and Zill-e-Shams, *Algorithm of encryption using graph theory*. Math. Sci. Appl., vol. 2, no. 2, (2023), pp. 73–78.

14. Medini H. R., Sabitha D'Souza, Devadas Nayak C, Pradeep G. Bhat. *Encoding and decoding of messages using graph labeling methods*. Muk Publications.

15. Prathipa Murugan, Sivakumar Nagarajan, *Geometric Mean Labeling in Cryptography: A Graph-Based Approach to Enhanced Security and Performance*. Computational Mathematics, (2025).

16. D. K. Gurjar. *Labeled Paths in Cryptography*. Nova Publishers, (2021).

17. DAA Sherin et al,*Encryption of Dual Numbers Using Edge Injective Labeling*. (2021).

18. Uma Dixit, *Cryptography A Graph Theory Approach*. International Journal of Advance Research in Science and Engineering, **6** (01),(2017), BVCNSCS 2017.

Sangeetha B.,
Department of Mathematics, BGS Science Academy and Research Centre, Chikkaballapur, Research Scholar, VTU Belagavi,
India.
E-mail address: sangeetha41.ss@gmail.com

and

Srinivasa Rao K.,
Department of Mathematics, Sri Venkateshwara College of Engineering, Vidyanagar, Bengaluru – 562157,
India.
E-mail address: srinivas.dbpur@gmail.com

and

Sunil S.,
Department of Mathematics, Sri Venkateshwara College of Engineering, Vidyanagar, Bengaluru – 562157,
India.
E-mail address: sunilmurthy86@gmail.com

and

Manjunath N. K.,
Department of Mechanical Engineering, Sri Venkateshwara College of Engineering, Vidyanagar, Bengaluru – 562157,
India.
E-mail address: manjunatha.nk16@gmail.com,

and

Madhu N. R.,
Department of Mathematics, RLJIT, Doddaballapur, Research Scholar, VTU Belagavi-590018,
India.
E-mail address: madhunr1990@gmail.com