



# Difference divisor labeling for graph-based cryptographic applications: a novel approach to secure encoding

P. Janaki<sup>1</sup> · V. Maheswari<sup>1</sup> · V. Balaji<sup>2</sup>

Received: 4 October 2025 / Accepted: 9 December 2025  
© Bharati Vidyapeeth's Institute of Computer Applications and Management 2026

## Abstract

This study introduces a novel labeling scheme to graph theory known as Difference Divisor Labeling that is aimed at facilitating cryptographic applications through an edge labeling based in mathematics. This method labels the vertices based on the divisors of a positive integer, and then obtains the edge labels based on the parity and/or difference of the adjacent vertices. There are a number of distinct and significant advantages of this labeling paradigm over traditional graph labeling algorithms, which tend to have constraints on applicability, scalability, and flexibility for dealing with complicated or irregular graphs. Difference Divisor Labeling is applied and demonstrated on a variety of classes of graphs, specifically cycle graphs, regular graphs, and complete bipartite graphs, to show that they all meet the specifications of the proposed labeling. The labeled edge values are used as plaintext to encrypt with affine and RSA ciphers, highlighting to the reader the goal of building some secure graph-based cryptographic system. The paper describes full encryption and decryption methods for both types of graphs, and demonstrates how the labeling can ensure unpredictable and secure ciphertext generation. By exceeding the limitations of traditional labelings and being easily integrated with newer cryptographic algorithms, Difference Divisor Labeling represents a versatile and secure communication platform in the digital networks. This will open innovative paths of graph-theoretic encryption as it converges discrete mathematical abstractions and concepts of information security.

**Keywords** Graph labeling · Difference divisor labeling · Cycle graph · Complete bipartite graph · Regular graph · Encryption · Decryption

## 1 Introduction

Graphs are structures used in mathematics to represent pairwise relationships between entities, is the focus of graph theory, an applied area of discrete mathematics [1, 2]. A graph is formed by vertices (or nodes) linked by edges

[3], and it offers a flexible model for describing networks like communication systems, transportation networks, social relations, and biological systems [4]. Graph theory has developed, over the years, into a very important tool in theoretical and applied research [5], since it reduces the complex into understandable models. Graph theory has its origins in 1736, with the famous Königsberg Bridge Problem was solved by the Swiss mathematician Leonhard Euler [6, 7]. The work of Euler served as the basis of what would eventually develop into the theory of networks and connectivity [8]. His Method introduced the idea of representing the landmasses as vertices and bridges as edges, and this resulted in the idea of an Eulerian path-one that would trace each of the graph's edges once [9].

Of the many subfields of graph theory, one important branch is graph labeling, which concerns the assignment of labels, usually numbers, to the vertices, edges, or both, according to specific rules or conditions [10]. Graph labeling has gained much attention not just because it enriches

---

✉ V. Maheswari  
maheswari.sbs@vistas.ac.in

P. Janaki  
janakisrihari8511@gmail.com

V. Balaji  
pulibala70@gmail.com

<sup>1</sup> Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Pallavaram, Chennai, Tamil Nadu, India

<sup>2</sup> Department of Mathematics, Sacred Heart College (Autonomous), Thirupattur, Vellore, Tamil Nadu, India

the knowledge about the structure of graphs [11], but also because of its applications in the fields of coding theory, image verification, circuit configuration, x-ray crystallography, and network topology. Various labelings like graceful, harmonious, edge-magic, and modular labelings have been studied comprehensively [12]. These label schemes are mostly used to determine distinct characteristics, reduce computation, or facilitate secure communication [13]. Nevertheless, most of these traditional labeling methods are subject to some drawbacks. They may not be adaptable to all types of graphs, involve heavy computation, or fail to adapt in dynamic networks. For example, elegant labeling is not universal for all trees, and a few labelings are not effective at scaling for large or higher-level networks [14]. Further, due to predictability and non-uniform integration within modern encryption methodologies, their utility within cryptographic mechanisms has been compromised [15].

To overcome such limitations, the Difference Divisor Labeling idea is proposed. This new labeling scheme labels nodes based on the difference and divisibility properties of node labels to yield edge values that are determined by the parity of the difference between adjacent vertices. It promotes cryptographic application with the generation of non-recurring, challenging-to-identify label patterns that can be employed as plaintext within cryptographic systems such as affine or RSA ciphers. It offers greater security, flexibility, and versatility, especially in networks of computers communicating with each other under the requirements that encoding a message in data should be resilient and robust. Difference Divisor Labeling provides an interesting alternative to common processes since it does not have structural restrictions in its utilization, has more applications on many graph structures, and is able to facilitate more secure and usable graph-based encryption practices.

#### Contribution

- In this research, Difference Divisor Labeling is introduced using the difference and divisibility of vertex labels.
- This study provides a step-by-step encryption and decryption procedure using labeled edge values as plaintext, thereby illustrating the robustness and security of the method.
- This paper highlights the flexibility, scalability, and suitability of this labeling technique for secure data encoding in communication networks.

## 2 Literature review

In 2021, Sugeng et al. [16] created a modular irregular labeling of two biregular graph classes, in this case the friendship graph class and the regular double-star graph class. Additionally, the labeling was erratic and equally strong as the modular example, because the friendship graph's modular irregularity strength also contained the minimal irregularity strength.

In 2022, Badr et al. [17] examined the path and cycle radio mean square numbers,  $rmsn(P_n)$  and  $rmsn(C_n)$ , respectively. They provided a rough approach to calculate graph  $G$ 's  $rmsn(G)$ . Lastly, a novel mathematical approach was presented to determine the upper bound of  $rmsn(G)$  for graph  $G$ . The suggested mathematical model and the suggested approximate algorithm were compared. Additionally, they demonstrated how the suggested approximate technique defeated the ILPM (integer linear programming model) based on the radio mean square number, as demonstrated by the computational results and their analysis. However, based on running time, the suggested ILPM fared better than the suggested approximate method.

In 2021, Aasi et al. [18] considered the use of multi-distance radio labeling for wireless communication channel assignment issues.  $\wp$ 's maximum value assigned to a graph vertex is called the span of labeling  $\wp$ . The minimal span acquired over all radio labelings of  $G$  was its radio number, represented by  $rn(G)$ . For some graph families, they also discovered relationships between a lexicographic product's radio number and radio mean number.

In 2024, Tharani and Saradha [19] suggested giving certain standard and unique graphs distinct labels. Additionally, the scenarios for which specific graphs relating to paths, stars, and cycles allow for discrete labeling were supplied. The EX-OR procedure used in this labeling simplified the situation of having two swords in a single sheath. In addition to minimizing the difference between the different edge labels and vertex labels, the cardinality of each vertex's neighboring labels was also considered.

In 2024, Almohanna and Alhulwah [20] presented NK-labeling, a new labeling scheme. The NK-chromatic index, represented by  $\chi' NK(G)$ , is graph  $G$ 's NK-labeling for the lowest positive integer. They looked at the NK-labeling of a number of popular graph classes. It was demonstrated that for odd  $n$ , the complete graph  $K_n$ 's NK-chromatic was  $n$ , and for  $n \geq 4$ , the NK-chromatic of the route  $P_n$  was three. Additional findings pertaining to the NK-labeling are also provided.

In 2022, Bonucci et al. [21] presented the idea of labeling a graph with weak harmonics. They offered multiple constructs that extended a given weak harmonic labeling over bigger graphs, as well as a variety of example families.

They created novel instances of strong harmonic labelings using finite weak models. Using harmonic subsets of  $Z$  to characterize graphs with weak labels was reported as a key result of this method, which showed quantitative proof of its effectiveness in computing all weakly labeled finite graphs in contrast to an exhaustive search calculation.

In 2022, Meena et al. [22] demonstrated the primacy of certain graph classes, such as  $\mathcal{H}$ -super subdivision of graphs associated with the cycle  $HSS(C_m)@K_2$ ,  $HSS(C_m)@2K_2$ ,  $HSS(C_m)@(K_3 \cup K_2)$ ,  $HSS(C_m)@(K_3 \cup 2K_2)$ ,  $HSS(C_m) \odot K_1$ . If  $m$  points on a graph  $G$  may be labeled with different positive numbers up to  $m$  so that the  $gcd$  of the labels of each pair of adjacent points is 1, then the graph is said to permit prime labeling. A prime graph is a graph  $G$  that admits prime labeling.

In 2025, Tomita and Maracini [23] presented the Pseudo-labeling Domain Adaptation (PDA) technique, which produced a strong cross-domain representation by utilizing pseudo-labels produced by several models. They also suggested a unique approach known as UMAP Domain Adaptation (UMAP DA), a UMAP-based technology that permits connections only between nodes from different domains, in order to further alleviate the domain-shift issue. The suggested approach improved interpretability and performance, providing a fresh approach to cross-domain learning with pseudo-labels.

In 2023, Gopi and Prakash [24] presented and examined the labeling graph for the  $k$ -super heronian mean. Any positive integer which is greater than 1 or more was represented by the symbol  $k$  in this case. A graph was referred to as a  $k$ -super heronian mean graph if it admits  $k$ -super heronian mean labeling.

In 2021, Nagaraja et al. [25] suggested the graphs likely the graphs' likely paths, umbrella  $U(m, n)$ , cycles, square graphs,  $K_1 + C_n$  for odd and even  $n$ ,  $C_n JK1$  and  $C_n JK2$ , comb, duplicating each vertex by an edge in path  $P_n$  were labeled with the power exponential mean labeling of graphs.

In 2025, Gupta et al. [26] focused on developing encryption and decryption algorithms utilizing graph theory techniques, specifically employing the Sun-let graph and Pan graph for data encryption and decryption.

In 2024, Shastri and Pragathi [27] presented a novel graph-based cryptosystem designed to ensure data integrity in user-to-user communication through crypto bipartite graph theory (CBGT). It mitigates the vulnerabilities of random key selection by using improved Teacher Learning-based Optimization for securely selecting edges between the sets of vertices, which improves the security of encryption without compromising efficiency in decryption.

In 2025, Djordjevic [28] discussed very important basics of conventional cryptography, which included basic

terminology, cryptographic schemes like symmetric and asymmetric cryptography, substitution and transposition ciphers, one-time pads, secrecy, authentication, and non-repudiation. Finally, it discusses various cryptanalytic attacks like ciphertext-only and chosen-plaintext attacks, an information-theoretic approach showing perfect security, unicity distance, and the principle of compression.

In 2025, Orduz [29] presented important cybersecurity concepts and keys in relation to their quantum counterparts, along with classical and quantum cryptography protocols. The authors want to potentially utilize concepts relating to quantum computing, machine learning, and/or deep learning to shape where future scientists may be heading, especially in the area of post-quantum cryptography. This project and the work with Orduz [29] will be ongoing to develop topics around these ideas and contribute to the development of future ciphers.

In 2024, Joshi [30] proposed a new secure data transmission technique to protect image data, inspired by graph theory, treating image pixels as graphs with edges that have weights assigned to them. The process uses minimum spanning trees (MSTs) and weighted adjacency matrices to encrypt and decrypt color digital images. Results from experiments and a security analysis show that the method is suitable and robust against statistical attacks, as revealed by analysis through statistical tests such as histograms, correlations, and entropy. This method is also robust to brute-force and occlusion attacks.

In 2023, Hartmann [31] examined important algorithms in computer science - namely, computer science as applied to graph theory, which presented concepts such as node and edges and their degrees, graphs, paths, cycles, isomorphisms, networks, and directed graphs. This paper covers trees, rooted trees, search trees for Huffman codings, specific algorithms, and search algorithms such as breadth-first search, depth-first search, and topological sorting in directed acyclic graphs.

### 3 Problem statement

Despite the extensive development of different types of graph labeling methods from modular irregular and radio to discrete, NK, harmonic, prime, and mean labelings, labeling approaches have some serious limitations, including computational complexity, limited applicability, scalability challenges, and limited flexibility in terms of cryptography. In fact, most of the labeling schemes we find in the literature have to be implemented with considerable efficiency or not at all in dynamic and large networks, and some of them simply do not have compatible secure data encoding processes. These limitations highlight a strong need for a

flexible, efficient, and encryption-friendly labeling scheme that can be used across a broader range of graph structures. The Proposed Difference Divisor Labeling is a scalable and flexible labeling system that can be used across various graph classes, thus breaking the limitations present now. Apart from being used in dynamic networks, it reduces computational complexity. It enhances security in applications of graph-based cryptography by fitting seamlessly into encryption algorithms such as Affine and RSA, compared to previous methods.

## 4 Algorithmic representation of the proposed methodology

The methodological framework for the Difference Divisor Labeling scheme is outlined in this section. The algorithmic form clarifies the process of a complete construction of edge and vertex labels, as well as the encoding stage of these labels into cryptographic encoding.

### 4.1 Keywords

We follow standard graph-theoretic notation [1, 2]. For a graph,  $G = (V, E)$ , let  $p = |V|$  and  $q = |E|$ . Since the labels of edges and vertices are collected from the divisor set, we can also define  $D(n)$  according to the parameters  $n = p + q$ . Basic terms such as adjacency, degree, cycle, and complete graph  $K_n$ , and a complete bipartite graph  $K_{n,m}$  follow the conventional definition. Only the new definition of labeling will be stated explicitly.

### 4.2 Definition of difference divisor labeling

Consider a graph  $G$  with  $V$  vertices and  $E$  edges. If there exist a function  $F : V(G) \rightarrow \{1, 2, \dots, n = p + q\}$  where  $p$  and  $q$  denotes the number of vertices and edges, respectively such that the vertices of the graph are labelled by the divisors of  $n$  and for each induced graph

$$F'(uv) = \begin{cases} \frac{|u-v|}{2} & \text{if } |u-v| \text{ is even} \\ \frac{|u-v|+1}{2} & \text{if } |u-v| \text{ is odd} \end{cases}, \text{ then this graph is called the difference divisor labeling.}$$

### 4.3 Algorithmic representation

The proposed Difference Divisor Labeling scheme is formally expressed below as a series of steps. The algorithmic representation clarifies the method of constructing both vertex and edge labels, which are then employed in cryptographic encoding.

**Algorithm** Difference divisor labeling & cryptographic encoding.

**Input:** Graph  $G = (V, E)$  with  $p$  vertices and  $q$  edges.

**Output:** A sequence of ciphertext generated from encrypting the edge labels.

#### Step 1: Initialization

Calculate  $n = p + q$ . Compute the divisor set  $D(n)$ .

#### Step 2: Vertex Labeling

Assign each vertex  $v_i \in V$  with a unique label from  $D(n)$ .

#### Step 3: Edge Labeling

For each edge  $(u, v) \in E$ , compute the induced label

$$F'(uv) = f(x) = \begin{cases} (u-v)/2, & \text{if } u-v \text{ is even} \\ (u-v+1)/2, & \text{if } u-v \text{ is odd} \end{cases}$$

#### Step 4: Plaintext Generation

Treat each label noted on each edge as a symbol in the plaintext and replace the numerical values with their alphabetic equivalents (for example,  $A = 0, B = 1$ , and  $C = 2$ , and so on to  $Z = 25$ ).

#### Step 5: Encryption

Encrypt the plaintext using one of the following ciphers:

- **Affine cipher:**  $C = aP + b \pmod n$  where  $a$  is coprime to  $n$ .
- **RSA cipher:** The edge labels are treated as plaintext blocks.

#### Step 6: Decryption

For the decryption phase, compute the modular inverse  $a^{-1}$  of  $a \pmod n$  and recover plaintext as follows:

$$P = a^{-1}(C - b) \pmod n$$

#### Step 7: Output

Output the ciphertext sequence and verify recovery of the original plaintext.

## 5 Experimental results

In this section, we present the results of the proposed Difference Divisor Labeling scheme applied to multiple graph classes. Examples, encryption and decryption procedures, and numerical examples are included to demonstrate the applicability of this approach. The results demonstrate that regular graphs, cycle graphs, complete bipartite graphs, and path-related graphs enable Difference Divisor Labeling and can be easily adapted for use in cryptography.

**Theorem 5.1** Prove that  $k$ -regular graph is a difference divisor labeling when  $n = 18$ .

**Proof** To prove this theorem, consider a 4-regular graph with  $p = 6$  vertices and  $q = 12$  edges. Assigning the vertex label for the 4-regular graph as  $V(G) = \{1, 2, \dots, n = p + q (18 = 6 + 12)\}$  and  $F(u)$  is the divisors of  $n$ . Therefore,  $v_1 = 1, v_2 = 2, v_3 = 3, v_4 = 6, v_5 = 9, v_6 = 18$ . According to the definition of difference divisor labeling, the induced edges are labelled as

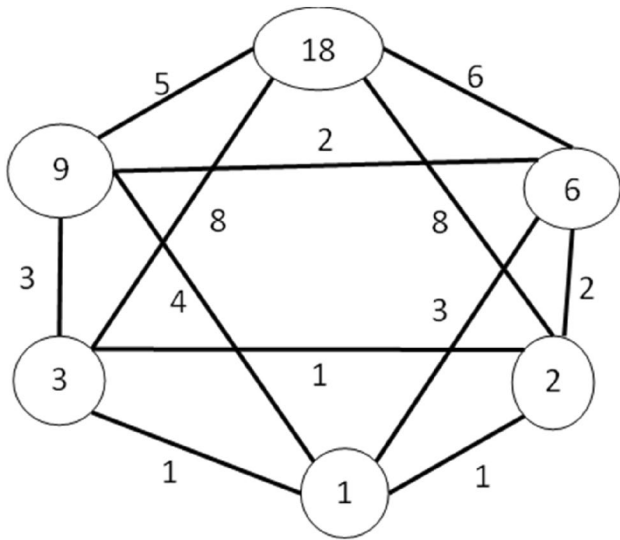


Fig. 1 4-Regular graph

$F'(E_1) = 5, F'(E_2) = 6, F'(E_3) = 3, F'(E_4) = 1, F'(E_5) = 1, F'(E_6) = 2, F'(E_7) = 8, F'(E_8) = 8, F'(E_9) = 2, F'(E_{10}) = 4, F'(E_{11}) = 1, F'(E_{12}) = 3$ . Hence, 4-regular graph is a difference divisor labeling. Therefore,  $k$ -regular graph is a difference divisor labeling when  $n = 18$ . The resultant graph with vertex and edge label for  $n = 18$  is given in Fig. 1.

Procedure for encryption and decryption

- For each graph G, edge label is considered as the plain text.
- Convert the numerical values into alphabet value for example A=0, B=1, ..., Z=25.

Plain text

5	6	3	1	1	2	8	8	2	4	1	3
F	G	D	B	B	C	I	I	C	E	B	D

- Cipher text (Encryption):  $C = (aP + b) \text{ mod } n$

Let  $a$  be relatively prime to  $n$ ,  $P$  denotes the plain text and  $b$  represents the multiple of  $n$ . For the above 4-regular graph,  $a = 5, b = 3$  and  $n = 18$ . Applying these values in encryption formula, cipher text is obtained.

$$C(5) = (5 \cdot 5 + 3) \text{ mod } 18 = 28 \text{ mod } 18 = 10$$

$$C(6) = (5 \cdot 6 + 3) \text{ mod } 18 = 33 \text{ mod } 18 = 15$$

$$C(3) = (5 \cdot 3 + 3) \text{ mod } 18 = 18 \text{ mod } 18 = 0$$

$$C(1) = (5 \cdot 1 + 3) \text{ mod } 18 = 8 \text{ mod } 18 = 8$$

$$C(2) = (5 \cdot 2 + 3) \text{ mod } 18 = 13 \text{ mod } 18 = 13$$

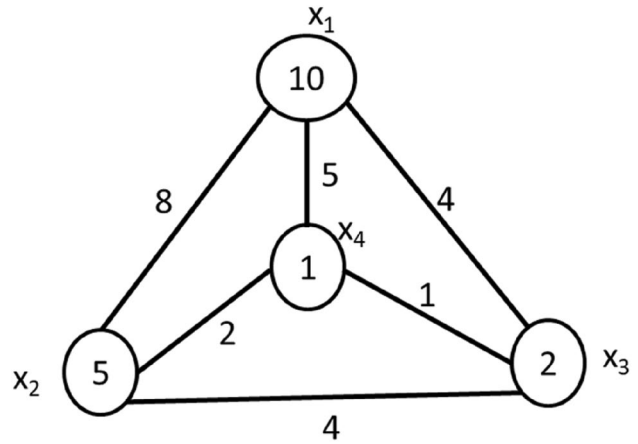


Fig. 2 3-Regular graph

$$C(8) = (5 \cdot 8 + 3) \text{ mod } 18 = 43 \text{ mod } 18 = 7$$

$$C(4) = (5 \cdot 4 + 3) \text{ mod } 18 = 23 \text{ mod } 18 = 5$$

Cipher text

10	15	0	8	8	13	7	7	13	5	8	0
K	P	A	I	I	N	H	H	N	F	I	A

- Decipher text (Decryption):  $P = a^{-1}(C - b) \text{ mod } n$

The inverse of encryption is called decryption. The modular inverse of  $a = 5 \text{ mod } 18 \rightarrow 5x \equiv 1 \text{ mod } 18 \rightarrow x = 11$ . i.e.,  $a^{-1} = 11$ .

Decipher text

5	6	3	1	1	2	8	8	2	4	1	3
F	G	D	B	B	C	I	I	C	E	B	D

Hence the plain text is FGDBBCCIICFDE, the cipher text is KPAINHHNKAF and the decipher text is FGDBBCCIICFDE.

**Remark 5.2** A 3-regular graph is a difference divisor labeling when  $n = 10$ . The resultant graph with vertex and edge label for  $n = 10$  is given in Fig. 2.

**Theorem 5.3** For  $n = 12$ , show that cycle,  $C_n$  graph is a difference divisor labeling.

**Proof** To prove this theorem, consider a cycle,  $C_6$  graph with vertices  $p = 6$  and edges  $q = 6$ . Assigning the vertex label for the cycle,  $C_6$  graph as  $V(G) = \{1, 2, \dots, n = p + q (12 = 6 + 6)\}$  and  $F(u)$  is the divisors of  $n$ . Therefore,  $x_1 = 12, x_2 = 4, x_3 = 2, x_4 = 1, x_5 = 3, x_6 = 6$ . According to the definition of difference divisor labeling, the induced edges are labelled as  $F'(x_1x_2) = 4, F'(x_2x_3) = 1, F'(x_3x_4) = 1, F'(x_4x_5) = 1, F'(x_5x_6) = 2, F'(x_6x_1) = 3$ . Hence, cycle,  $C_6$  graph is a difference divisor labeling. Therefore, cycle,  $C_n$  graph is a difference divisor labeling when

$n = 12$ . The resultant graph with vertex and edge label for  $n = 12$  is depicted in Fig. 3.

Procedure for encryption and decryption

- For cycle  $C_6$  graph, edge label is considered as the plain text.
- Converting the numerical values into alphabet value such as A=0, B=1, ..., Z=25, plain text is obtained.

**Plain text**

4	1	1	1	2	3
E	B	B	B	C	D

• Cipher text (Encryption):  $C = (aP + b) \bmod n$

Let  $P$  denotes the plain text,  $a$  refers to relatively prime to  $n$  and  $b$  represents the multiple of  $n$ . For the above cycle  $C_6$  graph,  $a = 5$ ,  $b = 3$  and  $n = 12$ . Applying these values in encryption formula, cipher text is obtained.

$$C(4) = (5 \cdot 4 + 3) \bmod 12 = 23 \bmod 12 = 11$$

$$C(1) = (5 \cdot 1 + 3) \bmod 12 = 8 \bmod 12 = 8$$

$$C(2) = (5 \cdot 2 + 3) \bmod 12 = 13 \bmod 12 = 1$$

$$C(3) = (5 \cdot 3 + 3) \bmod 12 = 18 \bmod 12 = 6$$

**Cipher text**

11	8	8	8	1	6
L	I	I	I	B	G

• Decipher text (Decryption):  $P = a^{-1}(C - b) \bmod n$

The inverse of encryption is called decryption. The modular inverse of  $a = 5 \bmod 12 \rightarrow 5x \equiv 1 \bmod 12 \rightarrow x = 5$  i.e.,  $a^{-1} = 5$ .

**Decipher text**

4	1	1	1	2	3
E	B	B	B	C	D

Hence the plain text is EBBBCD, the cipher text is LIIBIG and the decipher text is EBBBCD.

**Theorem 5.4** Show that when  $n = 24$ , a complete bipartite,  $K_{n,m}$  graph is a difference divisor labeling.

**Proof** Considering a complete bipartite,  $K_{n,m}$  graph with vertices  $p$  and edges  $q$ . For  $n = 24$ , assume the complete bipartite graph as  $K_{4,4}$  with 8 vertices and 16 edges which is depicted in the Fig. 4. Assigning the vertex label for the  $K_{4,4}$  graph as  $V(G) = \{1, 2, \dots, n = p + q (24 = 8 + 16)\}$  and  $F(u)$  is the divisors of  $n$ . Therefore,  $v_1 = 1, v_2 = 2, v_3 = 3, v_4 = 4, v_5 = 6, v_6 = 8, v_7 = 12, v_8 = 24$ . According to the definition of difference divisor labeling, the induced

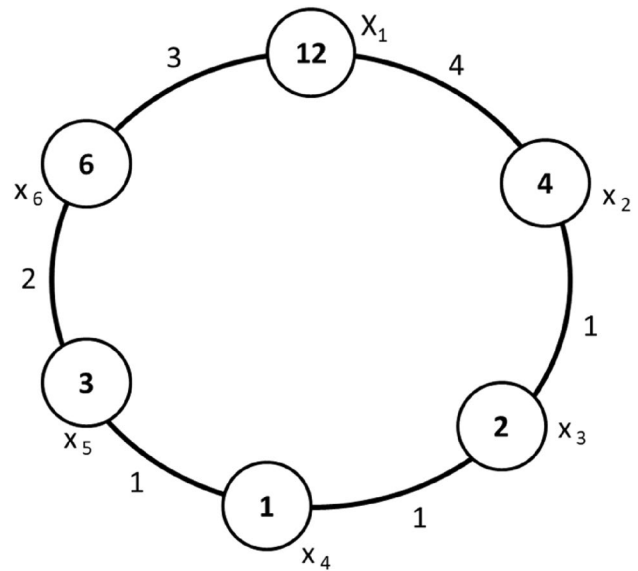


Fig. 3 Cycle  $C_6$  graph

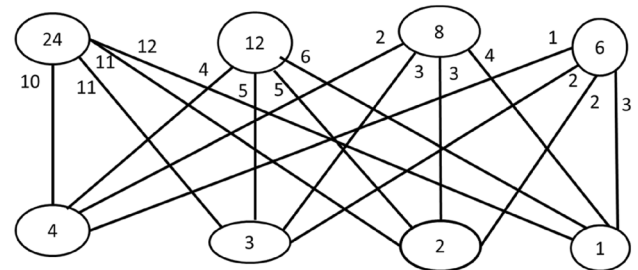


Fig. 4  $K_{4,4}$  graph

edges are labelled as  $F'(E_1) = 10, F'(E_2) = 11, F'(E_3) = 11, F'(E_4) = 12, F'(E_5) = 4, F'(E_6) = 5, F'(E_7) = 5, F'(E_8) = 6, F'(E_9) = 2, F'(E_{10}) = 3, F'(E_{11}) = 3, F'(E_{12}) = 4, F'(E_{13}) = 1, F'(E_{14}) = 2, F'(E_{15}) = 2, F'(E_{16}) = 3$ . Hence,  $K_{4,4}$  graph is a difference divisor labeling. Therefore, a complete bipartite,  $K_{n,m}$  graph is a difference divisor labeling when  $n = 24$ . The resultant graph with vertex and edge label is described below.

Procedure for encryption and decryption

- For  $K_{4,4}$  graph, edge label is considered as the plain text.
- Converting the numerical values into alphabet value such as A=0, B=1, ..., Z=25, plain text is obtained.

**Plain text**

10	11	11	12	4	5	5	6	2	3	3	4	1	2	2	3
K	L	L	M	E	F	F	G	C	D	D	E	B	C	C	E

• Cipher text (Encryption):  $C = (aP + b) \bmod n$

Let  $a$  be relatively prime to  $n$ ,  $P$  denotes the plain text and  $b$  represents the multiple of  $n$ . For the above  $K_{4,4}$  graph,  $a = 5$ ,  $b = 6$  and  $n = 24$ . Applying these values in encryption formula, cipher text is obtained.

$$C(10) = (5 \cdot 10 + 6) \bmod 24 = 56 \bmod 24 = 8$$

$$C(11) = (5 \cdot 11 + 6) \bmod 24 = 61 \bmod 24 = 13$$

$$C(12) = (5 \cdot 12 + 6) \bmod 24 = 66 \bmod 24 = 18$$

$$C(4) = (5 \cdot 4 + 6) \bmod 24 = 26 \bmod 24 = 2$$

$$C(5) = (5 \cdot 5 + 6) \bmod 24 = 31 \bmod 24 = 7$$

$$C(6) = (5 \cdot 6 + 6) \bmod 24 = 36 \bmod 24 = 12$$

$$C(2) = (5 \cdot 2 + 6) \bmod 24 = 16 \bmod 24 = 16$$

$$C(3) = (5 \cdot 3 + 6) \bmod 24 = 21 \bmod 24 = 21$$

$$C(1) = (5 \cdot 1 + 6) \bmod 24 = 11 \bmod 24 = 11$$

**Cipher text**

8	13	13	18	2	7	7	12	16	21	21	2	11	16	16	21
I	N	N	S	C	H	H	M	Q	V	V	C	L	Q	Q	V

• Decipher text (Decryption):  $P = a^{-1}(C - b) \bmod n$

The inverse of encryption is called decryption. The modular inverse of  $a = 5 \bmod 24 \rightarrow 5x \equiv 1 \bmod 24 \rightarrow x = 5$ . i.e.,  $a^{-1} = 5$ .

**Decipher text**

10	11	11	12	4	5	5	6	2	3	3	4	1	2	2	3
K	L	L	M	E	F	F	G	C	D	D	E	B	C	C	E

Hence the plain text is KLLMEFFGCDDEBCCE, the cipher text is SNNSCHHMQVVCLQQV and the decipher text is KLLMEFFGCDDEBCCE.

**Example 5.5** For  $n = 8$ ,  $P_n^2$  graph is proved as a difference divisor labeling. The figure of  $P_n^2$  graph is demonstrated in Fig. 5.

Procedure for encryption and decryption

- For  $P_n^2$  graph, edge label is considered as the plain text.
- Converting the numerical values into alphabet value such as A=0, B=1, ..., Z=25, plain text is obtained.

**Plain text**

2	3	1	1
C	D	B	B

• Cipher text (Encryption):  $C = (aP + b) \bmod n$

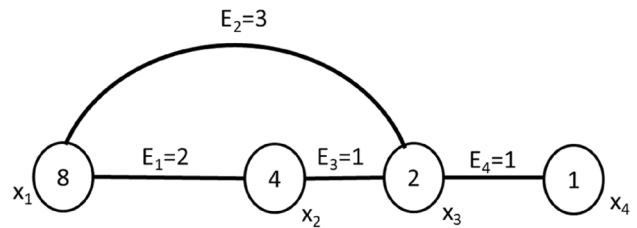


Fig. 5  $P_n^2$  graph

Let  $P$  denotes the plain text,  $a$  refers to relatively prime to  $n$  and  $b$  represents the multiple of  $n$ . For the above  $P_n^2$  graph,  $a = 5$ ,  $b = 3$  and  $n = 8$ . Applying these values in encryption formula, cipher text is obtained.

$$C(1) = (5 \cdot 1 + 3) \bmod 8 = 8 \bmod 8 = 0$$

$$C(2) = (5 \cdot 2 + 3) \bmod 8 = 13 \bmod 8 = 5$$

$$C(3) = (5 \cdot 3 + 3) \bmod 8 = 18 \bmod 8 = 2$$

**Cipher text**

5	2	0	0
F	C	A	A

• Decipher text (Decryption):  $P = a^{-1}(C - b) \bmod n$

The inverse of encryption is called decryption. The modular inverse of  $a = 5 \bmod 8 \rightarrow 5x \equiv 1 \bmod 8 \rightarrow x = 5$  i.e.,  $a^{-1} = 5$ .

**Decipher text**

2	3	1	1
C	D	B	B

Hence the plain text is CDBB, the cipher text is FCAA and the decipher text is CDBB.

**6 Conclusion**

Through mathematically based edge labeling, this study suggested a novel labeling scheme in graph theory called Difference Divisor Labeling, which aimed to enhance the usage of cryptography. Vertices were labeled based on a positive integer's divisors, while edge labels have determined by the parity and difference of neighboring vertices. This labeling paradigm provided a number of significant advantages over conventional graph labeling algorithms, which frequently suffered from issues with flexibility, scalability, and applicability when handling complicated or irregular graphs. A variety of graph classes, such as complete bipartite graphs, regular graphs, and cycle graphs, have used and proved to satisfy the requirements of the proposed labeling when Difference Divisor Labeling was applied. An encrypted graph-based cryptography system was created by using the labeled edge values as plaintext for affine and RSA ciphers. In order

to demonstrate how the labeling ensured the production of unpredictable and safe ciphertext, the paper described thorough encryption and decryption procedures for both kinds of graphs. Difference Divisor Labeling provided a general and safe platform for digital network communication by overcoming the drawbacks of conventional labelings and being easily integrated with new cryptographic algorithms. By combining discrete mathematical abstractions with information security notions, this research opened up new possibilities for graph-theoretic encryption. Future work may explore the application of Difference Divisor Labeling in dynamic and weighted graphs. Additionally, integrating this method with advanced cryptographic protocols and real-time network systems can further enhance security and scalability.

**Funding** No fund received for this project.

**Data availability** All the data is collected from the simulation reports of the software and tools used by the authors. Authors are working on implementing the same using real world data with appropriate permissions.

## Declarations

**Conflict of interest** The authors declare that they have no conflict of interest.

**Ethics approval and consent to participate** No ethics approval is required.

## References

- Hamad KJ, Mahmood SS (2025) An analytical study of graph algorithms: an overview of graph theory. *QALAAI ZANIST J* 10(1):1217–1238
- Gupta A, Matta P, Pant B (2021) Graph neural network: current state of Art, challenges and applications. *Mater Today: Proc* 46:10927–10932
- Xu M (2021) Understanding graph embedding methods and their applications. *SIAM Rev* 63(4):825–853
- Bhatti UA, Tang H, Wu G, Marjan S, Hussain A (2023) Deep learning with graph convolutional networks: an overview and latest applications in computational intelligence. *Int J Intell Syst* 2023(1):8342104
- Tanglay O, Dadario NB, Chong EH, Tang SJ, Young IM, Sughrue ME (2023) Graph theory measures and their application to neuro-surgical eloquence. *Cancers* 15(2):556
- Silver S (2023) Hogarth's networks and the eighteenth-century graphic novel. *Novel: a forum on fiction*, vol 56, no 2. Duke University Press, pp 256–279. <https://doi.org/10.1215/00295132-10562853>
- Gröger G, George B (2022) *Geometry and topology*. Springer handbook of geographic information. Springer International Publishing, Cham, pp 297–313
- Barnett JH (2022) Primary source projects as textbook replacements: A commognitive analysis. *ZDM—Mathematics Educ* 54(7):1569–1582
- Henderson A (2021) *Combinatorial characters*. The Palgrave Handbook of Literature and Mathematics, 493–512
- Bechler-Speicher M, Globerson A, Gilad-Bachrach R (2024) The intelligible and effective graph neural additive network. *Adv Neural Inf Process Syst* 37:90552–90578
- Xia F, Sun K, Yu S, Aziz A, Wan L, Pan S, Liu H (2021) Graph learning: A survey. *IEEE Trans Artif Intell* 2(2):109–127
- El Deen Z, Ramadan M (2024) Super edge magic harmonious labeling for certain graphs. *Front Sci Res Technol* 8(1). <https://doi.org/10.21608/fsrt.2023.248393.1114>
- Dhokrat VT, Jadhav DP, Gaikwad DS (2023) A survey study of association between graph and graph labeling techniques. *Int J Educ Mod Manage Appl Sci Social Sci (IJEMMASS)* 5(3):19–30
- Gawrychowski P, Janczewski W, Łopuszański J (2021) Shorter labels for routing in trees. In *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA)* (pp. 2174–2193). Society for Industrial and Applied Mathematics
- Beineke LW, Hegde SM, Kamalappan VV (2021) A survey of two types of labelings of graphs. *Discrete Math Lett* 6:8–18
- Sugeng KA, Barack ZZ, Hinding N, Simanjuntak R (2021) Modular irregular labeling on Double-Star and friendship graphs. *J Math* 2021(1):4746609
- Badr E, Nada S, Al-Shamiri A, Abdel-Hay MM, A., ELrokh A (2022) A novel mathematical model for radio mean square labeling problem. *J Math* 2022(1):3303433
- Aasi MS, Asif M, Iqbal T, Ibrahim M (2021) Radio labelings of lexicographic product of some graphs. *J Math* 2021(1):9177818
- Tharani AP, Saradha P (2024) Discrete labeling of graphs. *Indian J Sci Technol* 17:93–102
- Almohanna N, Alhulwah K (2024) NK-Labeling of graphs. *Am J Comput Math* 14(4):391–400
- Bonucci P, Nicolás, Capitelli (2022) Weak harmonic labeling of graphs and multigraphs. *Discrete Math* 345:112816
- Meena S, Gajalakshmi G, Kavitha P (2022) Prime labeling of h-super subdivision of cycle related graph. In *AIP Conference Proceedings* (Vol. 2516, No. 1). AIP Publishing
- Tomita VAK, Marcacini RM (2025) Pseudo-labeling domain adaptation using multi-model learning. *IEEE Access* 13:41486–41504. <https://doi.org/10.1109/ACCESS.2025.3547813>
- Gopi R, Prakash V (2023) Research article K-super contra harmonic mean labeling of graphs. *AJMS* 7(3):113–116
- Nagaraja KM, Ramachandraiah S, Siddappa VB (2021) Power exponential means labeling of graphs. *Montes Taurus J Pure Appl Math* 3(2):70–79
- Gupta P, Gupta S, Srivastav S (2025) *Crypto-Encoding Communication with Graph Theory*. In: Alam, K., Khan, A., Singh, R.C., Karaca, Y (Eds) *Mathematical modeling, applied analysis and computational methods*. ICAIM 2023. Springer Proceedings in Mathematics & Statistics, vol 482. Springer, Singapore. [https://doi.org/10.1007/978-981-96-3460-6\\_11](https://doi.org/10.1007/978-981-96-3460-6_11)
- Shastri VH, Pragathi C (2024) Data security using Crypto bipartite graph theory with modified Diffie–Hellman algorithm. *Wirel Pers Commun* 139:1905–1926. <https://doi.org/10.1007/s11277-024-11679-y>
- Djordjevic IB (2025) *Conventional cryptography fundamentals*. Physical-Layer Security, quantum key Distribution, and Post-Quantum cryptography. Springer, Cham. [https://doi.org/10.1007/978-3-031-88372-9\\_3](https://doi.org/10.1007/978-3-031-88372-9_3)
- Orduz J (2025) *Mathematical foundations for modern cryptography in the quantum era*. In: Arabnia HR, Deligiannidis L, Shenavarmasouleh F, Amirian S, Ghareh Mohammadi F (eds) *Computational science and computational intelligence*. CSCI 2024. Communications in computer and information science, vol 2510. Springer, Cham. [https://doi.org/10.1007/978-3-031-94956-2\\_16](https://doi.org/10.1007/978-3-031-94956-2_16)

30. Joshi AB, Kumar D, Kumar S et al (2024) A novel method of digital image encryption using graph theory. *Multimed Tools Appl* 83:6803–6828. <https://doi.org/10.1007/s11042-023-15698-y>
31. Hartmann P (2023) Graph theory. *Mathematics for computer scientists*. Springer, Wiesbaden. [https://doi.org/10.1007/978-3-658-40423-9\\_11](https://doi.org/10.1007/978-3-658-40423-9_11)

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.