A Novel Approach Using Edge Irregular Reflexive k-Labeling for Robust Keystream in Asymmetric Cryptography to Protect DNA Sequence

Marsidi, Dafik*, Susanto, Arika Indah Kristiana, and Nelly Oktavia Adiwijaya

***Abstract*—Data security is critical in the digital age, especially for protecting sensitive information such as DNA sequences. One approach can be used is asymmetric cryptography, where a robust keystream is required to maintain data confidentiality. This research proposes a new method using irregular reflexive edge k-labeling on graphs to generate a secure and complex robust keystream. This approach uses labeling theory to create keystreams that are difficult to predict, thus providing better protection against cryptography attacks, especially in protecting sensitive DNA sequences. The method used in this research involves several steps. First, the graph is determined to represent of the data structure to be labeled. Next, an irregular reflexive k labeling is applied to the graph to generate a secure keystream pattern. The results show that the resulting keystream has a high degree of complexity and is difficult to predict, effectively improving asymmetric cryptography's security. The discussion of implementing this labeling also shows that this method can significantly contribute to developing labeling theory and practical applications in protecting biological data such as DNA sequences.**

***Index Terms*—Edge irregular reflexive $k-$labeling, reflexive edge strength, Asymmetric Cryptography, Robust Keystream.**

I. Introduction

Technological developments in bioinformatics and biotechnology have significantly impacted the storage and transmission of genetic data, particularly DNA sequences, which contain detailed biological information about individual or species characteristics and are of great value in medical research, drug development, gene therapy, and forensics [1]. However, as the use of genetic data in medical and technological applications increases, so do the threats to its security, making DNA sequences a prime target for encryption and security. If left unprotected, this data can be misused for genetic discrimination, unethical insurance or employment decisions, or even biological identity theft, so strong protection through cryptography techniques is critical.

Manuscript received October 9, 2024; revised July 28, 2025. This work was supported in part by support of PUI-PT Combinatorics and Graph, CGANT-University of Jember, and LP2M-University of Jember, for the research collaboration of the year 2025.

Marsidi is a Postgraduate student in the Department of Postgraduate Mathematics Education, University of Jember, Jember, Indonesia (e-mail:marsidiarin@gmail.com).

Dafik is a Professor in the Department of Mathematics, University of Jember, Jember, Indonesia (Corresponding Author, e-mail:d.dafik@unej.ac.id).

Susanto is a Lecturer in the Department of Postgraduate Mathematics Education, University of Jember, Jember, Indonesia (e-mail:susanto.fkip@unej.ac.id).

A. I. Kristiana is a Lecturer in the Department of Postgraduate Mathematics Education, University of Jember, Jember, Indonesia (e-mail:arikakristiana@unej.ac.id).

N. O. Adiwijaya is a Lecturer in the Department of Informatics, University of Jember, Jember, Indonesia (e-mail:nelly.oa@unej.ac.id).

However, the biggest challenge in protecting DNA sequence data is ensuring that the cryptography methods used can provide a high level of security without sacrificing the efficiency of the encryption and decryption process. Genetic data has unique characteristics, including large volume and high complexity, making it vulnerable to cyber attacks if the security methods are not strong enough. In addition, because this data often needs to be accessed quickly and used in applications that require real-time responses, such as medical diagnosis or ongoing genetic research, cryptography systems must also be efficient and fast [2].

One of the cryptographic methods commonly used to secure DNA sequence data is asymmetric cryptography [3], [4], [5]. While this method can provide robust security, its reliability is highly dependent on the strength of the keystream used in the encryption process [6]. Therefore, developing of a robust and hard-to-guess keystream is critical to improving the robustness of cryptographic systems. To this end, a graph-theoretic approach, precisely edge irregular reflexive k labeling, offers an innovative solution for generating more random and difficult-to-crack keystreams.

Using edge irregular reflexive k-labeling, this research focuses on developing stronger and more dynamic keystreams in asymmetric cryptography systems. This system is essential for protecting of DNA sequences, one of the most sensitive and valuable forms of biological information. Through the edge irregular reflexive k-labeling technique, the distribution of labels on an irregular graph allows the creation of random keystream patterns, thus increasing the robustness against cryptography attacks aimed at predicting or breaking encryption keys. This is important because strong encryption algorithms alone are not enough, but also require an unpredictable keystream to provide an additional layer of security that is difficult to penetrate [7].

In addition to strengthening the security layer, this method is also designed to provide flexibility in the encryption and decryption process. This flexibility is important so that the process of encoding and recovering data can be performed efficiently without compromising its security level. In the context of DNA sequence encoding, this flexibility allows for effective data protection without compromising the processing speed or integrity of the encoded data. It also provides for the integration of current issues in cryptography, such as the challenges of protecting data in cloud-based systems or open networks that are vulnerable to attack.

Research on irregular edge reflexive k-labeling has been a topic of interest for many researchers in recent years, especially in the context of the development of graph theory. The basic concept of graph theory can be seen in [8], [9],

[10], [11], while the concept of labeling was introduced by Baca et al. [12]. The concept of irregular edge reflexive k-labeling was introduced by Tanna et. al. [13]. Some research results on irregular edge reflexive k labeling can be found in [14], [13], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25]. In addition, there are several studies that combine cryptography with labeling techniques. Dafik et al. introduced the concept of local super antimagic total face coloring to generate encryption keys for block ciphers by mapping graph components to natural numbers, enhancing key complexity and security [26]. This method was further developed in 2021 to create a cipher block chaining (CBC) key, providing secure encryption for IoT environments through unique face weights in graph labeling [26]. In 2022, rainbow antimagic coloring was applied to improve the robustness of the affine cipher, ensuring different edge weights for stronger encryption [27]. Prihandoko et al. also used graph labeling to generate stream-keys for a modified Vigenère cipher, assigning unique keys to each block of plaintext to enhance security [28]. Additionally, Agustin et al. introduced rainbow vertex antimagic coloring for constructing dynamic encryption keystreams, growing with plaintext size and applied in affine block ciphers [29]. This method strengthens symmetric cryptography, offering greater resilience against attacks compared to traditional ciphers like AES and DES. Overall, these studies demonstrate graph labeling techniques' increasing role in enhancing cryptographic systems' security and robustness across different encryption methods.

Research in graph theory and its applications has advanced significantly, particularly in developing labeling methods with practical implications, including cryptography [30]. The graceful chromatic number of unicyclic graphs provides insights into efficient coloring schemes relevant to communication networks [31]. The study of non-isolated resolving numbers in special graphs introduces novel approaches for identifying unique points, useful for data security [32]. Additionally, rainbow antimagic coloring enhances cryptographic systems by ensuring unique and unpredictable edge weights [33]. Further, investigations on the locating edge domination number and distance domination number in comb product graphs contribute to optimizing data protection through effective vertex and edge domination strategies [34], [35]. These studies form a robust foundation for advancing cryptographic methods to secure sensitive data like DNA sequences.

However, despite many related studies, the development and application of the irregular edge reflexive k labeling concept remains unique and novel. The contributions of these studies not only broaden the scope of graph theory, but also open up new opportunities for its application in cryptography. With this new approach, it is expected to achieve a breakthrough in cryptography technology for securing genetic data, which is increasingly used in various fields such as medical research, biotechnology, and digital biological data storage. Therefore, this research has the following objectives: (1) Construct robust keystream in asymmetric cryptography with irregular edge reflexive k labeling. This article derives a new theorem of irregular edge reflexive k labeling. (2) To determine the effectiveness of this method in improving the security of DNA sequence protection against the threat of cyber attacks by evaluation based on brute force attacks. (3) To determine the efficiency of this method in terms of encryption and decryption process efficiency compared to the asymmetric cryptographic approaches AES and DES in terms of time and size complexity.

II. Algorithm of Asymmetric Cryptography and Flowchart of Research

In this section, we will take a closer look at the technical aspects of securing biometric data, with a focus on DNA sequence data. We will examine three key components in the process of securing this data: the keystream algorithm, the encryption process, and the decryption process. Each of these elements plays a critical role in ensuring that DNA data containing highly personal and sensitive genetic information, is protected from unauthorized access and manipulation.

A. Asymmetric Cryptography Key Algorithm

First, we will understand the keystream algorithm, which is the heart of the encryption system. It generates a sequence of bits that transforms the information into a secure format that cannot be interpreted without the appropriate key when combined with the original data. The keystream algorithm is essential because of its ability to generate a random and unpredictable sequence, thus increasing the security of the data. The keystream algorithm is shown in Algorithm 1.

Algorithm 1: Keystream Algorithm using Edge Irregular Reflexive Labeling

Input : text (plain text DNA Sequence), G(graph $G(V, E)$)
Output: keystream (a and b)

length(text)
define v as vertex and e as an edge from G
define n as length(text)
relative primes = $gcd(w(e_i), 94)$
for *i in range(1,n)* **do**
    if *is relative prime(i,n)* **then**
        relative primes.append(i)
    return relative primes
define a as relative primes
obtain b from weight edge irregular reflexive labeling

B. Encryption Process Algorithm

Next, we will discuss the encryption process, the step in which DNA data is converted from its original format to an encrypted form. This process involves using a keystream algorithm to transform each bit of DNA data, resulting in an output that can only be interpreted or restored to its original form through a proper decryption process. The algorithm of the encryption process is shown in Algorithm 2.

C. Decryption Process Algorithm

In this subsection, we will examine the decryption process, which is the reverse of encryption. This process is essential to ensure that the encrypted DNA data can be restored to its original form, allowing secure and accurate access by authorized parties. The decryption process must be performed

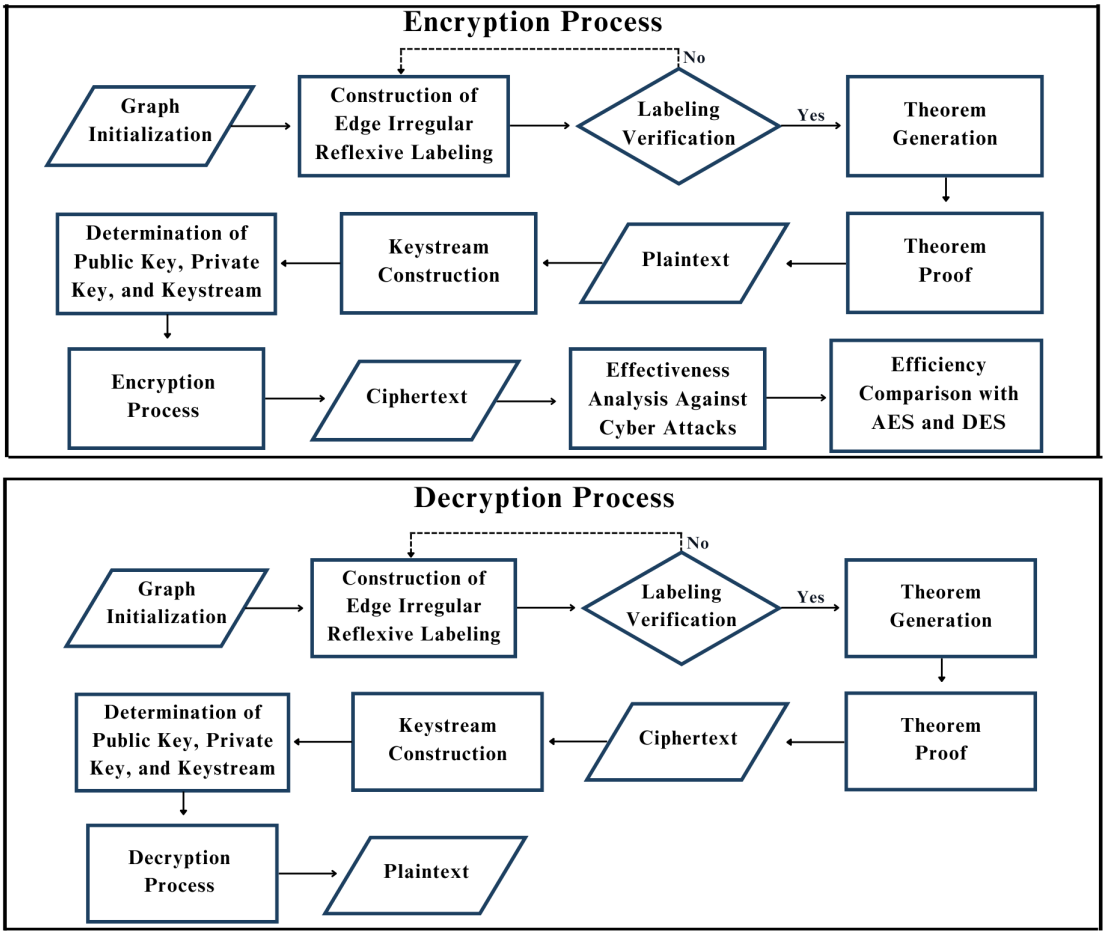

Fig. 1. Flowchart of Research.

Algorithm 2: Encryption Algorithm

Input : text (plain text DNA Sequence)
Output: cipher text (text encryption from DNA Sequence)

```
for char in text do
    if char.isalpha() then
        if char.islower() then
            block cipher += chr(((a * (ord(char) - ord('a')) + b) % 94) + ord('a'))
        else if char.ishigher() then
            block cipher += chr(((a * (ord(char) - ord('A')) + b) % 94) + ord('A'))
        block cipher += char
    return block cipher
combine all block cipher as C
determine p as private key from GCD(a, p) = 1
```

Algorithm 3: Decryption Algorithm

Input : cipher text (text encryption from DNA Sequence) and p
Output: text (plain text DNA Sequence)

```
define l as length(cipher text)
define v as vertex and e as edge from G
define L as length(keystream)
for char in cipher text do
    if char.isalpha() then
        if char.islower() then
            block decrypt += chr(((inv(a) * (ord(char) - ord('a')) + b) % 94) + ord('a'))
        else if char.ishigher() then
            block decrypt += chr(((inv(a) * (ord(char) - ord('A')) + b) % 94) + ord('A'))
        block decrypt += char
    return block decrypt
combine p to each all block decrypt to obtain text
```

rigorously to ensure that the integrity of the DNA data is maintained so that the resulting information remains accurate and reliable. The algorithm for the decryption process is shown in Algorithm 3.

D. Flowchart of Research

This section presents a research flowchart that provides a clear and systematic description of the steps taken throughout the research. The research flowchart is shown in Figure 1. This flowchart summarizes the main process, starting from the initial problem identification, through the construction and verification of the irregular reflexive edge labeling, to the implementation of the cryptographic system and its analysis. Each step is designed to ensure a logical progression from

theoretical foundations to practical application, allowing for a structured and efficient research process. The following flowchart illustrates the workflow of this research.

III. Data and Setup

In this chapter, we will explore the important process of data preparation for DNA sequences. We will use Google Collaboratory to perform the encryption and decryption process of the DNA sequence data. The specifications of Google Collaboratory are 13 GB RAM, 33 GB hard disk, and 16 GB DDR6 Nvidia Tesla T4 VGA. Next, we performed the data assembly process of DNA sequences from NCBI and EMBL datasets. The main purpose of this process is to ensure that the DNA data we use for further analysis or research is accurate, consistent, and reliable. Here are the steps involved in the data retrieval process:

1) Dataset selection: Select appropriate DNA datasets based on criteria such as relevance, quality, and data integrity.
2) Download and Validation: Downloading the selected dataset and validating it to ensure that the data is free of errors or defects.
3) Data cleaning: Removes redundant or irrelevant data and performs normalization for format and nomenclature consistency.
4) Annotation: Adding additional information to DNA data to enhance its analytical value.
5) Conversion and Presentation: Converts DNA sequences into formats suitable for analysis and presents data in a structured manner.
6) Storage and Management: Securely stores and manages data for easy access and future use.

After we receive the dataset, we will convert the dataset to numbers based on Table 1. The purpose of this conversion is to ensure the confidentiality of the DNA data. In addition, we also analyze the encryption and decryption results of DNA sequences using graph theorem and compare them with AES and DES cryptography. The encryption and decryption processes analyzed were brute force attacks, time attacks, encryption result length, and encryption time.

IV. Results and Discussions

The first step in this research is to determine the graph as the main object of study, namely $P_n \rhd P_3$. The next step is to construct the irregular reflexive edge labeling k. This labeling process is carried out with the aim of finding a pattern to obtain the weight of each graph edge, where each graph has different characteristics compared to other graphs. From this construction, the result obtained is then formulated in the following theorem. This theorem not only presents the final result of the labeling process, but is also accompanied by a mathematical proof that supports the validity of the theorem. The theorem makes a significant contribution to the development of graph theory, especially in the context of labeling theory. In addition to theoretical contributions, the following theorem provides novelties in graph labeling theory, especially in irregular reflexive k labeling.

Theorem 1: Let $P_n \rhd P_3$ be a comb product graph of P_n and P_3. For every natural number $n \geq 3$,

$$res(P_n \rhd P_3) = \begin{cases} \lceil \frac{3n-1}{3} \rceil + 1, & \text{if } \ 3n-1 \equiv 2 \pmod 6 \\ \lceil \frac{3n-1}{3} \rceil, & \text{otherwise} \end{cases}$$

Proof. Let $P_n \rhd P_3$, for $n \geq 3$, be a graph with the vertex set $V(P_n \rhd P_3) = \{x_i, y_{i,1}, y_{i,2} : 1 \leq i \leq n\}$ and the edge set $E(P_n \rhd P_3) = \{x_i x_{i+1} : 1 \leq i \leq n-1\} \cup \{x_i y_{i,1}, y_{i,1} y_{i,2} : 1 \leq i \leq n\}$. The order and size of $P_n \rhd P_3$ are $3n$ and $3n-1$, respectively. Based on lower bound Lemma of $res(G)$, we have $res(P_n \rhd P_3) \geq \lceil \frac{|E(G)|}{3} \rceil = \lceil \frac{3n-1}{3} \rceil + 1$ for $n \equiv 2(mod\ 6)$ and $res(P_n \rhd P_3) \geq \lceil \frac{|E(G)|}{3} \rceil = \lceil \frac{3n-1}{3} \rceil$ for otherwise.
Furthermore, we show an upper bound of reflexive edge strength of $P_n \rhd P_3$, by defining the following functions.

$$f_v(x_i) = \begin{cases} 0, & \text{if } \ i = 1 \\ 2\lceil \frac{i-1}{2} \rceil, & \text{if } \ i \geq 2 \end{cases}$$

$$f_v(y_{i,1}) = \begin{cases} 0, & \text{if } \ i = 1, 2 \\ 2, & \text{if } \ i = 3 \\ 2\lceil \frac{i-3}{2} \rceil + 2, & \text{if } \ i \geq 4 \end{cases}$$

$$f_v(y_{i,2}) = \begin{cases} 0, & \text{if } \ i = 1 \\ 2, & \text{if } \ i = 2 \\ 2\lceil \frac{i-2}{2} \rceil + 2, & \text{if } \ i \geq 3 \end{cases}$$

$$f_e(x_i x_{i+1}) = i : 1 \leq i \leq n-1$$

$$f_e(x_i y_{i,1}) = \begin{cases} 2, & \text{if } \ i = 1, 2 \\ i, & \text{if } \ i \geq 3 \text{ and } i \text{ odd} \\ i-2, & \text{if } \ i \geq 4 \text{ and } i \text{ even} \end{cases}$$

$$f_e(y_{i,1} y_{i,2}) = \begin{cases} 1, & \text{if } \ i = 1 \\ 3, & \text{if } \ i = 2 \\ i-1, & \text{if } \ i \geq 3 \end{cases}$$

The edge weight from the above function will give edge weight sets in the following.

$$w(y_{i,1} y_{i,2}) = \begin{cases} 1, & \text{if } \ i = 1 \\ 3i-1, & \text{if } \ 2 \leq i \leq n \end{cases}$$

$$w(x_i y_{i,1}) = \begin{cases} 2, & \text{if } \ i = 1 \\ 3i-2, & \text{if } \ 2 \leq i \leq n \end{cases}$$

$$w(x_i x_{i+1}) = 3i : 1 \leq i \leq n-1$$

We can see that the all edge weights on $P_n \rhd P_3$ are distinct. From the labeling on $P_n \rhd P_3$, it gives $res(P_n \rhd P_3) \leq \lceil \frac{3n-1}{3} \rceil + 1$ for $n \equiv 2(mod\ 6)$ and $res(P_n \rhd P_3) \leq$

TABLE I
CHARACTER TO NUMBER CONVERSION.

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

$\lceil \frac{3n-1}{3} \rceil$ for otherwise. Since the upper bound value reaches the lower bound, then it concludes that $res(P_n \rhd P_3) = \lceil \frac{3n-1}{3} \rceil + 1$ for $n \equiv 2(mod\ 6)$ and $res(P_n \rhd P_3) = \lceil \frac{3n-1}{3} \rceil$ for otherwise. □

From the labeling results, a robust keystream is developed to support asymmetric cryptography's encryption and decryption process. These keystreams ensure data security by creating complex and unpredictable encryption patterns. This makes the resulting encryption and decryption process more resistant to cyber-attacks, especially in the context of protecting biological data such as large DNA sequences.

A. Keystream Construction Using Edge Irregular Reflexive Labeling

This section describes the results of edge irregular reflexive labeling analysis on the $P_n \rhd P_3$ graph and its application to designing DNA sequence keys for asymmetric cryptography. The key analysis results are evaluated based on the level of cryptographic security and the efficiency of the encryption and decryption process with a focus on the use of DNA keys. The discussion also covers the security strength, encryption efficiency, and potential application of DNA keys in asymmetric cryptography.

Figure 2 illustrates the keystream construction process. The process begins by determining the length of the plaintext (l), which affects the number of nodes and edges in the graph. Next, the graph structure is determined based on the number of nodes and edges adjusted to the plaintext length using a mathematical formula. The public key is then assigned and chosen as the largest edge weight, which is relatively prime to 94 characters. Finally, a keystream is generated from the graph edge weights to enhance cryptographic security.

Next, we illustrate the keystream acquisition process using Theorem 1. For example, the DNA sequence part to be encrypted is "ATGCGCATTAGGTTGCAA". The first step is to determine the value of n based on the plaintext p. Theorem 1 discusses irregular edge reflexive labeling on the graph $P_n \rhd P_3$, with the formula $n = \left\lceil \frac{|p|+1}{3} \right\rceil$. Then the keystream a and b are determined, with a as the public key obtained from the largest weight that is relatively prime to 94, and b as the set of keystreams as many as p generated from the edge irregular reflexive labeling weights. Keystream b is divided into three blocks: block 1 is the edge weight $y_{i,1}y_{i,2}$, block 2 is the edge weight $x_iy_{i,1}$, and block 3 is the edge weight x_ix_{i+1}. Based on the given plaintext, $n = 7, a = 19$, and $b_i = \{1, 5, 8, 11, 14, 17, 20, 2, 4, 7, 10, 13, 16, 19, 3, 6, 9, 12, 15, 18\}$..

This section also describes the private key used in the decryption process. In asymmetric cryptography, the private key is part of the key pair that decrypts the message encrypted with the public key. The private key is generated by a cryptography algorithm that ensures a mathematical relationship with the public key but is not easily predictable. Therefore, the private key must be stored securely to keep the data confidential. In this context, the private key is derived from the graph edge weight and is the inverse of the public key a. The resulting private key is $\{5, 99, 193, 287, 381, \cdots\}$..

1) The Encryption Process: The encryption process using Edge Irregular Reflexive Labeling and asymmetric cryptography combines the concept of graph labeling with cryptographic techniques to produce a strong encryption method. The labels on the vertices and edges of this graph are used to generate weights that play a role in the formation of the keystream and encryption key.

As explained earlier, the keystream is a string of numbers used as encryption input. The encryption process is performed using the formula $C_i = ((a \times P_i) + b_i) mod\ 94$, where C_i is the ciphertext symbol generated from the plaintext symbol P_i. Variable a is the public key, and b_i is derived from the irregular reflexive labeling of edge weights. This formula ensures that each plaintext symbol is scrambled into an unreadable ciphertext without the corresponding key.

For example, a DNA sequence that originally contains the data "ATGCGCATTAGGTTAGGT" has been encrypted using the formula, resulting in a ciphertext of "B/cxi3U>?HehBEXsJM". Table II shows how the encryption formula transforms these plain-text symbols into ciphertext. This table facilitates a visual understanding of the transformation from plaintext to ciphertext in this encryption process.

This explanation emphasizes the importance of the keystream and how the encryption formula works to protect the confidentiality and integrity of data, especially in applications that involve encoding messages or protecting genetic information.

2) The Decryption Process: The decryption process uses a combination of EIRL and asymmetric cryptography, which involves using a private key to decrypt a message or data that has been encrypted with the associated public key. Elements in a structure scrambled using EIRL can act as key components or parameters in the decryption process, increasing the

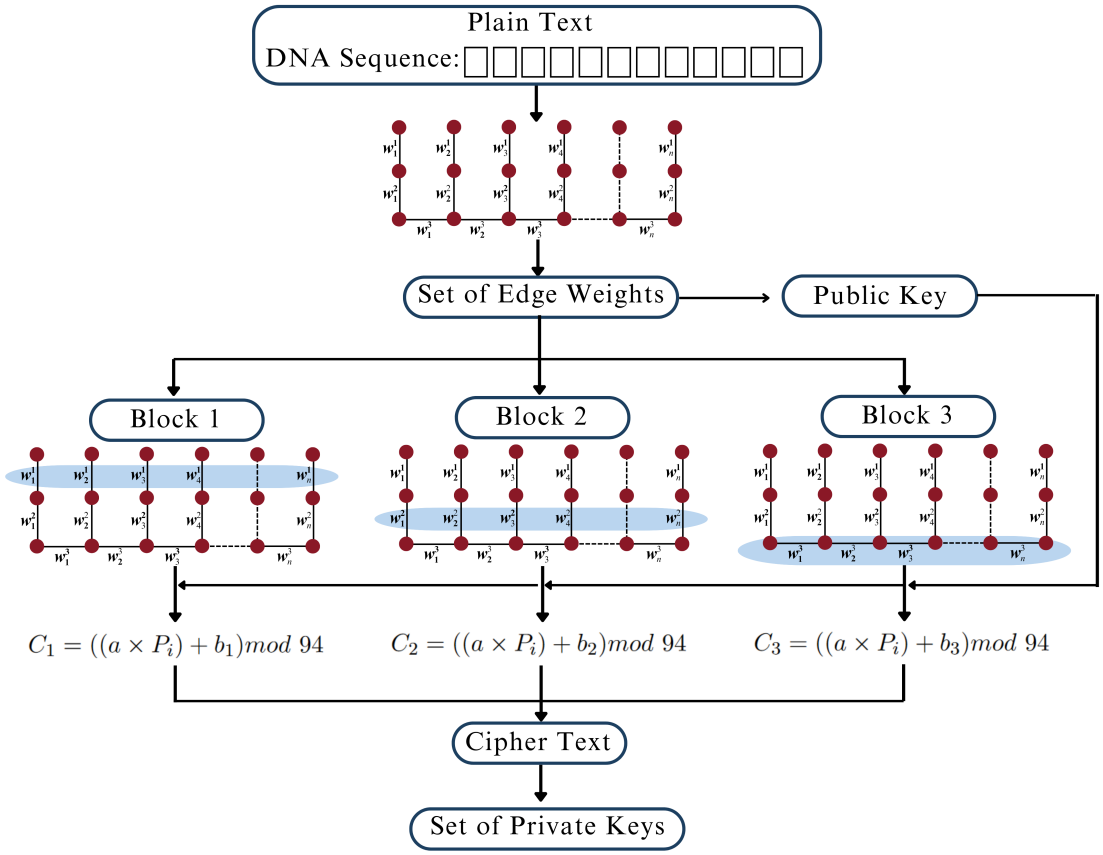

Fig. 2. Keystream Construction Process

TABLE II
ILLUSTRATION OF ENCRYPTION WITH ROBUST ASYMMETRIC CRYPTOGRAPHY BASED ON EDGE IRREGULAR REFLEXIVE LABELING

P	A	T	G	C	G	C	A	T	T	A	G	G	T	T	G	C	A	A
P_i	0	19	6	2	6	2	0	19	19	0	6	6	19	19	6	2	0	0
a	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
b_i	1	5	8	11	14	17	20	2	4	7	10	13	16	19	3	6	9	12
C_i	1	84	28	49	34	55	20	81	83	7	30	33	1	4	23	44	9	12
C	B	/	c	x	i	3	U	>	?	H	e	h	B	E	X	s	J	M

security and complexity of the overall cryptography system. This section will explore the basic concepts of asymmetric cryptography, the use of Edge Irregular Reflexive Labeling in a cryptography context, and how these two techniques can be combined to enhance security and privacy in data communication and storage. This exploration will provide a deep insight into the practical application of these theoretical concepts in the context of modern information security.

Subsection A has explained the process of obtaining the private key. The private key received from the previous example is $\{5, 99, 193, 287, 381, \cdots\}$. The decryption process uses the formula $P_i = ((C_i - b_i) \times a^{-1}) mod\ 94$, where a^{-1} is the set of private keys. An illustration of the decryption process can be seen in Table III. Based on Table III, we can know the illustration of the decryption process from ciphertext B/cxi3U>?HehBEXsJM to plaintext ATGCGCATTAGGTTGCAA.

B. Brute force attacks

A brute force attack is a technique used to obtain sensitive information such as usernames, passwords, or encryption keys by trying all possible combinations until the correct combination is found. This approach is very systematic but needs more sophistication, as brute force attacks do not try to identify specific weaknesses in the system but rely on pure processing power to try every possibility. Standard methods include dictionary attacks, which use a compiled list of words; pure brute force attacks, which try every possible combination of characters; and hybrid attacks, which combine elements of both. Analysis of the resulting brute force attacks shows that the resulting cipher text cannot be cracked using brute force attacks. This is because we use keystream edge irregular reflexive labeling.

In conclusion, a brute force attack is a systematic method of obtaining sensitive information by trying all possible combinations, such as usernames, passwords, or encryption keys. While this approach does not take advantage of specific

TABLE III
ILLUSTRATION OF DECRYPTION WITH ROBUST ASYMMETRIC CRYPTOGRAPHY BASED ON EDGE IRREGULAR REFLEXIVE LABELING

C	B	/	c	x	i	3	U	>	?	H	e	h	B	E	X	s	J	M
C_i	1	84	28	49	34	55	20	81	83	7	30	33	1	4	23	44	9	12
a^{-1}	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
b_i	1	5	8	11	14	17	20	2	4	7	10	13	16	19	3	6	9	12
P_i	0	19	6	2	6	2	0	19	19	0	6	6	19	19	6	2	0	0
P	A	T	G	C	G	C	A	T	T	A	G	G	T	T	G	C	A	A

weaknesses in the system, its strength lies in its ability to try every combination of characters. Commonly used methods include dictionary attacks, pure brute force attacks, and hybrid attacks. However, an analysis of brute force attacks shows that the developed cryptographic method, which uses keystream edge irregular reflexive labeling, cannot be cracked by brute force techniques. This is due to the complexity of the keystream generated, which makes finding the right key by brute force impractical and ineffective.

C. Validation of Graph-Based Cryptography: Insights from Rainbow Vertex Antimagic Coloring

The application of graph-based cryptographic techniques has gained significant attention due to its potential in enhancing key security and encryption robustness. One notable approach, Rainbow Vertex Antimagic Coloring (RVAC), has been successfully utilized in asymmetric cryptography, demonstrating its capability in generating secure and unique keystreams. The study "A Robust Algorithm for Asymmetric Cryptography Using Rainbow Vertex Antimagic Coloring" introduced an encryption method based on rainbow vertex antimagic labeling, which has proven effective in ensuring distinct key assignments and preventing cryptanalytic vulnerabilities [33].

1) Contributions of Rainbow Vertex Antimagic Coloring (RVAC) in Cryptography: The RVAC method provides an effective framework for asymmetric encryption through vertex labeling, ensuring unique weight distributions across cryptographic paths. Its key contributions include:

- Keystream Uniqueness: The labeling scheme ensures that each vertex has a distinct antimagic weight, reducing key duplication risks in asymmetric encryption.
- Security Enhancement: The rainbow path structure ensures that every cryptographic transaction follows a distinct antimagic sequence, preventing key predictability.
- Scalability in Cryptographic Applications: RVAC has been explored in various asymmetric encryption models, proving its adaptability to different cryptographic scenarios.

2) Extending Graph-Based Cryptography with Edge Irregular Reflexive k-Labeling: Building on the success of RVAC in asymmetric cryptography, this study introduces *Edge Irregular Reflexive k-Labeling* as an alternative approach for enhancing keystream generation in DNA sequence protection. While RVAC has demonstrated effectiveness in vertex-based encryption, this study explores an edge-based labeling approach, which offers a complementary perspective in key distribution strategies. The key enhancements in this method include:

1) Irregular Edge Labeling for Keystream Generation: Unlike RVAC, which focuses on vertex labeling to determine edge weights, Edge Irregular Reflexive k-Labeling generates unique keystreams by directly assigning irregular weights to edges, thereby enhancing security in cryptographic applications.
2) Adaptability for DNA Sequence Encryption: The flexibility of edge-based labeling allows for a secure and structured keystream applicable to biological encryption, particularly in protecting sensitive genetic data.
3) Complementary Strengths in Cryptographic Security: By leveraging edge irregularity, this approach adds an additional layer of unpredictability, which is crucial for safeguarding encryption processes against cryptanalytic attacks.

3) Comparative Insights: RVAC vs. Edge Irregular Reflexive k-Labeling: Both RVAC and Edge Irregular Reflexive k-Labeling contribute to the advancement of graph-based cryptographic methods, each offering unique strengths in different applications. The following comparison outlines their key attributes:

4) Key Takeaways from the Validation Process:

- RVAC has successfully demonstrated the feasibility of graph-based asymmetric cryptography, establishing a strong foundation for combinatorial graph techniques in key generation.
- Edge Irregular Reflexive k-Labeling expands upon these principles by introducing edge-based keystream generation, which is particularly suitable for DNA sequence encryption.
- Both approaches provide valuable contributions to cryptographic security, and their application depends on the specific encryption context and security requirements.

5) Implications for Graph-Based Cryptography and DNA Protection: The validation of RVAC confirms the effectiveness of combinatorial graph labeling in cryptographic keystream generation. By incorporating *Edge Irregular Reflexive k-Labeling*, this study extends the utility of graph-based encryption methods to DNA sequence protection, demonstrating that both vertex-based and edge-based approaches offer distinct yet complementary advantages in securing cryptographic applications.

This validation strengthens the argument that graph theory continues to be a powerful tool in asymmetric encryption, reinforcing the scientific foundation and practical relevance of the proposed method while building upon prior research in the field.

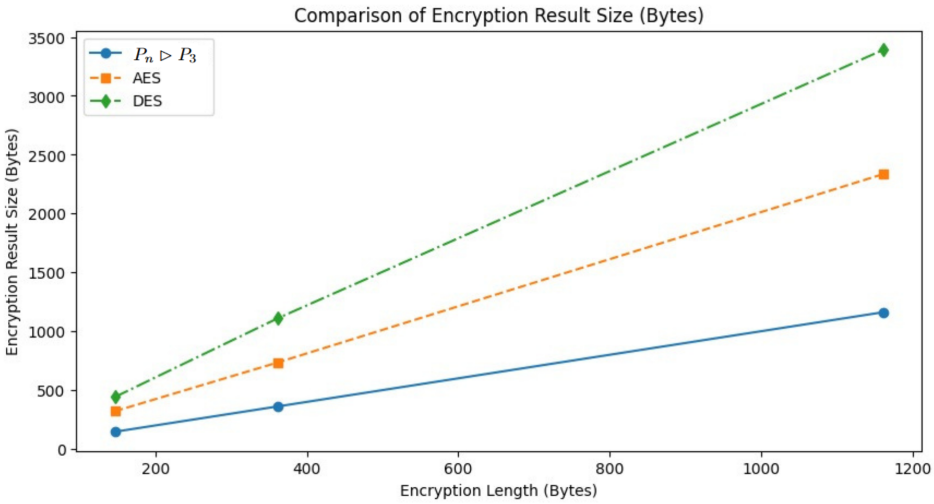

Fig. 3. Comparison of Encryption Result Size (Bytes)

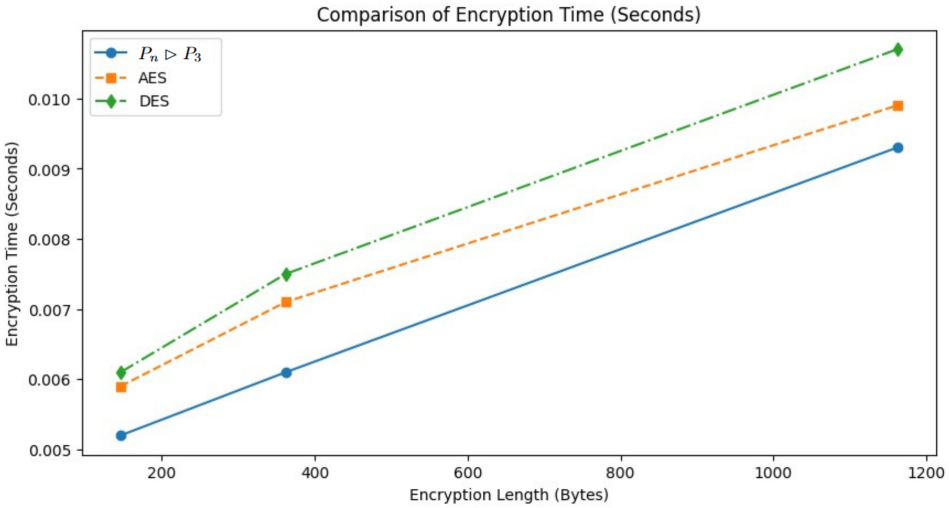

Fig. 4. Comparison of Encryption Time (Seconds)

D. Applying the Modified Robustness Cryptosystem

The next stage is the process of comparing asymmetric cryptography using the one edge irregular reflexive labeling theorem with the AES and DES algorithms. This comparison focuses on performance evaluation based on the processing time required for encryption and decryption. This comparison aims to assess the algorithmic complexity when using 1 edge irregular reflexive labeling theorem, AES, and DES. Algorithmic complexity is categorized into time complexity.

Table IV and Fig. 3 provides a comparison of encryption result sizes in bytes for different encryption types at different data lengths. The data lengths presented are 146 bytes, 362 bytes, and 1162 bytes. The row labeled $(P_n \triangleright P_3)$ shows the original size of *plaintext* before encryption, which corresponds to the data length (146, 362, and 1162 bytes, respectively). When this *plaintext* is encrypted using the AES algorithm, the encrypted size increases to 320 bytes, 736 bytes, and 2336 bytes respectively. In comparison, the DES algorithm produces larger encryption sizes: 441 bytes, 1112 bytes, and 3392 bytes for the same data length. This shows that DES produces larger encrypted data than AES for any given *plaintext* size.

We used various test scenarios with different plaintext sizes to perform the evaluation. This wide range of plaintext sizes allows us to observe the impact of increasing byte length on the encryption process. Table IV shows the encryption size comparison results for the cryptographic algorithms of Theorem 1 edge irregular reflexive labeling, AES, and DES. Based on the table, we know that the size of encryption produced by graph $P_n \triangleright P_3$ is the smallest among AES and DES cryptography. This demonstrates the efficiency of asymmetric cryptography combined with reflexive edge labeling, particularly in reducing storage requirements, making it highly suitable for scenarios where data compression is critical.

Table V compares the encryption time (in seconds) required for different types of encryption on the same data length as in Table IV. For the sizes of *plaintext* 146, 362, and 1162 bytes, the encryption time using the $P_n \triangleright P_3$ method is 0.0052 seconds, 0.0061 seconds, and 0.0093 seconds respectively. When AES is applied, the encryption time is slightly higher, at 0.0059 seconds, 0.0071 seconds, and 0.0099 seconds for the three data lengths. Meanwhile,

TABLE IV
COMPARISON OF ENCRYPTION RESULT SIZE (BYTES)

Encryption Type \ Encryption Length	146 bytes	362 bytes	1162 bytes
$P_n \triangleright P_3$	146	362	1162
AES	320	736	2336
DES	441	1112	3392

DES takes the longest time: 0.0061 seconds, 0.0075 seconds, and 0.0107 seconds. This highlights the advantage of the $P_n \triangleright P_3$ method, which achieves faster encryption performance, making it more suitable for real-time cryptographic applications.

As shown in Table V and Fig. 4, the use of asymmetric cryptography using Theorem 1 edge irregular reflexive labeling proves to be the most effective compared to AES and DES. It not only provides faster and more efficient encryption performance but also maintains the smallest encryption size, a combination that is particularly advantageous for managing large-scale sensitive data like DNA sequences. The ability of this method to reduce computational time and storage requirements underscores its practical value in modern cryptographic systems, especially where real-time processing and resource optimization are critical.

In addition to the results presented in this study, previous research has also explored the integration of graph theory with cryptography to enhance data security mechanisms. For instance, Agustin et al. [29] demonstrated the use of rainbow vertex antimagic coloring in constructing encryption keystreams, highlighting the potential of graph-based approaches in cryptographic applications. Similarly, Prihandoko et al. [28] implemented super H-antimagic total graphs for establishing stream ciphers, showcasing the versatility of graph labeling techniques in securing communication channels. Moreover, Dafik et al. [26] utilized local super antimagic total face coloring in the development of cipher block chaining keys, providing a robust framework for improving encryption methodologies. These studies emphasize the growing relevance of graph-based cryptographic techniques, which align with the contributions of the irregular reflexive edge labeling method proposed in this paper. Collectively, these efforts underline the significance of leveraging graph theory in advancing modern cryptographic systems and addressing critical challenges in data security.

V. CONCLUDING REMARKS

This research introduces a novel approach using irregular edge reflexive k-labeling to generate stronger and more robust keystreams in asymmetric cryptography, especially in protecting DNA sequences in real environments with large scale biological data. The results show that the labeling method used is able to increase the complexity of the keystream, thus strengthening the security of biological data. In addition to making significant contributions to the development of graph labeling theory, these findings also have great potential applications in modern cryptography and bioinformatics. Through this innovative approach, it is expected that the resulting keystream can function effectively in maintaining data security, especially in the context of biotechnology and medicine. Although this approach has shown promising results, several questions still need to be answered for further development.

Open Problem 1: How to optimize irregular edge reflexive k-labeling for other graphs, as well as how this method can be adapted or combined with other labeling techniques to create a more efficient security system. In addition, further research is needed for other cryptography applications beyond DNA sequences.

REFERENCES

[1] E. Farri and P. Ayubi, "A robust digital video watermarking based on CT-SVD domain and chaotic DNA sequences for copyright protection," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 10, pp. 13113–13137, 2023.

[2] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, "Elliptic curve cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey," *Computer Science Review*, vol. 47, pp. 100530, 2023.

[3] M. Merkepci and M. Abobala, "On some novel results about split-complex numbers, the diagonalization problem, and applications to public key asymmetric cryptography," *Journal of Mathematics*, vol. 2023, no. 1, pp. 4481016, 2023.

[4] J. Shetty, G. Sudhakara, and V. Madhusudanan, "Encryption system involving matrix associated with semigraphs," *IAENG International Journal of Applied Mathematics*, vol. 52, no. 2, pp. 458–465, 2022.

[5] S. V. Shree and S. D. Dhanalakshmi, "Information security by employing RSA algorithm and graph labeling," *IAENG International Journal of Applied Mathematics*, vol. 54, no. 12, pp. 2563–2568, 2024.

[6] D. N. H., S. R. Bhat, R. Bhat, and S. G. Bhat, "Some graph based encryption techniques," *IAENG International Journal of Applied Mathematics*, vol. 54, no. 12, pp. 2727–2734, 2024.

[7] S. Wang and J. He, "Design of chaotic systems with multiple scrolls via anti-control method and its encryption application," *IAENG International Journal of Applied Mathematics*, vol. 54, no. 12, pp. 2636–2644, 2024.

[8] G. Chartrand, L. Lesniak, and P. Zhang, "Graphs and digraphs," 6th ed., *Taylor and Francis Group*, Boca Raton, New York, 2016.

[9] J. A. Gallian, "A dynamic survey of graph labeling," *The Electronic Journal of Combinatorics*, vol. 20, no. 1, pp. 1–432, 2017.

[10] G. Chartrand, M. S. Jacobson, J. Lehel, O. R. Oellermann, S. Ruiz, and F. Saba, "Irregular networks," *Congressus Numerantium*, vol. 64, pp. 187–192, 1988.

[11] J. A. Gallian, "A dynamic survey of graph labeling," *The Electronic Journal of Combinatorics*, vol. 1, no. Dynamic Surveys, pp. DS6, 2018.

[12] M. Baca, S. Jendrol', M. Miller, and J. Ryan, "On irregular total labelings," *Discrete Mathematics*, vol. 307, pp. 1378–1388, 2007.

[13] D. Tanna, J. Ryan, and A. Semaničová-Feňovčíková, "Reflexive edge irregular labelling of prisms and wheels," *Australasian Journal of Combinatorics*, vol. 69, pp. 394–401, 2017.

[14] I. H. Agustin, I. Utoyo, D. Dafik, and M. Venkatachalam, "Edge irregular reflexive labeling of some tree graphs," *Journal of Physics: Conference Series*, vol. 1543, pp. 012008, 2020.

[15] I. Tarawneh, R. Hasni, and A. Ahmad, "On the edge irregularity strength of corona product of cycle with isolated vertices," *AKCE International Journal of Graphs and Combinatorics*, vol. 13, pp. 213–217, 2016.

TABLE V
COMPARISON OF ENCRYPTION RESULT SIZE (SECONDS)

Encryption Type \ Encryption Length	146 bytes	362 bytes	1162 bytes
$P_n \triangleright P_3$	0.0052	0.0061	0.0093
AES	0.0059	0.0071	0.0099
DES	0.0061	0.0075	0.0107

[16] M. Bača, M. Irfan, J. Ryan, A. Semaničová-Feňovčíková, and D. Tanna, "On edge irregular reflexive labellings for the generalized friendship graphs," *Mathematics*, vol. 5, no. 67, pp. 1–11, 2017.

[17] D. Tanna, J. Ryan, and A. Semaničová-Feňovčíková, "Edge irregular reflexive labeling of prisms and wheels," *Australasian Journal of Combinatorics*, vol. 69, no. 3, pp. 394–401, 2017.

[18] M. Bača, M. Irfan, J. Ryan, A. Semaničová-Feňovčíková, and D. Tanna, "Note on edge irregular reflexive labelings of graphs," *AKCE International Journal of Graphs and Combinatorics*, vol. 16, pp. 145–157, 2019.

[19] M. Bača, M. Irfan, J. Ryan, A. Semaničová-Feňovčíková, and D. Tanna, "Note on edge irregular reflexive labelings of graphs," *AKCE International Journal of Graphs and Combinatorics*, vol. 16, pp. 145–157, 2019.

[20] X. Zhang, M. Ibrahim, S. A. U. H. Bokhary, and M. K. Siddiqui, "Edge irregular reflexive labeling for the disjoint union of gear graphs and prism graphs," *Mathematics*, vol. 6, pp. 1–10, 2018.

[21] K. K. Yoonga, M. Irfan, I. Taraweh, and A. Ahmad, "On the edge irregular reflexive labeling of corona product of graphs with path," *AKCE International Journal of Graphs and Combinatorics*, vol. 18, pp. 53–59, 2021.

[22] J. L. G. Guirao, S. Ahmad, M. K. Siddiqui, and M. Ibrahim, "Edge irregular reflexive labeling for disjoint union of generalized Petersen graph," *Mathematics*, vol. 6, no. 304, pp. 1–10, 2018.

[23] M. Ibrahim, S. Majeed, and M. K. Siddiqui, "Edge irregular reflexive labeling for star, double star and caterpillar graphs," *TWMS Journal of Applied and Engineering Mathematics*, vol. 10, no. 3, pp. 597–606, 2020.

[24] Y. Ke, M. J. A. Khan, M. Ibrahim, and M. K. Siddiqui, "On edge irregular reflexive labeling for Cartesian product of two graphs," *European Physical Journal Plus*, vol. 136, no. 1, pp. 1–13, 2021.

[25] M. Bača, M. Irfan, J. Ryan, A. Semaničová-Feňovčíková, and D. Tanna, "On edge irregular reflexive labellings for the generalized friendship graphs," *Mathematics*, vol. 5, no. 67, pp. 1–11, 2017.

[26] Dafik, R. Nisviasari, T. K. Maryati, I. H. Agustin, and M. Venkatachalam, "On local super antimagic total face coloring and the application in developing a cipher block chaining key," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 4, pp. 1101–1111, 2021.

[27] R. Nisviasari, Dafik, I. H. Agustin, E. Y. Kurniawati, I. N. Maylisa, and B. J. Septory, "Improving the robustness of the affine cipher by using a rainbow antimagic coloring," *Journal of Physics: Conference Series*, vol. 2157, no. 1, p. 012017, 2022.

[28] A. C. Prihandoko, Dafik, and I. H. Agustin, "Implementation of super H-antimagic total graph on establishing stream cipher," *Indonesian Journal of Combinatorics*, vol. 3, no. 1, pp. 14–23, 2019.

[29] I. H. Agustin, D. Dafik, R. Nisviasari, R. I. Baihaki, E. Y. Kurniawati, S. Kartini, and V. Nagaraja, "On rainbow vertex antimagic coloring and its application to the encryption keystream construction," *Applied Mathematics*, vol. 18, no. 4, pp. 783–794, 2024.

[30] D. Dafik, S. Venkatraman, G. Sathyanarayanan, R. I. Baihaki, I. L. Mursyidah, and I. H. Agustin, "Enhancing text encryption and secret document watermarking through hyperladder graph-based keystream construction on asymmetric cryptography technology," *Statistics, Optimization & Information Computing*, vol. 14, no. 1, pp. 247–263, 2025.

[31] R. Alfarisi, R. M. Prihandini, R. Adawiyah, E. R. Albirri, and I. H. Agustin, "Graceful chromatic number of unicyclic graphs," *Journal of Physics: Conference Series*, vol. 1306, no. 1, p. 012039, 2019.

[32] Dafik, I. H. Agustin, Surahmat, R. Alfarisi, and S. Sy, "On non-isolated resolving number of special graphs and their operations," *Far East Journal of Mathematical Sciences*, vol. 102, no. 10, pp. 2473–2492, 2017.

[33] K. A. Santoso, I. L. Mursyidah, I. H. Agustin, D. Dafik, S. Venkatraman, and M. Venkatachalam, "A robust technique of asymmetric cryptography using rainbow vertex antimagic coloring," *Statistics, Optimization & Information Computing*, vol. 13, no. 5, pp. 1984–1999, 2025.

[34] I. H. Agustin, M. Hasan, R. Adawiyah, R. Alfarisi, and D. A. R. Wardani, "On the locating edge domination number of comb product of graphs," *Journal of Physics: Conference Series*, vol. 1022, no. 1, p. 012003, May 2018.

[35] A. W. Gembong and I. H. Agustin, "Bound of distance domination number of graph and edge comb product graph," *Journal of Physics: Conference Series*, vol. 855, no. 1, p. 012014, June 2017.

Marsidi Marsidi is a lecturer at the Department of Mathematics Education, Faculty of Teacher Training and Education, Universitas PGRI Argopuro Jember, Indonesia. He obtained his S.Si. and M.Si. degrees in mathematics from the Department of Mathematics, Faculty of Mathematics and Science, University of Jember, Indonesia, in 2006 and 2012, respectively. He is currently a postgraduate student in the Department of Postgraduate Mathematics Education, University of Jember, Jember, Indonesia. His main research interest is in graph theory, particularly in graph labeling such as antimagic and reflexive labeling. He has published in various national and international journals and proceedings in both mathematics and mathematics education. He is a member of the Indonesian Mathematical Society (IndoMS).

Dafik Dafik is a professor specializing in combinatorics, graph theory, and combinatorial mathematics education at the University of Jember, where he has held this position since 2013. He earned his doctorate in combinatorics and graph theory from the University of Ballarat, Australia, in 2007. He currently serves as a senior lecturer at both the Department of Postgraduate Mathematics Education and the Department of Postgraduate Mathematics, University of Jember. In addition, he is the chairman of the PUI-PT Center for Combinatorics and Graph at the same university. His research interests encompass graph theory, mathematics education, and applied mathematics. He actively serves as a reviewer for several national and international journals in the field of applied mathematics. Dafik also holds the position of President of the Indonesian Mathematical Society (IndoMS).

Susanto Susanto is a lecturer at the Department of Postgraduate Mathematics Education, University of Jember, Indonesia. He earned his doctorate in mathematics education from Universitas Negeri Surabaya in 2011, after completing his master's degree at Universitas Negeri Malang and his undergraduate degree at Universitas Jember. His research focuses on mathematics education, particularly geometry learning, STEM-based instruction, and the use of digital media in teaching. He has published in several national and international journals and is a member of the Indonesian Mathematical Society (IndoMS).

Arika Indah Kristiana Arika Indah Kristiana is a lecturer in the Department of Postgraduate Mathematics Education, University of Jember, Jember, Indonesia, and an active researcher at the PUI-PT Combinatorics and Graph (CGANT), University of Jember. She earned her bachelor's degree in mathematics from Institut Teknologi Sepuluh Nopember in 2001, her master's degree in mathematics education from Universitas Negeri Malang in 2019, and her doctoral degree in mathematics from Universitas Airlangga in 2021. Her research focuses on graph theory and mathematics education. She has published in several national and international journals and currently serves as the Treasurer of the Indonesian Mathematical Society (IndoMS).

Nelly Oktavia Adiwijaya Nelly Oktavia Adiwijaya is a lecturer in the Department of Informatics, Faculty of Computer Science, University of Jember, Jember, Indonesia. She obtained her bachelor's degree in science from Universitas Jember and her master's degree in engineering from Institut Teknologi Bandung in 2009. Her research interests include data science, machine learning, and image processing, with applications in agriculture and business intelligence. She has published several papers in national and international journals and conference proceedings in the field of informatics.