Information Security by employing RSA Algorithm and Graph Labeling

S. Vani Shree, S. Dhanalakshmi*

***Abstract*—The RSA technique provides security for every user connected across the network. The mathematical factorization problem, which demonstrates how challenging it is to find two prime numbers whose product equals a particular extremely large number, provides the foundation for this theory. In order to have a decent public key cryptosystem, it need really high integers, it can be dealt using RSA technique. In this work we have introduced a Total Edge Bimagic Mean Labeling of Graphs (TEBMML). TEBMML of a graph G is a bijection ψ: $V(G) \rightarrow \{1, 2, 3, \ldots |V|\}$ such that $\psi^*(uv) = \lfloor\frac{\psi(u)+\psi(uv)+\psi(v)}{3}\rfloor$is either k_1 or k_2, a constant for any edge $uv \in E(G)$. A graph is known as Total edge bimagic mean graph if it admits Total edge bimagic mean labeling. Also it is examined that Comb graph, Bistar graph, twig graph and Coconut tree graph are total edge bimagic mean graphs. Along with that information security is determined by exerting RSA algorithm with the above quoted labeling technique.**

***Index Terms*—Total edge bimagic mean labeling, Comb graph, Coconut tree graph, bistar graph, twig graph, encryption, decryption.**

I. Introduction

GRAPH labeling has numerous kinds of applications, including information security. In communication networks, magic labeling has several applications. Vertex, edge and total labeling are identified based on the domain. Graph labeling subject to some conditions results in enormous real life applications which are projected by G.J.Gallian [3]. In 1963, Magic labeling was given by Sedl´aˇcek. Rosa and Kotzig defined magic labeling and explored some results in [1]. Ringel and Llado introduced edge magic labeling which is one of the extensions of magic labeling, and discussed some interesting results in tree conjecture in their work. Edge-magic total labeling, developed by W. D. Wallis, et al. resulted in same labeling for some special graphs. W. D. Wallis enhanced the idea of magic graphs. Data security is a topic that must be handled carefully in order to secure important data, since it offers privacy, integrity, secrecy and authentication. Cryptography is one of the traditional methods for protecting data and it is typically regarded as a key data security component.

In the current circumstances, network security is a complex topic, and several approaches have been developed to ensure safety against attacks. The network connects millions of individuals and it aims to safeguard data and ensure timely delivery to its destination. The network security ensures confidentiality, integrity, access control and authorization. Symmetric and asymmetric key cryptography both use public keys and private keys [12]. Symmetric-key cryptography uses a single public key for encryption and decryption on both sides, making it susceptible to the third-party access. Symmetric-key cryptography includes DES, AES and Blowfish algorithms. Asymmetric key cryptography uses two keys: a public key and a private key. Data is encrypted by the receiver's public key and decrypted by the receiver's private key [2], making it a more secure method of data transmission. RSA and Elliptic Curve algorithms are the types of asymmetric key cryptography.

The RSA algorithm was initially developed in 1978 [10] by R. Rivest, A. Shamir, and L. Adleman. The RSA cryptosystem is based on the stark disparity between how easy it is to locate big primes and how difficult it is to factor the product of two large prime numbers [4]. RSA employs an exponential expression. Each block of the plaintext encryption procedure has a binary value that is less than some integer n. To put it another way, the block size must be smaller than or equal to $log_2(n) + 1$. The algorithm is built on modular exponentiation. The form of encryption and decryption for some plaintext block M and ciphertext block C [11] is as follows. Both the sender and the reciver must be conversant with the value of n. Only the receiver has knowledge of the value of d; the sender knows the value of e, consequently, this is a public-key encryption technique. The public exponent is denoted by the number e, the private exponent by the number d, and the modulus by the number N. The inverses of e and d are multiplicative mod $\phi(n)$. It should be noted that this is only accurate in accordance with the regulations of modular arithmetic if d (and consequently e) is substantially prime to $\phi(n)$. $Gcd(\phi(n), d) = 1$ is equivalent. The following prerequisites need to be fulfilled for this method in order to be suitable for public-key encryption.

- To ensure that M^{ed} (mod n) = M for all $M < n$, values of e, d, and n can be determined.
- It is relatively easy to compute C = M^e (mod n) and C^d (mod n) for all values of $M < n$.
- It is infeasible to determine d given e and n

Asymmetric algorithms are those that employ distinct keys for encryption and decryption. Communications can be encrypted by any individual with the public key, but they can only be decrypted by the holder who owns the private key [5]. In contrast, Anyone with the access to the public key can decode messages encrypted by the person who possesses the secret key. Anyone who is able to successfully decrypt such communications will be certain that only the holder of the secret key is able to encrypt them. It is computationally infeasible to determine the decryption key which gives the knowledge of the cryptographic algorithm [9]. This knowledge serves as the foundation for the digital signa-

Manuscript received December 18, 2023; revised September 8, 2024.

S. Vani Shree is a Research Scholar, Department of Mathematics, SRM Institute of Science and Technology - Ramapuram, Chennai - 600089, India. (e-mail: vs3455@srmist.edu.in)

Dr. S. Dhanalakshmi is an Assistant Professor, Department of Mathematics, Faculty of Engineering and Technology, SRM Institute of Science and Technology - Ramapuram, Chennai - 600089, India. (Corresponding author e-mail: dhanalas1@srmist.edu.in)

ture method. This approach is contemporary by distributing public keys and generating secret keys. The cryptographic RSA algorithm can be used to verify the integrity of digital data [13]. Also it can safeguard data at the row and column level while ensuring its integrity within the user's authority. The RSA technique utilizes the most advanced Asymmetric randomization data algorithm for public key cryptography.

The mean labeling of graph concept was proposed by Somasundaram and Ponraj and it is verified for some graphs [7]. S. Arockiaraj and A. Meenakumari [8] proposed the notion of F-face magic mean labeling. Jayapal Baskar Babujee and Babitha Suresh [6] have investigated Super edge bimagic and construction of edge bimagic total bimagic labeling. New Results on Face Magic Mean Labeling of Graphs [15] have been investigated by S. Vani Shree and S. Dhanalakshmi. Face Bimagic Mean Labeling is introduced by S. Vani Shree and S. Dhanalakshmi [14] and it is verified for Duplication of a Path Graph. Application of edge bimagic mean labeling in data security [16] using slanting ladder graph and latitude graph has been examined by S. Vani Shree and S. Dhanalakshmi. Also, S. Vani Shree et.al have explored the results on face bimagic mean labeling using herschel graph and graph operations [17]. In this work, a graph admits Total edge bimagic mean labeling for graph $P_n \odot K_1$, $n \geq 2$, bistar graph, twig graph and coconut tree graph. Also, it is examined that information security is determined by exerting RSA algorithm and the above quoted labeling technique.

II. PRELIMINARIES

Definition 2.1 Total edge bimagic mean labeling of a graph G (V,E) with V vertices and E edges is a bijection mapping ψ: $V(G) \cup E(G) \to \{1, 2, 3, \ldots |V| + |E|\}$ such that $\psi^*(uv) = \lfloor \frac{\psi(u)+\psi(uv)+\psi(v)}{3} \rfloor$is either k_1 or k_2, for any edge $uv \in E(G)$.

Definition 2.2 By joining a single pendant edge to each vertex of a path *comb graph* is obtained. It is also defined as $P_n \odot K_1$, $n \geq 2$.

Definition 2.3 A Coconut tree graph CT(m,n), $\forall$ positive integer n and $m \geq 2$ is obtained from the path P_m by appending 'n' new pendant edges at an end vertex of P_m.

Definition 2.4 The graph obtained from a path by attaching exactly two pendant edges to each internal vertex of the path is called a Twig Graph.

Definition 2.5 $B_{n,n}$ is the bistar obtained from two disjoint copies of $K_{1,n}$ by joining the centre vertices through an edge. In a bistar there are 2n+2 vertices and 2n+1 edges, altogether there are 4n+3 elements. There are totally 2n pendant vertices and 2 centre vertices. The degree of the pendant vertices are 1 and the degree of the central vertices are n+1 obtained from both the n edges of $K_{1,n}$ and the common edge of the centres.

III. ENCRYPTION AND DECRYPTION TECHNIQUE

A. Key Generation

The following are the key components of the RSA algorithm

- In order for the product n = pq to have its required bit length, two major random primes, p and q, need be generated.
- Calculate n = pq and $\phi(n) = (p-1)(q-1)$
- Choose an integer e, $1 < e < \phi(n) \in gcd$ $(\phi(n), e)$ = 1
- Determine the decryption exponent d, $1 < d < \phi(n)$, so that d = $(e^{-1} mod(\phi(n)))$
- The private key is (d, p, q) while the public key is (n, e). All of the d, p, q, and ϕ variables should be kept private.
- The modulus is denoted by n.
- The public exponent or encryption exponent is denoted by e.
- The secret exponent or decryption exponent is denoted by d.

B. Working Rule

The structure of encryption and decryption is as follows, by taking some plaintext block M and cipher text block C into consideration.
C = $M^e(mod(n))$
M = $C^d(mod(n))$
M^e (mod n) and C^d (mod n) are extremely trivial to calculate for all values of $M < n$.
It is infeasible to determine d given e and n.

- Select two distinctive prime numbers, p and q.
- Let n = pq and $\phi(n) = (p-1)(q-1)$
- Select an integer e such that $1 < e < \phi(pq)$, and GCD (e, $\phi(pq)$) = 1, e and $\phi(pq)$ are coprime.
- Find d where d= e^{-1} (mod$\phi(n)$)

Using a formula, the message M is encrypted, and the encrypted message is C. The encrypted message is decrypted using an algorithm.

Note: The RSA Algorithm perception is employed, and Core Java has been carried out for the examination process.

IV. MAIN RESULTS

Theorem 4.1: Comb graph $P_n \odot K_1$, $n \geq 2$ admits total edge bimagic mean labeling.

Proof: Let G(V,E) be a comb graph $P_n \odot K_1$,$n \geq 2$ has $2n$ vertices and $2n - 1$ edges. Let the vertex set be V, where $V = \{u_r, v_r : 1 \leq r \leq n\}$ and $E = \{u_r v_r : 1 \leq r \leq n\} \cup \{u_r u_{r+1} : 1 \leq l \leq n-1\}$.
Define a mapping $\psi : V(G) \cup E(G) \to \{1, 2, 3, ...4n-1\}$ as follows,

$$\psi(u_r) = r; 1 \leq r \leq n$$
$$\psi(v_r) = 3n - r; 1 \leq r \leq 2n-1; r \equiv 1(mod\ 2)$$
$$\psi(u_r v_r) = 3n + r - l; 1 \leq r \leq n$$
$$\psi(u_r u_{r+1}) = 3n - 2r; 1 \leq r \leq n-1$$

Hence, the Total Edge Bimagic Mean constants in G is obtained as,
$$\psi^*(u_r u_{r+1}) = \lfloor \frac{3n+1}{3} \rfloor \ \ or\ n$$
$$\psi^*(u_r v_r) = \lfloor \frac{6n}{3} \rfloor \ \ or\ 2n$$

■

A. Functioning of Encryption and Decryption process

Input: The original text P H I L O S O P H Y and the comb graph
Output: The encrypted numeric string is 71 63 08 72 14 44 14 71 63 33

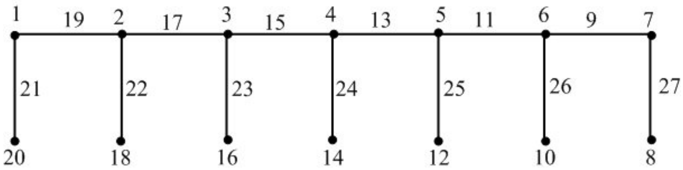

Fig. 1: TEBMML of $P_7 \odot K_1$

Encrypt: C = M^e (mod n)

1) From the graph $P_n \odot K_1$, let the two prime numbers be bimagic constant k_1 and number of edges.
   $p = 7$, $q = 13$,
   where $n = pq = 7(13) = 91$
2) $\phi(n) = (p-1)(q-1) = (6)(12) = 72$
   $e = 1 < e < \phi(n) = 1 < e < 72$
   $gcd(\phi(n), e) = 1$
   $gcd(72, 5) = 1$
   e = 5,
   d = $(e^{-1} mod \phi(n))$
   d = $(5^{-1}(mod 72))$
   5×x = 1 (mod 72)
   5 × 29 = 1 (mod 72)
   d=29
3) The plain text P H I L O S O P H Y is replaced with its corresponding ordinal number – 15 07 08 11 14 18 14 15 07 24. Let the ordinal numbers in the resulting sequence to be P in a text is convert each text into a numeric value using a linear system.
   C = M^e (mod (n))
   For Example M = 15,
   C = 15^5 (mod 91)
   C = 71
   By solving the aforementioned equations,
   The solution C= 71 is obtained.
4) Convert the other text in the similar form, yields the numeric string-71 63 08 72 14 44 14 71 63 33 which is the encrypted values.

   Decrypt: M = C^d (mod n)
5) $M = 71^{29}$ (mod 91) $\implies M = 15$
   By solving the obtained solution is M = 15
   The sequence M was derived in a similar manner for the sequence with regard to C. The obtained numeric string is 15 07 08 11 14 18 14 15 07 24
   As a result the corresponding plain text is – P H I L O S O P H Y.

Theorem 4.2: Coconut tree graph $CT(m, n)$, $m, n \geq 2$ admits total edge bimagic mean labeling.

Proof: Let G(V,E) be a Coconut tree graph $CT(m, n)$, $m, n \geq 2$ has $n + m$ vertices and $n + m - 1$ edges. Let the vertex set be V, where $V = \{u_r : 1 \leq r \leq n\} \cup \{v_r : 1 \leq r \leq m\}$ and $E = \{u_r v_n, u_r u_{r+1} : 1 \leq r \leq n-1\}$.
Define a mapping $\psi : V(G) \cup E(G) \to \{1, 2, 3, ...2n+2m-1\}$ as follows,
Case (i): n is odd and $m \geq 2$
$\psi(u_r) = r; 1 \leq r \leq m$
$\psi(v_{2r}) = n + m - r + 1; 1 \leq r \leq n-2$
$\psi(v_{2r-1}) = \frac{n+2m-r+2}{2}; 1 \leq r \leq n-1$
$\psi(v_r v_{r+1}) = n + m + r; 1 \leq r \leq n-1$
$\psi(u_r v_n) = 2n + 2m - r; 1 \leq r \leq m$
Hence, the Total Edge Bimagic Mean constants in G is obtained as,
$\psi^*(u_r v_r) = \lfloor \frac{1}{3}(3m + 2n + 1) \rfloor$
$\psi^*(v_r v_{r+1}) = \lfloor \frac{1}{3}(\frac{6m+5n+3}{2}) \rfloor$
Case (ii): n is even and $m \geq 2$
$\psi(u_r) = r; 1 \leq r \leq m$
$\psi(v_{2r}) = \frac{n+m+r+3}{2}; 1 \leq r \leq n-2; r \equiv 1(mod\ 2)$
$\psi(v_{2r-1}) = n + m + r - 4; 1 \leq r \leq n-2$
$\psi(v_r v_{r+1}) = 2n + m - r; 1 \leq r \leq n-1$
$\psi(u_r v_n) = 2n + 2m - r; 1 \leq r \leq m$
Hence, the Total Edge Bimagic Mean constants in G is obtained as,
$\psi^*(u_r v_r) = \lfloor m + n \rfloor$
$\psi^*(v_r v_{r+1}) = \lfloor m + n - 1 \rfloor$

■

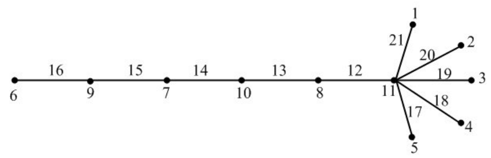

Fig. 2: Edge Bimagic Mean Labeling of Ln_4

B. Functioning of Encryption and Decryption process

Input: The original text P H I L O S O P H Y and the coconut tree graph
Output: The encrypted numeric string is 115 06 57 132 53 138 53 115 06 106

Encrypt: C = M^e (mod n)

1) From the graph $CT(m, n)$, let the two prime numbers be bimagic constant k_1 and number of vertices. $p = 11$, $q = 13$
   $n = pq = 11(13) = 143$
2) $\phi(n) = (p-1)(q-1) = (10)(12) = 120$
   $e = 1 < e < \phi(n) = 1 < e < 120$
   $gcd(\phi(n), e) = 1$
   $gcd(120, 7) = 1$
   e = 7
   d = $(e^{-1} mod \phi(n))$
   d = $(7^{-1}(mod 120))$
   7×x = 1 (mod 120)
   7 × 103 = 1 (mod 120)
   d=103
3) The plain text P H I L O S O P H Y is replaced with its corresponding ordinal number – 15 07 08 11 14 18 14 15 07 24. Let the ordinal numbers in the resulting sequence to be P in a text is convert each text into a numeric value using a linear system.
   C = M^e (mod (n))
   For Example M = 15,
   C = 15^7 (mod 143)
   C = 115

By solving the aforementioned equations,
The solution C=115 is obtained.

4) Convert the other text in the similar form, yields the numeric string-115 06 57 132 53 138 53 115 06 106 which is the encrypted values.

Decrypt: M = C^d (mod n)

5) $M = 115^{103}$ (mod 143) $\implies M = 15$
By solving the obtained solution is
M=15
The sequence M was derived in a similar manner for the sequence with regard to C. The obtained numeric string is 15 07 08 11 14 18 14 15 07 24
As a result the corresponding plain text is – P H I L O S O P H Y.

Theorem 4.3: Twig graph G admits total edge bimagic mean labeling.

Proof: Let G(V,E) be a twig graph T_m is formed from a path graph P_n, with m internal vertices has 3m+1 edges and 3m+2 vertices. Let the vertex set be V, where $V = \{u_r; 1 \leq r \leq n\} \cup \{v_r, w_r : 1 \leq r \leq n-2\}$ and the edge set be E, where $E = \{u_r u_{r+1} : 1 \leq r \leq n-1\} \cup \{u_{r+1}v_r, u_{r+1}w_r : 1 \leq r \leq n-2\}$
Consider a mapping $\psi : V(G) \cup E(G) \rightarrow \{1, 2, 3, ..., 6m+3\}$ as follows,

$$\psi(u_{2r-1}) = n-2+r; \begin{cases} 1 \leq r \leq \frac{n+1}{2}, when\ n\ is\ odd \\ 1 \leq r \leq \frac{n}{2}, when\ n\ is\ even \end{cases}$$

$$\psi(u_{2r}) = n+1+r; \begin{cases} 1 \leq r \leq \frac{n-1}{2}, when\ n\ is\ odd \\ 1 \leq r \leq \frac{n}{2}, when\ n\ is\ even \end{cases}$$

$$\psi(v_{2r-1}) = r; 1 \leq r \leq \frac{n+1}{2}$$

$\psi(v_{r+1}) = \frac{n+r}{2}; 1 \leq r \leq \frac{n-1}{2} for\ (r \equiv 1\ (mod\ 2))$: for odd value of n

$\psi(v_{2r}) = \frac{n-2}{2} + r; 1 \leq r \leq \frac{n}{2} - 1$: for even values of n

$$\psi(w_{2r-1}) = 2n-2+r; 1 \leq r \leq \frac{n-1}{2}$$

$$\psi(w_{2r}) = 2n+r; \begin{cases} 1 \leq r \leq \frac{n-1}{2} - 1, when\ n\ is\ odd \\ 1 \leq r \leq \frac{n}{2} - 1, when\ n\ is\ even \end{cases}$$

$$\psi(u_r u_{r+1}) = 5n-r-6; 1 \leq r \leq n-1$$

$$\psi(u_{r+1}v_r) = 6n-r-8; 1 \leq r \leq n-2$$

$$\psi(u_{r+1}w_r) = 4n-r-5; 1 \leq r \leq n-2$$

Hence, the Total Edge Bimagic Mean constants in G is obtained in two cases,
When n is odd

$\psi^*(u_r u_{r+1}) = \lfloor \frac{5n-7}{2} \rfloor$

$\psi^*(u_{r+1}v_r) = \lfloor \frac{5n-7}{2} \rfloor$

$\psi^*(u_{r+1}w_r) = \lfloor \frac{5n-7}{2} \rfloor\ and\ \lfloor \frac{5(n-1)}{2} \rfloor$

When n is even $\psi^*(u_r u_{r+1}) = \lfloor \frac{5n-8}{2} \rfloor$

$\psi^*(u_{r+1}v_r) = \lfloor \frac{5n-8}{2} \rfloor$

$\psi^*(u_{r+1}w_r) = \lfloor \frac{5n-8}{2} \rfloor\ and\ \lfloor \frac{5n-6}{2} \rfloor$

■

C. *Functioning of Encryption and Decryption process*

Input: The original text P H I L O S O P H Y and the coconut tree graph
Output: The encrypted numeric string is 78 49 50 121 105 37 105 78 49 47

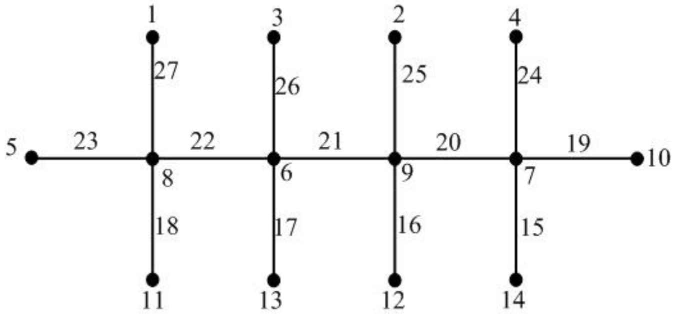

Fig. 3: Edge Bimagic Mean Labeling of T_4 formed from P_6

Encrypt: C = M^e (mod n)

1) From the graph T_m is formed from a path graph P_n, let the two prime numbers be bimagic constant k_1 and number of vertices. $p = 7$, $q = 19$
$n = pq = 7(19) = 133$
2) $\phi(n) = (p-1)(q-1) = (10)(12) = 108$
$e = 1 < e < \phi(n) = 1 < e < 108$
$gcd(\phi(n), e) = 1$
$gcd(108, 5) = 1$
e = 5
d = $(e^{-1} mod \phi(n))$
d = $(5^{-1}(mod\ 108))$
5×x = 1 (mod 108)
5 × 65 = 1 (mod 108)
d¯ 65
3) The plain text P H I L O S O P H Y is replaced with its corresponding ordinal number – 15 07 08 11 14 18 14 15 07 24. Let the ordinal numbers in the resulting sequence to be P in a text is convert each text into a numeric value using a linear system.
C = M^e (mod (n))
For Example M = 15,
C = 15^5 (mod 133)
C = 78
By solving the aforementioned equations,
The solution C = 78 is obtained.
4) Convert the other text in the similar form, yields the numeric string-78 49 50 121 105 37 105 78 49 47 which is the encrypted values.

Decrypt: M = C^d (mod n)

5) $M = 78^{65}$ (mod 133) $\implies M = 15$
By solving the obtained solution is
M=15
The sequence M was derived in a similar manner for the sequence with regard to C. The obtained numeric string is 15 07 08 11 14 18 14 15 07 24
As a result the corresponding plain text is – P H I L O S O P H Y.

Theorem 4.4: Bistar graph B_n,$n \geq 2$ admits total edge bimagic mean labeling.

Proof: Let G(V,E) be a bistar graph $B_{n,n}$,$n \geq 2$, with 2n+1 edges and 2n+2 vertices. Let the vertex set be V, where $V = \{u_r, v_r : 1 \leq r \leq n\} \cup \{u, v\}$ and the edge set be E, where $E = \{u_r y_1, v_r y_2 : 1 \leq r \leq n\} \cup \{uv\}$
Consider a mapping $\psi : V(G) \cup E(G) \rightarrow \{1, 2, 3, ..., 4n+3\}$

as follows,

$\psi(u_r) = 2r; 1 \leq r \leq n$

$\psi(v_r) = 2r - 1; 1 \leq r \leq 2n - 1$

$\psi(u) = n + 3$

$\psi(v) = n + 4$

$\psi(uu_r) = 4n - 2r + 4; 1 \leq r \leq n$

$\psi(vv_r) = 4n - 2r + 5; 1 \leq r \leq n$

$\psi(uv) = 2n + 3$

Hence, the Total Edge Bimagic Mean constants in G is obtained as,

$\psi^*(uu_r) = \left\lfloor \frac{6n+5}{3} \right\rfloor = \lfloor 2n + 1 \rfloor$

$\psi^*(vv_r) = \left\lfloor \frac{6n+6}{3} \right\rfloor = \lfloor 2n + 2 \rfloor$

$\psi^*(uv) = \left\lfloor \frac{6n+5}{3} \right\rfloor = \lfloor 2n + 1 \rfloor$

■

Remark: In order to process with RSA algorithm, it requires two different prime numbers whereas bistar graph produces a same set of prime number and hence the result of above theorem does not support the specified encryption process.

Flow chart of encryption process and decryption process for RSA Algorithm using graph labeling

The following figure represents the structural outline of encryption and decryption process for comb graph, coconut tree graph and twig graph.

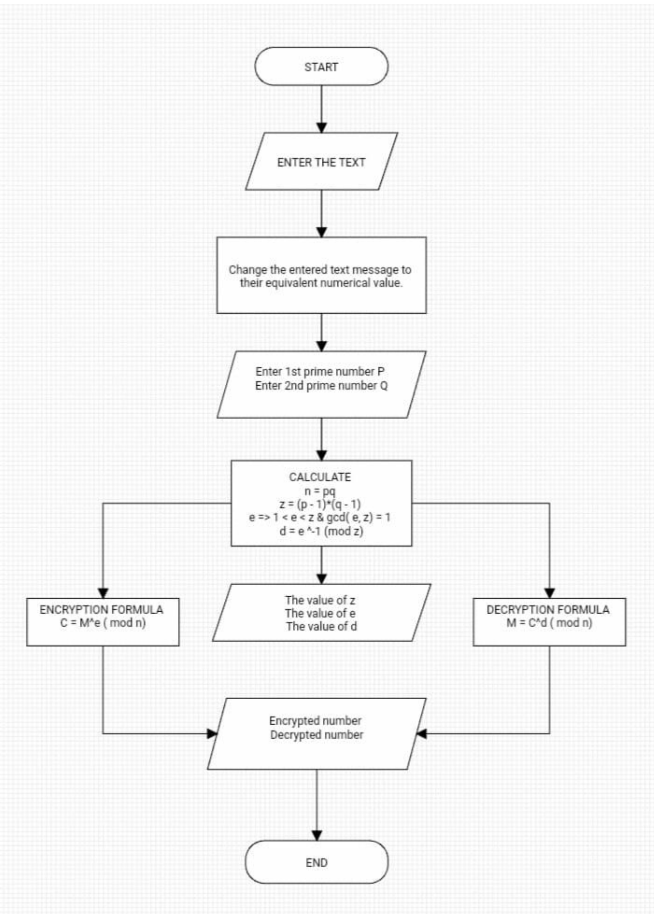

Fig. 4: Flow Chart - encryption and decryption process for $P_n \odot K_1$, $CT(m, n)$ and T_m is formed from a path graph P_n.

Images of some Java programmes

```
import java.util.*;
import java.math.*;

public class test {
  public static void main(String[] args) {

    int p,q,n,z,e,d=0,i,a,b=0,val;
    char ch;
    double c ;

     System.out.println("Enter text :");
     Scanner sc = new Scanner (System.in);
     String str = sc.nextLine();


     System.out.println("Enter 1st prime number p");
     p=sc.nextInt();
     System.out.println("Enter 2nd prime number q");
     q=sc.nextInt();

     n=p*q;
     z=(p-1)*(q-1);
     System.out.println("the value of z = "+z);

     for(e=2;e<z;e++)
     {
        if(gcd(e,z)==1)
        {
           break;
        }
     }
```

```

      c=(Math.pow(b,e))%n;
      val= (int)c;
     System.out.print(val+ " ");
     gt [i] = c;
     }
     System.out.println();

  System.out.println("Decrypted number is : -");
      for (double dc : gt){
      BigInteger N = BigInteger.valueOf(n);


     BigInteger C = BigDecimal.valueOf(dc).toBigInteger();
    BigInteger msgback = (C.pow(d)).mod(N);
 System.out.print(msgback + " ");

      }

  }
  static int gcd(int e, int z)
  {
     if(e==0)
        return z;
     else
        return gcd(z%e,e);
  }
}
```

V. Conclusion

This study introduces and discusses the concept of total edge bimagic mean labeling for comb graph, bistar graph, twig graph, and coconut tree graph. Also, Encryption and decryption processes of a text are analyzed by implementing RSA algorithm and the above quoted graph labeling. In future, it will be interesting for the researchers to study various graphs and investigate the applications of this labeling.

References

[1] A. Kotzig and A. Rosa, ”Magic valuations of finite graphs”, Canad. Math. Bull. 13(4), (1970), 451-461.
[2] Thomas Koshy, ”Elementary Number Theory with Applications”, Second Edition , Academic Press, (2002).
[3] Gallian, J. A. ”A dynamic survey of graph labeling”. *Electronic Journal of Combinatorics*, 1(DynamicSurveys), (2022), Article #DS6.
[4] William Stallings,“Cryptography and Network Security Principles and Practices”, Fourth Edition, Prentice Hall.
[5] Douglas R. Stinson , Maura B. Paterson, “Cryptography theory and practices”, fourth edition, CRC press,Taylor & franchise group.
[6] Jayapal Baskar Babujee, Babitha Suresh, “New Constructions of Edge Bimagic Graphs from Magic Graphs”, *Applied Mathematics*, (2011), 2, 1393-1396, doi:10.4236/am.2011.211197.
[7] A. Meena Kumari and S. Arockiaraj, “On (1,0,0)-F-Face magic mean labeling of some graphs”, *International Conference on Applied and Computational Mathematics*, IOP Conf. Series: Journal of Physics: Conf. Series 1139 (2018) 012049, doi:10.1088/1742-6596/1139/1/012049.
[8] A. Meena Kumari and S. Arockiaraj, “Further results on F-Face magic mean graphs”, *International Journal of Advanced Science and Technology*, Vol. 29, No. 7s, (2020), pp.1129-1138.
[9] Christof Paar • Jan Pelzl, “Understanding Cryptography”, Springer Heidelberg Dordrecht London New York, DOI 10.1007/978-3-642-04101-3.
[10] Jean-Philippe Aumasson,”SERIOUS CRYPTOGRAPHY A Practical Introduction to Modern Encryption”, William Pollock, (2018) ,No Starch Press, Inc.
[11] M. Preetha, M. Nithya, “A study and performance analysis of rsa algorithm”, *International Journal of Computer Science and Mobile Computing*, IJCSMC, Vol. 2, Issue. 6, June 2013, pg.126 – 139.
[12] Abhishek, Dr.Vandana,“A Study on Modified RSA Algorithm in Network Security”, *International Research Journal of Modernization in Engineering Technology and Science*, Vol (4)(1),2022.
[13] Hengki Tamando Sihotang, Syahril Efendi, “Design and Implementation of Rivest Shamir Adleman’s (RSA) Cryptography Algorithm in Text File Data Security”,*Journal of Physics: Conference Series*,1641,2020 doi:10.1088/1742-6596/1641/1/012042.
[14] S. Vani Shree, S. Dhanalakshmi, “On Face Bimagic Mean Labeling of Duplication of a Path Graph”, *Telematique*, Volume 21 Issue 1, 2022 ISSN: 1856-4194 3262 - 3267.
[15] S. Vani Shree, S. Dhanalakshmi, “New Results on Face Magic Mean Labeling of Graphs”, *Mathematics and Statistics* 11(1): 199-205, 2023 DOI: 10.13189/ms.2023.110123.
[16] S. Vani Shree, S. Dhanalakshmi, “Application of Edge Bimagic Mean Labeling in Data Security”, *Asia Pacific Journal of Mathematics* Volume 10 (2023),41, ISSN: 2357-2205, doi:10.28924/APJM/10-41.
[17] S.Vani Shree, S.Dhanalakshmi, “Face Bimagic Mean Labeling of Herschel Graphs and Its Operations”. *Contemp. Math*,Vol(5)(1),2024, PP-209-221.