ENCRYPTING NUMBERS USING PAIR LABELING IN PATH GRAPHS

J. Baskar Babujee¹, V. Vishnupriya^{2§}

¹Department of Mathematics
Anna Universtiy
Chennai, 600 025, INDIA

²Department of Mathematics
SASTRA University
Thanjavur, 613401, INDIA

²SRM University
Ramapuram Campus, Chennai, 600 089, INDIA

Abstract: Encryption today has grown into such specialized field that involve mathematical, non-linear cryptosystem that even a relatively powerful computers take months or even years to break the cipher text. Now a day's most of the fields say clients' credit card numbers, social security numbers, tax file numbers etc needs to be kept secret when they send it electronically. There are various methods used to encrypt the numbers. It has been recognized that encryption and decryption mostly emerges from mathematical disciplines. In this paper, we give a new combinatorial technique to encrypt and decrypt numbers through labeled graphs using the residue modulo class Z_3 .

AMS Subject Classification: 94A60, 05C78

Key Words: algorithms, encryption, decryption, digraphs, magic, labeling

1. Introduction

The concept of graph labeling was introduced by Rosa in 1967 [4]. A graph

Received: November 11, 2016

Revised: February 23, 2017

Published: May 6, 2017

© 2017 Academic Publications, Ltd.

url: www.acadpubl.eu

[§]Correspondence author

labeling is an assignment of integers to the vertices or edges or both, subject to certain conditions. Labeled graphs serve as useful models for a broad range of applications such as coding theory, X-ray crystallography, radar, astronomy, circuit design, communication network addressing and database management. Detail survey of graph labeling can be seen in A dynamic survey of graph labeling by J.A. Gallian [3].

A graph $G(p, q)$ is said to be $(1, 1)$ edge magic with the common edge count k_0 if there exists a bijection $f : V(G) \cup E(G) \rightarrow \{1, 2, \dots, p + q\}$ such that $f(u) + f(v) + f(e) = k_0$ for all $e = (u, v) \in E(G)$. It is said to be $(1, 1)$ edge antimagic if $f(u) + f(v) + f(e)$ are distinct for all $e = (u, v) \in E(G)$. A labeling of the type $(1, 1, 1)$ assign labels from the set $\{1, 2, \dots, p + q + r\}$ to the vertices, edges and faces of a planar graph G in such a way that each vertex, edge and face receives exactly one label and each number is used exactly once as a label. A Labeling of type $(1, 0, 0)$ and $(0, 1, 0)$ is a bijection from the set $\{1, 2, \dots, p + q\}$ to the vertices and edges of a graph G .

The weight of a face under a label is the sum of labels carried by that face and edges and vertices on its boundary. A labeling is said to be face magic, if for every numbers, all s side faces have equal weight. Variations of magic and antimagic graphs are studied from [7, 8].

Definition 1.1. [6] Duplication of an edge $e = v_i v_{i+1}$ by a new vertex v in a graph G produces a new graph G such that $N(v) = \{v_i, v_{i+1}\}$.

Definition 1.2. [6] Duplication of a vertex v_k by a new edge $e = v v$ in a graph G produces a new graph G such that the neighborhood of v and v are respectively $N(v) = \{v_k, v\}$ and $N(v) = \{v_k, v\}$.

Theorem 1.1. Let G be a graph obtained from the path P_n by duplication of all the vertex by edge. Then G admits $(1, 0, 0)$ face antimagic labeling.

Proof. Let $u_1, u_2, \dots, u_n$ be the vertices and $\{u_i u_{i+1}; 1 \leq i \leq n - 1\}$ be the edges of the path P_n . Let the graph G obtained by duplicating all the vertices in path P_n . The graph G has p vertices, q edges and r faces. Then the vertex set $V = \{u_i, v_i, w_i; 1 \leq i \leq n\}$ and the edge set $E = E_1 \cup E_2 \cup E_3 \cup E_4$, where

$$E_1 = \{u_i u_{i+1}; 1 \leq i \leq n - 1\}, \quad E_2 = \{u_i v_i; 1 \leq i \leq n\},$$

$$E_3 = \{v_i w_i; 1 \leq i \leq n\}, \quad E_4 = \{u_i w_i; 1 \leq i \leq n\}.$$

We define a bijective function $f : V(G) \rightarrow \{1, 2, \dots, 3n\}$ as follows:

For any vertex $f(u_i) = i; 1 \leq i \leq n; f(v_i) = 2n + i; 1 \leq i \leq n; f(w_i) = 2n + 1 - i; 1 \leq i \leq n$

Now we calculate face weight as $\lambda(F_i) = f(u_i) + f(v_i) + f(w_i) = i + 2n + i + 2n + 1 - i = 4n + 1 + i$; $1 \leq i \leq n$ which forms an arithmetic progression with $\{(4n + 2), (4n + 2) + d, \dots, (4n + 2) + (r - 1)d\}$ and all the values are distinct. Hence G admits $(1, 0, 0)$ face antimagic labeling.

Let $G(p, q, r)$ be a graph obtained from path P_n by duplication of all the vertices by an edge. We have $3n$ vertices and $4n - 1$ edges where vertex set $V = \{v_i\}_{i=1}^{3n}$ and edge set $E = \{v_i v_{i+1}\}_{i=1}^{n-1} \cup \{v_i v_{n+i}, v_i v_{2n+i}, v_{n+i} v_{2n+i}\}_{i=1}^n$ and the faces as $\{v_i v_{n+i} v_{2n+i}\}_{i=1}^n = F_i$. Let $\{1, 2, \dots, n\}$ be the labels of the vertices of P_n . We get the graph G with labels $\{n + 1, n + 2, \dots, 3n\}$ of the vertices and $\{3n + 1, \dots, 7n - 1\}$ the labels of edges. We calculate face weight as follows $\lambda(F_i) = f(u_i) + f(v_i) + f(w_i) + f(u_i v_i) + f(v_i w_i) + f(u_i w_i)$ $\square$

We give the following example for vertex by edge duplication of path P_5 that admits $(1, 1, 0)$ face antimagic labeling with distinct weights $\{101, 102, 103, 104, 105\}$.

Figure 1: $(1, 1, 0)$ face antimagic labeling of vertex duplication of path P_5

In [2] J. Baskar Babujee and S. Babitha has introduced pair labeling in graphs to encrypt and decrypt numbers using Number Theory technique in complete graph k_9 . In this paper we use the same technique of encryption of numbers over the vertex by edge duplication of path P_n .

2. Main Results

2.1. The Proposed Cryptosystem

Graphs can be effectively used for the encryption. We take vertex by edge duplication of the graph P_n , where $n \equiv 0 \pmod{3}$. To make our encryption complicated we adopt the following steps:

1. Partition the number into three parts using modulo class of Z_3 .
2. Take a path P_n with the vertex v_i from $1 \leq i \leq n$, where $n \equiv 0 \pmod{3}$. Construct a vertex by edge duplication for P_n . Now the new graph G has $3n$ vertices, $4n - 1$ edges and n faces. The faces are triangles i.e., C_3 cycles.
3. The labels of the vertex of G is an ordered pair $[\alpha, i]$, $1 \leq i \leq 3n$ and that for edges are $[\beta, j]$, where the first component of an ordered pair $[\alpha, i]$ and $[\beta, j]$ will be labeling number obtained by using residue class of Z_3 . The second component of pair $[\alpha, i]$ and $[\beta, j]$ will be the number $\{1, 2, \dots, 7n - 1\}$.
4. G is made $(1, 0, 0)$ face and orientation is given for all its edges.
5. Assign edge magic labeling for the three edges of exactly one face C_3 and make all other edges in G as $(1, 1)$ edge antimagic.

2.2. Algorithm for Encryption

Input: The secret number N , the number of vertices of path P_n , $[n \equiv 0 \pmod{3}]$ and the magic constant K .

Output: Encrypted labeled digraph G .

begin

Step 1: Define the graph G obtained from the path P_n by duplication of all the vertices by edges, $n \equiv 0 \pmod{3}$ with vertex set $V = V_1 \cup V_2 \cup V_3$ where $V_1 = \{v_i; 1 \leq i \leq n\}$; $V_2 = \{v_i; n + 1 \leq i \leq 2n\}$; $V_3 = \{v_i; 2n + 1 \leq i \leq 3n\}$ and edge set are defined as

$E = E_1 \cup E_2 \cup E_3 \cup E_4$ where

$E_1 = \{v_i v_{i+1}; 1 \leq i \leq n - 1\}$, $E_2 = \{v_i v_{n+i}; 1 \leq i \leq n\}$

$E_3 = \{v_i v_{2n+i}; 1 \leq i \leq n\}$, $E_4 = \{v_{n+i} v_{2n+i}; 1 \leq i \leq n\}$ and the faces as $F = \{v_i v_{n+i} v_{2n+i}\}_{i=1}^n$.

Step 2: The vertex labeling of V is given by the bijective function $f : V \rightarrow [\alpha, i]$, $\alpha \in \{0, 1, 2\}$, $1 \leq i \leq n$ defined as

$$f(v_i) = \begin{cases} [(i - 1) \bmod 3, i] & \text{for } 1 \leq i \leq n \\ [(i + 1) \bmod 3, i] & \text{for } n + 1 \leq i \leq 2n \\ [i \bmod 3, i] & \text{for } 2n + 1 \leq i \leq 3n \end{cases}$$

Step 3: If $N \equiv 0 \pmod{3}$ goto step 4 else goto step 5.

Step 4: Split N as $N = \sum_{i=0}^2 N_i$ such that $N_i \equiv i \pmod{3}$ for $i = 0, 1, 2$ and

$N_i > 3$. Create a uni directed magic cycle C_3 be taking $v_p \in v_1$, $v_q \in v_2$ and $v_r \in v_3$ and $E = \{\overrightarrow{v_p v_r}, \overrightarrow{v_r v_q}, \overrightarrow{v_q v_p}\}$. Assign the labels for the edges of C_3 as follows

$$f(\overrightarrow{v_p v_r}) = \left[\left\lfloor \frac{N_1}{3} \right\rfloor, K - (p + r) \right];$$

$$f(\overrightarrow{v_r v_q}) = \left[\left\lfloor \frac{N_2}{3} \right\rfloor, K - (q + r) \right];$$

$$f(\overrightarrow{v_q v_p}) = \left[\left\lfloor \frac{N_3}{3} \right\rfloor, K - (p + q) \right];$$

Go to step 6.

Step 5: Split N as $N = \sum_{i=0}^2 N_i$ such that any two of N_i has same residue value

over Z_3 and $N_i > 3$. Create a directed cycle C_3 , by taking $v_p \in V_1$, $v_q \in V_2$ and $v_r \in V_3$ which does not have uni-direction but depends upon the residue value of N_i for $i = 0, 1, 2$. The orientation of this cycle C_3 will be $\{\overrightarrow{v_p v_q}, \overrightarrow{v_p v_r}, \overrightarrow{v_q v_r}\}$. Assign the labels for the edges C_3 as follows. If two of the N_i (say N_a, N_b) have residue value 0 when it is divisible by 3, then

$$f(\overrightarrow{v_q v_p}) = \left[\left\lfloor \frac{N_a}{3} \right\rfloor, K - (p + q) \right];$$

$$f(\overrightarrow{v_p v_r}) = \left[\left\lfloor \frac{N_b}{3} \right\rfloor, K - (p + r) \right];$$

Step 6: Let $E = E - E_1$. The orientation of E is defined as,

$$v_i v_j = \begin{cases} \overrightarrow{v_i v_j} & \text{if } i + j \equiv 0 \pmod{2} \\ \overrightarrow{v_j v_i} & \text{otherwise} \end{cases}$$

Step 7: Edge labeling of E is given by the bijective function

$$f : E \rightarrow \left\{ [\beta, j], \beta \in \left\{ 0, \left\lfloor \frac{N_i}{3} \right\rfloor; i = 0, 1, 2 \right\} \right\}$$

and $3n + 1 \leq j \leq 7n - 1$ defined as follows, $E = E \cup E_1$. Labeling of E_1 is given in Step 4 and Step 5. Now we have to define the function of the set E . The first component of edge labeling (i.e.,) β value given as follows.

If $i \pmod{3} = (i - 1) \pmod{3}$ then

$$f(\overrightarrow{v_i v_{i+1}}) = [0, j] \text{ for } v_i v_{i+1} \in E_1$$

$$\text{else } f(\overrightarrow{v_i v_j}) = \begin{cases} \left[\left\lfloor \frac{N_0}{3} \right\rfloor, j \right] & \text{if } n + 1 \leq j \leq 2n \in E_3 \\ \left[\left\lfloor \frac{N_1}{3} \right\rfloor, \gamma \right] & \text{if } 2n + 1 \leq j \leq 3n \in E_3 \\ \left[\left\lfloor \frac{N_2}{3} \right\rfloor, \gamma \right] & \text{if } n + 1 \leq j \leq 2n \in E_4 \end{cases}$$

The second component of the edge labeling j value given in Step 8.

Step 8: We assign the j value by ignoring the orientation of edges in E .

Let $S = \{3n + 1, 3n + 2, \dots, 4n - 1\} - \{f(\overrightarrow{v_i v_j}); f(\overrightarrow{v_i v_j}) \in E_1\}$

- (i) Store the elements of S in a array of size $(4n - 1) - 3$.
- (ii) Start with $a[0]$, assign labels to the edges $f(\overrightarrow{v_i v_j})$ consecutively by ignoring the orientation of $1 \leq i, j \leq n$ in E .
- (iii) Do the process until the array will be empty.

Step 9: Except one cycle $C_3(v_p, v_q, v_r)$ all the cycles receive $(1, 1)$ edge antimagic labeling is obtained for the digraph by duplication of vertex by edge of P_n , where $n \equiv 0 \pmod{3}$.

end.

2.3. Rigor of the Encryption and Decryption Algorithm with Illustration

Consider the graph P_n where $n \equiv 0 \pmod{3}$. Obtain the graph G by the vertex duplication of the path P_n . The vertex set $V = V_1 \cup V_2 \cup V_3$ where $V_1 = \{v_i; 1 \leq i \leq n\}$; $V_2 = \{v_i; n + 1 \leq i \leq 2n\}$; $V_3 = \{v_i; 2n + 1 \leq i \leq 3n\}$ and edge set are defined as

$E = E_1 \cup E_2 \cup E_3 \cup E_4$ where

$E_1 = \{v_i v_{i+1}; 1 \leq i \leq n - 1\}$, $E_2 = \{v_i v_{n+i}; 1 \leq i \leq n\}$

$E_3 = \{v_i v_{2n+i}; 1 \leq i \leq n\}$, $E_4 = \{v_{n+i} v_{2n+i}; 1 \leq i \leq n\}$.

Each vertex of G is labeled as $[\alpha, i]$ where α takes the values of residue class of Z^3 (i.e.,) 0, 1 and 2 repeatedly to all the vertices of graph G and i takes the values of $\{1, 2, \dots, 3n\}$. The given number N is split into three numbers in such a way that each number N_i ; $0 \leq i \leq 2$ should be greater than 3 and $N_i \equiv i \pmod{3}$. If the given number N is divisible by 3 then each partition number N_i ; $0 \leq i \leq 2$ will give residues [0], [1] and [2] respectively when it is divisible by 3. If the number N is not divisible by 3 then also it split into three but two of the partition number N_i ; $0 \leq i \leq 2$ will give some residue value when it is divisible by 3. Each edge of G is labeled as $[\beta, j]$. Consider any one of the cycle C_3 with vertex $v_p \in v_1$; $v_q \in v_2$ and $v_r \in v_3$ whose vertex labels are $[0, p]$, $[1, q]$ and $[2, r]$ respectively. The orientation of this $C_3\{\overrightarrow{v_p v_r}, \overrightarrow{v_r v_q}, \overrightarrow{v_q v_p}\}$ in unidirectional when N is divisible by 3 and directed cycle C_3 when N is not divisible by 3. Next we define edge label $[\beta, j]$ of the cycle C_3 is as follows. First we define β value then define the j value of the cycle C_3 . Consider the

number N which is going to be encrypted. Here N_i be the partition number which has residue value α when it is divisible by 3, then the number $\beta = \left\lfloor \frac{N_i}{3} \right\rfloor$ is placed to any one of the edges which is incident to the vertices having the label α and the direction of edge will be towards the same vertex having label α . Label j value to the edges as $f(\overrightarrow{v_p v_q}) = k - (p + q)$; $f(\overrightarrow{v_q v_r}) = k - (q + r)$; $f(\overrightarrow{v_r v_p}) = k - (r + p)$. The orientation of all edges is given as, for $i < j$,

$$v_i v_j = \begin{cases} \overrightarrow{v_i v_j} & \text{if } i + j \equiv 0 \pmod{2} \\ \overrightarrow{v_j v_i} & \text{otherwise} \end{cases}.$$

The edge labeling $[\beta, j]$ for remaining edges other than the cycle C_3 is given as follows: For β value, the numbers N_i ; $0 \leq i \leq 2$ be the partition numbers which has residue value α when it is divisible by 3, then the number $\beta = \left\lfloor \frac{N_i}{3} \right\rfloor$ is placed to the edges which is incident to the vertex having the label α . For j value, ignoring the orientation of the remaining edges other than the cycle C_3 . Let $S = \{3n + 1, 3n + 2, \dots, 7n - 1\} - \{f(\overrightarrow{v_i v_j}); \overrightarrow{v_i v_j} \in E_1\}$. The remaining $(4n - 1) - 3$ edges labeled using the set of elements of S . There are many ways to place the j values to the edges without forming magic cycle C_3 . First we write the numbers in the set S in ascending order. Starting with the first element of S , store the elements in the edges $f(v_i v_j)$ for $1 \leq i, j \leq n$ in E consecutively by ignoring the orientation. Continue this until the set S will be empty. i.e., until all the edges will be labeled. Finally we get the encrypted digraph.

2.3.1. Illustration-1

The secret number to be encrypted is 360 which is divisible by 3.

Encryption: Given secrete number $N = 360$. This secret number can be encrypted as follows:

Since $n = 9$, we have n faces i.e., 9 triangles and let total magic constant $k = 71$.

- The vertex set and edge set are as defined earlier.
- Each vertex of graph G is labeled as $[\alpha, i]$ where α takes the values of residue class Z_3 (i.e.,) 0, 1 and 2 repeatedly to all the vertices by edge duplication of path P_n i.e., G and i takes the values of $\{1, 2, \dots, 3n\}$. Each edge of G is labeled as $[\beta, j]$.
- Given number can be partitioned as

$$N = 360 = N_0 + N_1 + N_2 = 90^{(0)} + 172^{(1)} + 98^{(2)}$$
- Consider the cycle $C_3 \{v_4 v_{22} v_{13}\}$ with vertex label $[0, 4]$, $[1, 22]$ and $[2,$

13] respectively and the orientation of this C_3 be $\overrightarrow{v_4v_{22}}$, $\overrightarrow{v_{22}v_{13}}$, $\overrightarrow{v_{13}v_4}$ unidirectional. Now for every $v_4, v_{22}, v_{13} \in V$ in C_3 , $f(v_4) = [0, 4]$, $f(v_{22}) = [1, 22]$, $f(v_{13}) = [2, 13]$ and also $f(\overrightarrow{v_4v_{22}}) = [57, 45]$; $f(\overrightarrow{v_{22}v_{13}}) = [32, 36]$; $f(\overrightarrow{v_{13}v_4}) = [30, 54]$.

- Here $E_1 = \{\overrightarrow{v_4v_{22}}, \overrightarrow{v_{22}v_{13}}, \overrightarrow{v_{13}v_4}\}$ and $E = E - E_1$ then $E = E \cup E_1$.
- Now

$$f : E \rightarrow \left\{ [\beta, j]; 10 \leq j \leq 62 \text{ and } \beta \in \left\{ 0, \left\lfloor \frac{N_i}{3} \right\rfloor; i = 0, 1, 2 \right\} \right\}$$

as follows. Here $E = E \cup E_1$. For the set E_1 , $f(\overrightarrow{v_i v_j})$ is given as above. Now we define the function f for the set E using the step 7 of encryption algorithm. For β value, if $i \pmod 3 = (i - 1) \pmod 3$ then

$$f(\overrightarrow{v_i v_{i+1}}) = [0, j] \text{ else } f(\overrightarrow{v_i v_j}) = \begin{cases} [57, j] & \text{for } 1 \leq i \leq n \\ [32, j] & \text{for } 2n + i \leq i \leq 3n \\ [30, j] & \text{for } n + i \leq i \leq 2n \end{cases}$$

- Next we calculate the j value by ignoring the orientation of edges in E . Let $S = \{28, 29, \dots, 62\} - \{36, 45, 54\}$. Store the elements of S in an array of size $4n - 1$. Start with $a[0] = 28$ remove the element from S and place to the first edge $f(v_i v_j)$, $1 \leq i \leq n - 1$, $2 \leq j \leq n$ then $f(v_i v_{n+i})$; $1 \leq i \leq n$; $f(v_i v_{2n+i})$, $1 \leq i \leq n$ and $f(v_{n+i} v_{2n+i})$, $1 \leq i \leq n$ in E consecutively.
- Start with 28 and label the edges of E_1 in the set $S - \{28, 29, \dots, 35\}$. Then for edges of E_2 from 37 by remaining numbers and continue the process until S will be empty.

Figure 2: Encrypted directed labeled graph for G -vertex by edge duplication of P_9

Decryption: Find the cycle C_3 having total edge magic from the labeled digraph G using dummy labeling of vertices and edges say be values in the pair $[a, b]$. For further decryption we only consider this C_3 and original labeling of vertices and edges of C_3 . For each edge $f(\overrightarrow{v_i v_j})$ of C_3 , we have to calculate $(3 \times f(\overrightarrow{v_i v_j}) + f(v_j))$. Then for the secrete number we have to sum these values for all the three edges of C_3 .

Consider the encrypted labeled graph G with key value as total edge magic triangle.

Figure 3: Edge magic cycle C_3

$$N = \Sigma(3 \times f(\overrightarrow{v_i v_j}) + f(v_j))$$

for all $v_i v_j \in E(C_3)$;

$$= [(3 \times 57) + 1] + [(3 \times 32) + 2] + [(3 \times 30) + 0] = 360.$$

If the given number N is divisible by 3 then labeled cycle C_3 is unidirectional. Otherwise it is directed cycle C_3 . Next we give example for the number which is not divisible by 3.

2.3.2. Illustration-2

Consider the number 721 which is not divisible by 3. Using the above algorithm we can encrypt the given number 721 which is not divisible by 3. Let $K = 71$. $N = 721 = 105^{(0)} + 31^{(1)} + 104^{(0)} = N_a + N_b + N_c$ with N_a and N_c have same residue value 0 when it is divided by 3 and N_b has residue value 1 when it is divided by 3. Then for the cycle $C_3 \{v_4 v_{22} v_{13}\}$, $f(\overrightarrow{v_{22} v_4}) = [105, 45]$; $f(\overrightarrow{v_{13} v_4}) = [104, 54]$; $f(\overrightarrow{v_{13} v_{22}}) = [31, 36]$.

$$N = \Sigma(3 \times f(\overrightarrow{v_i v_j}) + f(v_j)),$$

for all $v_i v_j \in E(C_3)$;

$$= [(3 \times 105) + 0] + [(3 \times 31) + 1] + [(3 \times 104) + 0] = 721.$$

Figure 4: Encrypted labeled for directed graph G -vertex by edge duplication of P_9

Figure 5: Edge magic cycle C_3

3. Conclusion

We have exhibited face antimagic labeling for duplication of all the vertices by edge in path graph. By using pair labeling technique we have done encrypted numbers using number theory as a tool. In future we have planned to work in encryption and decryption of numbers which leads to several application of graph labeling.

References

- [1] J. Baskar Babujee, On graph coding, The Mathematics Education, Volume, XXIX, No. 3, September 2005.
- [2] J. Baskar Babujee and S. Babitha, Encrypting and Decrypting Number using Labeled Graphs, European Journal of Scientific Research, Vol. 75, No. 1, pp. 14–24, 2012.
- [3] J.A. Gallian, A dynamic survey of graph labeling, The Electronic Journal of Combinatorics (2013), #DS6.
- [4] Rosa, On certain valuations of vertices of a graph, Theory of Graphs Internet Symposium, Rome, Gordon and Breach, NY (1967), Dunod, Paris, July 1966, pp. 349–355.
- [5] S.G. Telang, Number Theory, Tata McGraw - Hill Publishing Company Limited, 1996.

- [6] S.K. Vaidhya and C.M. Barasara, Product cordial graphs in the context of some graph operations, *International Journal of Mathematics and Scientific Computing*, 1(2) (2011).
- [7] V. Yegnanarayanan, On magic graphs, *Utilitas Math.*, 59 (2001), 181–204.
- [8] W.D. Wallis, *Magic graphs*, Birkhauser (2001).