International Journal of Engineering & Technology, 7 (4.10) (2018) 806-809

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Encrypting Numbers through Square Grid Graphs

L. Shobana*

Department of Mathematics
SRM Institute of Science and Technology
Kattankulathur– 603 203, India.
**Corresponding author E-mail: shobana.l@ktr.srmuniv.ac.in*

Abstract

Cryptography emphasizes the mathematics behind the theory of public key cryptosystems and digital signature schemes. Encryption is essential for ensured and trusted delivery of sensitive information whereas the decryption is the process of decoding the data which has been encrypted in to a secret format. An authorized user can only decrypt data since decryption requires a secret key or password. There are several methods to encrypt the numbers. In this paper, a combinatorial technique to encrypt and decrypt numbers through labeled strong face of a square grid graph using residue class of Z_3 has been investigated.

Keywords: *encryption: decryption; digraph;, magic; labeling.*

1. Introduction

Most graph labeling methods trace their origin to one introduced by Rosa in 1967. Assignment of integers to the vertices or edges or both, subject to certain conditions is known as Graph labeling. Numerous types of labeling have been investigated in by (Gallian, J.A, 2017). It plays a vital role in the main stream of Mathematics because of its application in diverse fields which includes Bio-chemistry in genomics, Computer Science in algorithms, Operation Research in scheduling and so on. J. Baskar Babujee introduced encryption of numbers through labeled graphs applying the fundamental theorem of arithmetic (Baskar Babujee, 2005). In [2] the concept of pair labeling to encrypt and decrypt numbers using combinatorial technique was proposed by Baskar Babujee. A strong face graph G^* is obtained from G by adding a new vertex to every face of G except the external face and joining this vertex with all vertices surrounding that face, so that all faces of the graph G^* are isomorphic to the cycle C_3. (Mohammed Ali Ahmed & Baskar Babujee, 2017).
In this paper, a combinatorial technique to encrypt and decrypt numbers through labeled strong face of a square grid graph using residue class of Z_3 has been investigated.

2. Graph Labeling Technique

Among the various types of labeling investigated (Gallian, J.A, 2017), one such labeling is the total edge magic labeling. A graph G(m, n) with p vertices and q edges is known to be total edge magic with each edge count r if there exists a bijection f: $V \cup E \rightarrow \{1, 2, \ldots, m+n\}$ such that for each edge $uv \in E$, $f(u) + f(v) + f(uv) = r$. The total edge magic labeling is slightly modified and introduce magic cycle C_3 which plays important role in encryption and decryption of a given number.
Let G be a strong face of a square grid graph P_nXP_n where $n\equiv0$ (mod 3). Consider a bijective mapping f: $VUE\rightarrow\{1,2,\ldots,8n^2-12n+5\}$ with $(2n^2-2n+1)$ vertices, $(6n^2-10n+4)$ edges and $(4n^2-8n+4)$ cycles of length three. A magic cycle C_3 is fixed for which all the three edges have common edge count k.

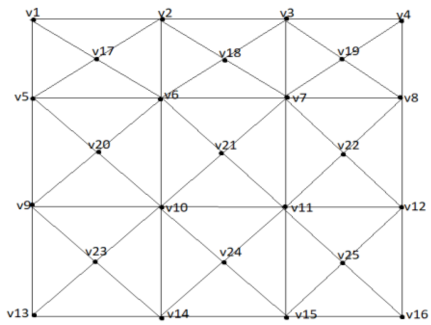

Fig.1: Strong face of a square grid graph P_4XP_4

3. The Planned Cryptosystem

There are various methods to encrypt and decrypt the given data. One of the most interesting and effective method to encrypt the data is by graphical representation. To encrypt a given number Nm, consider the strong face of a square grid graph P_nxP_n where $n\geq3$ and $n\equiv0$ mod 3, on which the concept of total edge magic labeling is applied. The following steps are to be followed to make our encryption complicated:
1. Split the number Nm in to three parts using modulo class of Z_3.
2. Let $V=\{v_i;1\leq i\leq n^2\}$ be the vertex set of a square grid graph. Applying the concept of strong face to the square grid graph, the newly obtained graph G, has $(2n^2-2n+1)$ vertices, $(6n^2-10n+4)$ edges and $4(n^2-2n+1)$ faces where the faces are triangles.
3. Consider k to be a fixed magic constant which is used as a key of our encryption. This constant k is the value of the fixed triangle

(Cycle C_3) where all the three sides of the triangle receive the same constant.
4. The vertices and edges of G are labeled as [x,t], $1 \le t \le 2n^2-2n+1$ and [y,s], where the labels of x and y are residue class of Z_3 and, t and s are labeled from $\{1,2,3,4,\ldots,8n^2-12n+5\}$.
5. Consider the orientation for all the edges of G.
6. Fix one cycle C_3 to be total edge magic labeling.

4. Bounds For The Magic Count

Let $\{1,2,3,\ldots,n^2,n^2+1,\ldots,2n^2-2n+1\}$ and $\{2n^2-2n+2,2n^2-2n+3,\ldots,8n^2-12n+5\}$ are the labels of the vertices and edges of a strong face of a square grid graph P_nxP_n, $n\geq3$ respectively. By the definition of total edge magic,

$$f(u)+f(uv)+f(v)=k \text{ for all } uv \in E. \qquad (1)$$

Case i: when $n\equiv0 \bmod 3$; $n\equiv 1 \bmod 2$
Suppose consider a total edge magic cycle C_3 with large labels of vertices say $2n^2-2n+1>2n-1>3n-1$ and $k=4n^2-n+1$. Consider the edges from cycles C_3 with end vertices having labels $2n^2-2n+1$ and $3n-1$, then (1) becomes $(2n^2-2n+1)+f(uv)=4n^2-n+1$ which implies $f(uv)=2n^2-2n+1$ which is a contradiction to the fact that $f(uv) \in \{2n^2-2n+2,\ldots,8n^2-12n+5\}$ for all $uv \in E$. Hence

$$k > 4n^2-n+1. \qquad (2)$$

Similarly, consider a total edge magic cycle C_3 with smaller labels of the vertices say $1<n+1<n^2+1$ and $k=8n^2-13n+8$. Consider the edges from cycles C_3 with end vertices having labels 1 and n+1, then (1) becomes $1+f(uv)+n+1=8n^2-13n+8$ which implies $f(uv)=8n^2-12n+6$ which is a contradiction to the fact the $f(uv) \in$

$$\{2n^2-2n+2,\ldots,8n^2-12n+5\}. \text{ Hence } k < 8n^2-13n+8. \qquad (3)$$

From equations (2) and (3) the bounds for k is given by $4n^2-n+2 \le k \le 8n^2-13n+7$. This common edge count k which is a magic constant is going to play a vital role as a key value of our cryptosystem which lies between $4n^2-n+2 \le k \le 8n^2-13n+7$.
Case ii: when $n\equiv0 \bmod 3$; $n\equiv 0 \bmod 2$
Suppose consider a total magic cycle C_3 with large labels of the vertices say $2n^2-2n+1>n^2-1>n^2$ and $k=5n^2-4n+2$, and smaller labels of the vertices say $1<2<n^2+1$ and $k=8n^2-12n+9$, then with the similar argument as mentioned above, the bounds for k as follows: $5n^2-4n+2 < k < 8n^2-12n+9$.

5. Algorithm For Encryption

Input: The secret number Nm is greater than or equal to 12, a strong face of a square grid graph P_nXP_n, where n is divisible by 3 and k.

Output: Labeled encrypted G.

Step 1: Fix the strong face of a square grid graph G with vertex set $V = V_1 \cup V_2 \cup V_3$ where $V_1=\{v_i:i\equiv1 \bmod 3\}$, $V_2=\{v_i:i\equiv2 \bmod 3\}$ and $V_3=\{v_i:i\equiv0 \bmod 3\}$ for $1\le i\le 2n^2-n+1$. The edge set is defined as
$E=\{E_i^{(1)};1\le i\le n\}\cup\{E_i^{(2)};1\le i\le n-1\}\cup\{E_i^{(3)};1\le i\le n-1\}\cup \{E_i^{(4)};1\le i\le n-1\}\cup\{E_i^{(5)};1\le i\le n-1\}\cup\{E_i^{(6)};1\le i\le n-1\}$ where

$E_1^{(1)}=\{v_iv_{i+1}; 1\le i\le n-1\}$	$E_1^{(2)}=\{v_iv_{i+n}; 1\le i\le n\}$	$E_1^{(3)}=\{v_iv_{n^2+i}; 1\le i\le n-1\}$
$E_2^{(1)}=\{v_iv_{i+1}; n+1\le i\le 2n-1\}$	$E_2^{(2)}=\{v_iv_{i+n}; n+1\le i\le 2n\}$	$E_2^{(3)}=\{v_iv_{n^2+i-1}; n+1\le i\le 2n-1\}$
$E_3^{(1)}=\{v_iv_{i+1}; 2n+1\le i\le 3n-1\}$	$E_3^{(2)}=\{v_iv_{i+n}; 2n+1\le i\le 3n\}$	$E_3^{(3)}=\{v_iv_{n^2+i-2}; 2n+1\le i\le 3n-1\}$
$E_n^{(1)}=\{v_iv_{i+1}; n^2-n+1\le i\le n^2-1\}$	$E_{n-1}^{(2)}=\{v_iv_{i+n}; n^2-2n+1\le i\le n^2-n\}$	$E_{n-1}^{(3)}=\{v_iv_{n^2-n+2+i}; n^2-2n+1\le i\le n2-n-1\}$

Step 2: Consider a bijective function $f : V \to [x, t]$, $x\in \{0,1,2\}$; $1 \le t \le 2n^2-n+1\}$ defined as $f(v_t)=[t-1 \bmod 3,t]$; $1\le t\le 2n^2-n+1$.

Step 3: when Nm is divisible by 3, proceed to step 4 otherwise move to step 5.

Step 4: Partition $Nm=\sum_{i=0}^{2} Nm_i$ in such a way Nm_i is congruent to I modulo 3 where i = 0, 1, 2 and $Nm_i > 3$, distinct. Create a unidirected magic cycle C_3 be taking $v_x \in V_1$, $v_y \in V_2$ and $v_z \in V_3$ and $E'=\{\overrightarrow{v_xv_y},\overrightarrow{v_yv_z},\overrightarrow{v_zv_x}\}$. Label the edges of C_3 as
$f(\overrightarrow{v_xv_y})=\left[\left\lfloor\frac{Nm_1}{3}\right\rfloor,k-(x+y)\right]$; $f(\overrightarrow{v_yv_z})=\left[\left\lfloor\frac{Nm_2}{3}\right\rfloor,k-(y+z)\right]$;
$f(\overrightarrow{v_zv_x})=\left[\left\lfloor\frac{Nm_0}{3}\right\rfloor,k-(z+x)\right]$.

$$f(\overrightarrow{v_zv_x})=\left[\left\lfloor\frac{Nm_0}{3}\right\rfloor,k-(z+x)\right].$$

Go to step 6.
Step 5: Split Nm as $Nm=\sum_{i=0}^{2} Nm_i$ in such a manner any two of Nm_i has same value over Z_3 and Nm_i is greater than 3. Create a directed cycle C_3, by taking $v_x \in V_1$, $v_y \in V_2$ and $v_z \in V_3$ which does not have uni -direction but depends upon the residue value of Nm_i for i = 0, 1, 2. The orientation of this cycle C_3 will be one of the following: $\{\overrightarrow{v_yv_x},\overrightarrow{v_zv_y},\overrightarrow{v_zv_x}\}$ $\{\overrightarrow{v_yv_x},\overrightarrow{v_yv_z},\overrightarrow{v_zv_x}\}$ $\{\overrightarrow{v_xv_y},\overrightarrow{v_zv_y},\overrightarrow{v_zv_x}\}$ $\{\overrightarrow{v_xv_y},\overrightarrow{v_zv_y},\overrightarrow{v_xv_z}\}$ $\{\overrightarrow{v_xv_y},\overrightarrow{v_yv_z},\overrightarrow{v_xv_z}\}$ $\{\overrightarrow{v_yv_x},\overrightarrow{v_yv_z},\overrightarrow{v_xv_z}\}$. Assign the labels for the edges of C_3 as follows:
If two of the Nm_i (say Nm_a, Nm_b) have residue value 0 when it is divisible by 3, then
$f(\overrightarrow{v_yv_x})=\left[\left\lfloor\frac{Nm_a}{3}\right\rfloor,k-(y+x)\right]$; $f(\overrightarrow{v_zv_x})=\left[\left\lfloor\frac{Nm_b}{3}\right\rfloor,k-(z+x)\right]$ and if Nm_c have residue 1 and 2 when it is divisible by 3, $f(\overrightarrow{v_zv_y})=\left[\left\lfloor\frac{Nm_c}{3}\right\rfloor,k-(z+y)\right]$ and $f(\overrightarrow{v_yv_z})=\left[\left\lfloor\frac{Nm_c}{3}\right\rfloor,k-(y+z)\right]$ respectively.

If two of the Nm_i (say Nm_a, Nm_b) have residue value 1 when it is divisible by 3,
then $f(\overrightarrow{v_xv_y})=\left[\left\lfloor\frac{Nm_a}{3}\right\rfloor,k-(x+y)\right]$; $f(\overrightarrow{v_zv_y})=\left[\left\lfloor\frac{Nm_b}{3}\right\rfloor,k-(z+y)\right]$ and if Nm_c have residue 0 and 2 when it is divisible by 3,
$f(\overrightarrow{v_zv_x})=\left[\left\lfloor\frac{Nm_c}{3}\right\rfloor,k-(z+x)\right]$ and $f(\overrightarrow{v_xv_z})=\left[\left\lfloor\frac{Nm_c}{3}\right\rfloor,k-(x+z)\right]$ respectively.
If two of the Nm_i (say Nm_a, Nm_b) have residue value 2 when it is divisible by 3, then
$f(\overrightarrow{v_xv_z})=\left[\left\lfloor\frac{Nm_a}{3}\right\rfloor,k-(x+z)\right]$; $f(\overrightarrow{v_yv_z})=\left[\left\lfloor\frac{Nm_b}{3}\right\rfloor,k-(y+z)\right]$ and if Nm_c have residue 0 and 1 when it is divisible by 3,
$f(\overrightarrow{v_yv_x})=\left[\left\lfloor\frac{Nm_c}{3}\right\rfloor,k-(y+x)\right]$ and $f(\overrightarrow{v_xv_y})=\left[\left\lfloor\frac{Nm_c}{3}\right\rfloor,k-(x+y)\right]$ respectively.
Goto step 6.

Step 6: Let $E^{**}=E - E^*$. The direction of edges in E^{**} is defined as, for i<j

$$v_iv_j=\begin{cases}\overrightarrow{v_iv_j} & \text{if } i+j\equiv0 \pmod 2\\ \overrightarrow{v_jv_i} & \text{otherwise}\end{cases}$$

Step 7: Consider a bijective function

$$f: E \to \left\{[p,q];\ p \in \left\lfloor \frac{Nm_i}{3} \right\rfloor : i = 0,1,2 \quad and \quad 2n^2 - 2n + 2 \le q \le 8n^2 - 12n + 5\right\}$$

defined as E=E*∪E**. The labeling pattern of E* is defined in step 4 and step 5. Now define the function f for the set E''. The first component of edge labeling p value is as follows. If

$i(\mathrm{mod}\,3) = j(\mathrm{mod}\,3)$ then $f(\overrightarrow{v_i v_j}) = [0,q]$ else

$$f(\overrightarrow{v_i v_j}) = \begin{cases} \left[\left\lfloor \frac{Nm_0}{3} \right\rfloor, q\right] & \text{if } v_j \in V_1 \\ \left[\left\lfloor \frac{Nm_1}{3} \right\rfloor, q\right] & \text{if } v_j \in V_2 \\ \left[\left\lfloor \frac{Nm_2}{3} \right\rfloor, q\right] & \text{if } v_j \in V_3 \end{cases}$$

The second component of q value is defined in step 8.

Step 8: Fix q value by avoiding the direction of one edges in E**. Let

$S = \{2n^2 - 2n + 2, \ldots, 8n^2 - 12n + 5\} - \{f(\overrightarrow{v_i v_j}) : \overrightarrow{v_i v_j} \in E'\}$

i) The elements of S are stored in an array of size $8n^2$-12n+2.

ii) Start with a[0], each time remove the 9th element of array in a circular manner and assign to the edge $f(\overrightarrow{v_i v_j})$ by ignoring the orientation for $1 \le i,j \le 2n^2-2n+1$ in E''.

iii) Do the process until the array is emptied.

Step 9: The labeled directed graph of a strong face of a square grid graph $P_n x P_n$; n≡0 mod 3 is obtained.

6. Algorithm For Decryption

Input: The labeled strong face of a square grid graph with key as total edge magic cycle C_3.
Output: The Secret number Nm.
Step 1: Find the cycles C_3 having total edge magic labeling from the labeled directed graph G by dummy labeling of vertices and edges say b value in [a,b].
Step 2: Each $f(\overrightarrow{v_i v_j})$ of cycle C_3 is calculated from the formula

$(3 * f(\overrightarrow{v_i v_j}) + f(v_j))$ for all $\overrightarrow{v_i v_j} \in E(C_3)$.

Step 3: The Secret number Nm, is the sum of the values of all the three edges C_3 i.e.

$$N = \sum_{ij \in E(C_3)} ((3 * f(\overrightarrow{v_i v_j}) + f(v_j)) \text{ for all } \overrightarrow{v_i v_j} \in E(C_3).$$

7. Rigor of the Encryption and Decryption Algorithm

7.1 Encryption

Consider a strong face of a square grid graph $P_n X P_n$ where n≡0 mod 3. The vertex and edge set of G is defined in step 1 and step 2 of section 5 [Algorithm for encryption]. Each vertex of G is labeled as [l,i] where l takes the values of residue class of Z_3 and i takes the values of {1,2,…,$2n^2$-2n+1}.The given number Nm greater than or equal to 12 is split in to Nm_0, Nm_1 and Nm_2 which should be greater than 3 and Nm_i is congruent to i modulo 3 and distinct. When Nm is congruent to 0 modulo 3 then Nm_0, Nm_1 and Nm_2 will give [0], [1] and [2] respectively. When Nm is not congruent to 0 modulo 3 then again split in to three in which two Nm_i will give same residue when divided by 3. The edges of G are labeled as [p,q]. Consider any one of the cycle C_3 with vertex $v_x \epsilon V_1$, $v_y \epsilon V_2$ and $v_z \epsilon V_3$ whose vertex labels are [0, x], [1, y] and [2,z] respectively. The direction of this cycle C_3 $\{\overrightarrow{v_x v_y}, \overrightarrow{v_y v_z}, \overrightarrow{v_z v_x}\}$ is unidirectional if Nm is congruent to 0 modulo 3 and directed cycle C_3 if Nm is not congruent to 0 modulo 3.

Define the edge labeling [p,q] of the cycle C_3 as follows: define p value followed by defining q value of the cycle C_3. Consider the number Nm which is going to be encrypted. Here Nm_i has residue value l when it is congruent to 0 modulo 3,then $p = \left\lfloor \frac{Nm_i}{3} \right\rfloor$ is located in any of the edges which is incident to the vertex with label a and direction of the edge will be towards the same vertex having the label a. Now q will be calculated using the magic constant k. Let q value to the edges as

$f(\overrightarrow{v_x v_y}) = \left[\left\lfloor \frac{Nm_1}{3} \right\rfloor, k - (x+y)\right]$; $f(\overrightarrow{v_y v_z}) = \left[\left\lfloor \frac{Nm_2}{3} \right\rfloor, k - (y+z)\right]$;

$f(\overrightarrow{v_z v_x}) = \left[\left\lfloor \frac{Nm_0}{3} \right\rfloor, k - (z+x)\right]$.

The orientation of remaining edges except for the unidirectional cycle C_3 is clearly defined in step 6, step 7 and step 8 of section 5[Algorithm for Encryption].

7.2 Decryption

Consider the unidirectional cycle C_3 having total edge magic and the original labeling of vertices and edges of C_3. For each edge $f(\overrightarrow{v_i v_j})$ of C_3, calculate $(3 * f(\overrightarrow{v_i v_j}) + f(v_j))$ then the sum of the values of all three edges of C_3 leads to a secret number Nm.

Example: The secret number to be encrypted is 369 which is divisible by 3 and let total magic constant for unidirectional cycle C_3 is 174.

Given number can be partitioned as Nm=369 =Nm_0+Nm_1+Nm_2= 123 +91 +155. Let k=174. The encrypted labeled directed graph of a strong face of a square grid graph $P_6 X P_6$, is as follows.

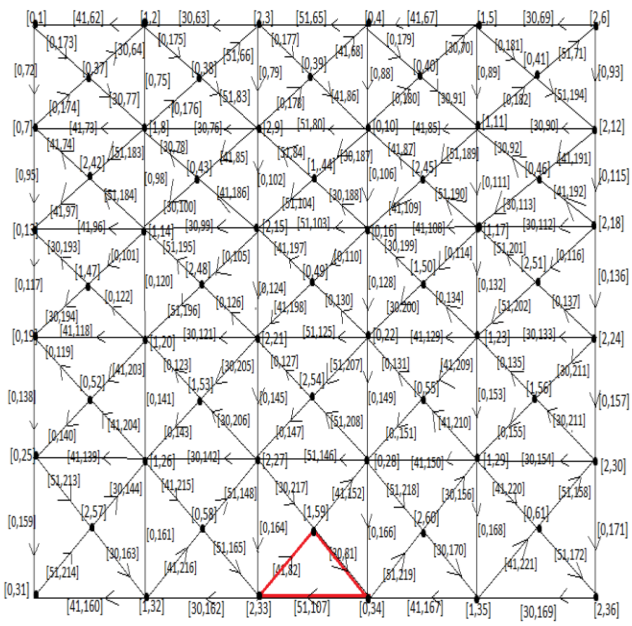

Fig. 2: Encrypted labeled strong face of a square grid graph $P_6 X P_6$ with key value as total edge magic triangle.

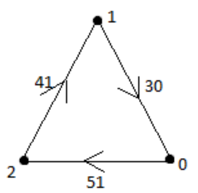

Fig. 3: Edge magic Cycle C_3

$$Nm = \sum_{ij \in E(C_3)} ((3 * f(\overrightarrow{v_i v_j}) + f(v_j)) \;\; for\ all\ \overrightarrow{v_i v_j} \in E(C_3)$$

= [(3×41)+1]+[(3×30)+0]+[(3×51)+2] =369.

8. Analysis

The common edge count k, which is a magic constant lies between $4n^2\text{-}n+2 \leq k \leq 8n^2\text{-}13n+7$ for n≡0 mod 3 and n≡ 1 mod 2 and lies between $5n^2\text{-}4n+2 < k < 8n^2\text{-}12n+9$ for n≡0 mod 3 and n≡ 0 mod 2. Also, the number of triangles of the strong face of a square grid graph is given by $4n^2\text{-}8n+4$, which shows that the worst case running time to decrypt the algorithm is $O(n^2)$.

9. Conclusion

Cryptography is the science of using mathematics to encrypt and decrypt data. In this paper, the method of encrypting numbers using labeled strong face of a square grid graph is investigated. Similar type of labeling technique can be used to encrypt using numbers for various graph structures to make the encryption complicated.

References

[1] Baskar Babujee, J. (2004), "On Edge Bimagic Labeling. Journal of Combinatorics, Information & System Sciences", *28-29(1-4)*, 239-244.

[2] Baskar Babujee, J., & Babitha, S. (2012), "Encrypting and Decrypting Number using Labeled Graphs", *European Journal of Scientific Research, 75(1)*, 14–24.

[3] Baskar Babujee, J., & Vishnupriya, V. (2017), "Encryption Numbers using Pair Labeling in Path Graphs", *International Journal of Pure and Applied Mathematics, 114(2)*, 249-259.

[4] Gallian, J.A. (2017), *A dynamic survey of graph labeli*ng, The Electronic Journal of Combinatorics, *#DS6*.

[5] Mohammed Ali Ahmed & Baskar Babujee, J. (2017), "Encryption through Labeled Graphs Using Strong Face Bimagic Labeling" , *International Mathematical Forum,* 12(4), 151-158.

[6] Rosa. (1966), "On certain valuations of vertices of a graph", *Theory of Graphs Internet Symposium, Rome, Gordon and Breach, NY (1967), Dunod, Paris,* 349–355.

[7] Telang, S.G. (1996). *Number Theory*, Tata McGraw-Hill Publishing Company Limited.

[8] Wallis, W.D. (2001). *Magic graphs*, Birkhauser.