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 $\mathbb{Z}_3$ 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 $G^r$ 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 $G^r$ 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 $f : V \cup E \to \{1, 2, \ldots, m+n\}$ 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 $C_j$ which plays important role in encryption and decryption of a given number.

Let $G$ be a strong face of a square grid graph $P_m \times P_n$ where $n \equiv 0 \pmod{3}$. Consider a bijective mapping $f : VUE \to \{1, 2, \ldots, 8n^2 \}$ with $(2n^2-2n+1)$ vertices, $(6n^2-10n+4)$ edges and $(4n^2-8n+4)$ cycles of length three. A magic cycle $C_j$ is fixed for which all the three edges have common edge count $k$.

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 $N_m$, consider the strong face of a square grid graph $P_m \times P_n$ where $n \geq 3$ and $n \equiv 0 \pmod{3}$, 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 $N_m$ into three parts using modulo class of $\mathbb{Z}_3$.
2. Let $V = \{v_i \leq 5n^2\}$ be the vertex set of a square grid graph.
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

![Fig.1: Strong face of a square grid graph $P_m \times P_n$.](image)

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.
4. Bound For The Magic Count

Let \{1,2,3,...,n^2+1,...,2n^2+n+1\} and \{2n^2+2n+2,2n^2+3,...,8n^2-12n+5\} be the labels of the vertices and edges of a strong face of a square grid graph \(P \times P_n\), \(n \geq 3\) respectively. By definition of total edge magic, 

\[ f(u)+f(v)+f=sk \text{ for all } u \in E. \]  

Case i: when \(n \equiv 0 \mod 3\); \(n \equiv 1 \mod 2\) 

Suppose consider a total edge magic cycle \(C_1\) with large labels of vertices say \(2n^2+2n+2,1+2n^1-3n+1\) and \(k=4n^2+n+1\). Consider the edges from cycles \(C_1\) with end vertices having labels \(2n^2-2n+1\) and \(3n-1\), then (1) becomes \(4+4(u)+4(u)\) implying \(f(u)+f(v)+f = 2n^2+2n+1\) which is in contradiction to the fact that \(f(u) \in [2n^2+2n+1,8n^2-12n+5]\) for all \(u \in E\). Hence 

\[ k > 4n^2+n+1. \]  

Similarly, consider a total edge magic cycle \(C_1\) with smaller labels of the vertices say \(1+2n+1n^2+1\) and \(k=8n^2-13n+8\). Consider the edges from cycles \(C_1\) with end vertices having labels \(1\) and \(n+1\), then (1) becomes \(4+4(u)+1+4(u)\) implying \(f(u)+f(v)+f = 8n^2-13n+8\) which implies 

\[ k < 8n^2-13n+8. \]  

From equations (2) and (3) the bounds for \(k\) is given by \(4n^2+n+2 \leq k \leq 8n^2-13n+7\). 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 \(4n^2+n+2 \leq k \leq 8n^2-13n+7\). 

Case ii: when \(n \equiv 0 \mod 3\); \(n \equiv 0 \mod 2\) 

Suppose consider a total magic cycle \(C_1\) with large labels of the vertices say \(2n^2+2n+2,1+2n^1-3n+1\) and \(k=5n^2-4n+2\), and smaller labels of the vertices say \(1<2n^2+1\) 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 \(P \times P_n\), where \(n\) is divisible by 3 and \(k\).

**Output:** Labeled encrypted \(G\).

**Step 1:** Fix the labeled of a square grid graph \(G\) with vertex set \(V = V_1 \cup V_2 \cup V_3\) where \(V_1 = \{i; i \equiv 1 \mod 3\}; V_2 = \{i; i \equiv 2 \mod 3\}\) and \(V_3 = \{i; i \equiv 0 \mod 3\}\) for \(1 \leq i \leq 2n^2+n+1\). The edge set is defined as 

\[ E = \{E(1,3); 1 \leq i \leq 8n^2-12n+5\} \cup \{E(0,3); 1 \leq i \leq 8n^2-12n+5\} \cup \{E(2,3); 1 \leq i \leq 8n^2-12n+5\} \cup \{E(1,0); 1 \leq i \leq 8n^2-12n+5\} \]  

**Step 2:** Consider a bijective function \(f: V \rightarrow [x, t], x \in \{0,1,2\}; 1 \leq t \leq 2n^2+n+1\) defined as \(f(v_i) = t - 1 \mod 3\); \(1 \leq t \leq 2n^2+n+1\).

**Step 3:** If \(Nm\) is divisible by 3, proceed to step 4 otherwise move to step 5.

**Step 4:** Partition \(Nm = \sum_{i=0}^{N^m_{0}} Nm_i\) in such a way \(Nm_i\) is congruent to \(1\) modulo 3 where \(i = 0, 1, 2\) and \(Nm_i > 3\), distinct. Create a unidirected magic cycle \(C_1\) by taking \(v_i \in V_1, v_j \in V_2\) and \(v_k \in V_3\) and 

\[ E = \{V_1, V_2, V_3, V_4, V_5, V_6\}. \]  

Label the edges of \(C_1\) as 

\[ \begin{align*} f(v_1, v_2) &= \left\lceil \frac{Nm}{3} \right\rceil - (k-y+z) f(v_2, v_3) &= \left\lceil \frac{Nm}{3} \right\rceil - (k-y+z) \end{align*} \]  

Go to step 6.

**Step 5:** Split \(Nm\) as \(Nm = \sum_{i=0}^{N^m_{0}} Nm_i\) in such a manner any two of \(N^m_{0}\) has same value over \(Z_i\) and \(Nm_i\) is greater than 3. Create a directed magic cycle \(C_2\) by taking \(v_1 \in V_1, v_2 \in V_2\) and \(v_3 \in V_3\) which does not have unidirectional 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: 

\[ \begin{align*} V_1, V_2, V_3, V_4, V_5, V_6, V_7, V_8, V_9, V_{10}, V_{11}, V_{12}, V_{13}, V_{14}, V_{15} \end{align*} \]  

Assign the labels for the edges of \(C_3\) as follows: 

If two of the \(Nm_i\) (say \(Nm_1, Nm_2\)) have residue value 0 when it is divisible by 3, then

\[ f(v_1, v_2) = \left\lceil \frac{Nm}{3} \right\rceil - (k-y+z) f(v_2, v_3) = \left\lceil \frac{Nm}{3} \right\rceil - (k-y+z) \]  

and if \(Nm\) have residue 1 and 2 when it is divisible by 3, then

\[ f(v_1, v_2) = \left\lceil \frac{Nm}{3} \right\rceil - (k-y+z) f(v_2, v_3) = \left\lceil \frac{Nm}{3} \right\rceil - (k-y+z) \]  

respectively.

If two of the \(Nm_i\) (say \(Nm_1, Nm_2\)) have residue value 1 when it is divisible by 3, then

\[ f(v_1, v_2) = \left\lceil \frac{Nm}{3} \right\rceil - (k-y+z) f(v_2, v_3) = \left\lceil \frac{Nm}{3} \right\rceil - (k-y+z) \]  

and if \(Nm\) have residue 0 and 2 when it is divisible by 3, then

\[ f(v_1, v_2) = \left\lceil \frac{Nm}{3} \right\rceil - (k-y+z) f(v_2, v_3) = \left\lceil \frac{Nm}{3} \right\rceil - (k-y+z) \]  

respectively.

If two of the \(Nm\) (say \(Nm_1, Nm_2\)) have residue value 2 when it is divisible by 3, then

\[ f(v_1, v_2) = \left\lceil \frac{Nm}{3} \right\rceil - (k-y+z) f(v_2, v_3) = \left\lceil \frac{Nm}{3} \right\rceil - (k-y+z) \]  

respectively.

Goto step 6.

**Step 6:** Let \(E^{**} = E' - E^*\). The direction of edges in \(E^{**}\) is defined as, for \(i \neq j\)

\[ f(v_i) = \frac{v_i}{v_j} \text{ if } i + j \equiv 0 \mod 2 \]

\[ f(v_i) = v_j \text{ if } \text{otherwise} \]
Consider a strong face of a square grid graph \( P_n \times P_n \) where \( n \equiv 0 \mod 3 \). 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 \([i,l]\) where \( l \) takes the values of residue class of \( Z_3 \) and \( i \) takes the values of \( \{1,2,\ldots,2n^2-2n+1\} \). The given number \( N_m \) greater than or equal to 12 is split in to three edges \( C_3 \), \( C_2 \) and \( C_1 \) respectively. The direction of this cycle \( C_3 \) is unidirectional if \( N_m \) is congruent to 0 modulo 3 and directed cycle \( C_1 \) if \( N_m \) 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 \( N_m \) which is going to be encrypted. Here \( N_m \) has residue value 1 when it is congruent to 0 modulo 3, then \( p = \frac{N_m}{3} \) 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 \( q = \frac{N_m}{3} k - (x+y) \). 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 \( f(v_i, v_j) \) of \( C_3 \), calculate \( 3^i f(v_i, v_j) + f(v_i) \) then the sum of the values of all three edges of \( C_3 \) leads to a secret number \( N_m \).

**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 \( N_m = 369 = 117 + 118 + 134 \) where \( k = 174 \). The encrypted labeled directed graph of a strong face of a square grid graph \( P_5 \times P_5 \) is as follows.

![Fig. 2: Encrypted labeled strong face of a square grid graph P_5 \times P_5.](image)

![Fig. 3: Edge magic Cycle C_3.](image)
\[ Nm = \sum_{i,j \in E(C)} ((3 \times f(v_i)) + f(v_j)) \text{ for all } v_i, v_j \in E(C) \]
\[ = [(3 \times 41) + 1] + [(3 \times 30) + 0] + [(3 \times 51) + 2] = 369. \]

8. Analysis

The common edge count \( k \), which is a magic constant lies between \( 4n^2 - n^2 + 2 \leq k \leq 8n^2 - 13n + 7 \) for \( n \equiv 0 \mod 3 \) and \( n \equiv 1 \mod 2 \) and lies between \( 5n^2 - 4n^2 + 2 \leq k \leq 8n^2 - 12n + 9 \) for \( n \equiv 0 \mod 3 \) and \( n \equiv 0 \mod 2 \). Also, the number of triangles of the strong face of a square grid graph is given by \( 4n^2 - 8n + 4 \), 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