Proceedings of the Jangjeon Mathematical Society
27 (2024), No. 4, pp. 707 - 720

www.jangjeon.or.kr
http://dx.doi.org/10.17777/pjms2024.27.4.707

GENERATING KEYS USING EOH LABELING FOR COMBINED CIPHERS

SHIVAPRIYA. P AND K. N. MEERA

Abstract. Let $G = (V, E)$ be a simple graph with $p = |V(G)|$ and $q = |E(G)|$. A one-one function $f : V \to \{1, 3, ..., 2p - 1\}$ is said to be an even-odd harmonious labeling of G if the induced function of edges $f^* : E \to \{0, 2, ..., 2(q - 1)\}$, $f^*(e = uv) = (f(u) + f(v))(mod\, 2q)$ is bijective. In this paper, we explore even-odd harmonious labeling for a few classes of graphs like odd cycles, Triangular book and $\langle C_3, nK_{1,r}\rangle$. An algorithm to obtain even-odd harmonious labeling for a triangular book $B_{(3,3)}$ is proposed. We further illustrate the use of this labeling to generate keys in cryptography by combined cipher techniques. The cipher techniques to be used here are Columnar transposition cipher and Vigenere cipher.

2010 Mathematics Subject Classification. 05C78, 94A60.

Keywords. Bijective, Cryptography, Even-odd harmonious, Triangular book.

1. Introduction

For basic graph theory terminology we refer [2]. In the vast area of graph theory, labeling of graphs is one of the fascinating fields with boundless opportunities in research. Labeling of graphs is simply assigning values/integers to vertices, edges or both in a graph. The three most common labelings are, vertex labeling, edge labeling and total labeling. Assigning values only to vertices is vertex labeling and assigning values only to edges is edge labeling. Assigning values to both vertices and edges in a graph gives total labeling. Some of the known graph labeling techniques are graceful labeling, edge-graceful labeling, lucky labeling, harmonious labeling, magic labeling and anti-magic labeling.

Even-odd harmonious(EOH) labeling is an important graph labeling technique introduced in 2015 by Adalin Beatress and Sarasija. In EOH labeling, we consider a one-one function for vertices, so that they are assigned with odd positive integers which then induces a function on edges satisfying certain conditions. Several authors have tried to explore the classes of graphs which admit EOH labeling and few papers have been published in the years following its introduction. In [6], the authors worked on proving the existence of EOH labeling for few families of acyclic graphs like caterpillar graph $cat_m^{+t}(l, r)$, 1-regular lobster graph, Coconut tree CT_{mn}, Spider tree graph with n legs and length l, and Star graph $S_{m,3}$. The authors continued their work for cyclic graphs like Fan graph F_n, Ladder graph L_n, Prism graph P_2 x C_{2m+1}, Total graph $T(P_n)$, Braid graph B(n), Jellyfish graph $J(m, n)$, Petersen graph, the graphs $P_{2n}(+)N_m$ and $(P_2 \cup mK_1) + N_2$ in [7]. In [8],

the authors have proved the existence of EOH labeling for graphs obtained through various graph operations like union of graphs, superimposition of graphs and Corona product graphs. Later, in [4] authors manifested definite graphs and proved the existence of EOH labeling for some graphs like H-graph, Comb graph C_{bn}, Bistar graph and the graph $< k_{1,n}^{(1)}, k_{1,n}^{(2)}, k_{1,n}^{(3)} >$, which is a combination of three star graphs.

Numerous graph labeling techniques are applied by researchers under various fields of interest, one of which is Cryptography. Cryptography is a method that ensures secure communication and data transmissions using cryptosystems [1, 5]. In a cryptosystem, a message is passed from sender to receiver through a channel. The message/plaintext on encryption produces a ciphertext that is decrypted by the receiver to obtain the message [12]. The process of encryption and decryption is carried out using a key. Various cryptographic techniques were developed throughout the years to reduce attacks by third parties(or adversaries) [11]. By combining ciphers, a stronger cryptosystem can be formed which makes it difficult for any adversaries to hack the message. A combination of the ciphers; Columnar transposition and Vigenere, are applied in this work. Each cipher uses a key for encryption and decryption. These keys are generated using labeled graphs [9, 3].

The article is divided into 5 sections. In section 2 we recall the definitions of harmonious and EOH labeling, and discover new classes of graphs admitting EOH labeling. In section 3, an algorithm is described that is used to label the Triangular book $B_{(3,m)}$. In section 4, the concept of EOH labeling is used to generate keys for encryption and decryption of the cipher techniques. An illustration explaining the same is given in the section. Finally, in section 5 we conclude with some open problems.

2. EOH labeling of graphs

First, we recall some basic definitions and present the results later on. We show that certain classes of graphs like odd cycles, Triangular book and $\langle C_3, nK_{1,r}\rangle$ admit EOH labeling. $\langle C_3, nK_{1,r}\rangle$ is the graph obtained by identifying each of the central vertices of n copies of the star graph with n vertices of C_3, where $1 \leq n \leq 3$.

Definition 1. Let G be a graph with $p = |V(G)|$ and $q = |E(G)|$. A one-one function $f : V(G) \to \mathbb{Z}_q$, is said to be harmonious labeling if it induces a bijective function $f^* : E(G) \to \mathbb{Z}_q$ as $f^*(e = u'v') = ((f(u') + f(v'))mod\, q$ where $\mathbb{Z}_q$ is the group under addition modulo q. A graph admitting such labeling is known as a harmonious graph [10].

The harmonious labeling of a Fan graph is given in Figure 1.

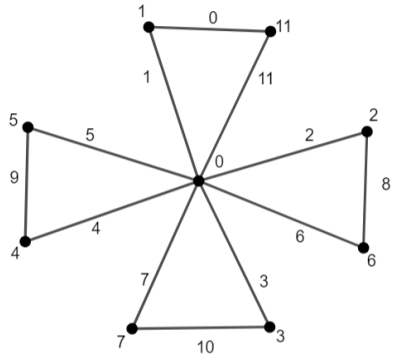

FIGURE 1. Harmonious labeling of Fan graph F_4

Definition 2. Let G be a graph with $p = |V(G)|$ and $q = |E(G)|$. A one-one function $f : V(G) \to \{1, 3, ..., 2p-1\}$, is said to be EOH labeling if it induces a bijective function $f^* : E(G) \to \{0, 2, ..., 2q-2\}$, as $f^*(e = u'v') = ((f(u') + f(v'))mod\, 2q$. A graph admitting such labeling is known as an EOH graph.

An EOH labeling of the star graph $K_{1,6}$ is given in Figure 2.

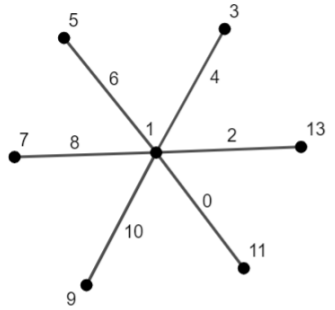

FIGURE 2. EOH labeling of Star graph $K_{1,6}$

Theorem 2.1. All odd cycles C_n, $n = 2k+1,\ k \geq 1$ admit EOH labeling.

Proof. Consider the odd cycle $C_{2k+1},\ k \geq 1$.
Let $V = \{u_i : 1 \leq i \leq 2k+1\}$ be the vertex set and $E = \{u_1u_{2k+1}\} \cup \{u_iu_{i+1} : 1 \leq i \leq 2k\}$ be the edge set respectively.
We define a one-one function $f : V \to \{1, 3, ..., (4k+1)\}$ as,
$f(u_i) = 2i - 1,\ 1 \leq i \leq 2k+1$
The induced function $f^* : E \to \{0, 2, ..., 4k\}$ is given by,
$f^*(e_i) = (f(u_i) + f(u_{i+1}))mod\,(4k+2)$
$= (2i - 1 + 2i + 1)mod\,(4k+2)$
$= (4i)mod\,(4k+2),\ \forall\ i,\ 1 \leq i \leq 2k$

$f^*(e_{2k+1}) = (f(u_1) + f(u_{2k+1}))mod\,(4k+2)$
$= (1 + 4k + 1)mod\,(4k+2)$
$= (4k+2)mod\,(4k+2)$
$= 0$
We see that $f^*(e_{2k+1}) = 0$ and $f^*(e_i) \neq 0$ for any value of i.
Hence, we can say that $f^*(e_{2k+1}) \neq f^*(e_i)$.
Now, we must prove that no labels for edges are repeated for given vertex labelings.
We shall prove this by using the method of contradiction.
The set of all possible edge labels for a cycle C_{2k+1} is $\{0, 2, ..., 4k\}$.
Suppose that at least one label from the set is repeated or f^* is not bijective, then the chances of the labels to be repeated is after every $(4k+2)^{th}$ term i.e. $\{(0 + 4k + 2), (2 + 4k + 2), ..., (4k + 4k + 2)\}$
$= \{4k + 2,\ 4k + 4, ...,\ 8k + 2\}$
On taking modulo of these,
$\implies \{(4k + 2)mod\,(4k + 2), (4k + 4)mod\,(4k + 2), ..., (8k + 2)mod\,(4k + 2)\}$
$= \{0, 2, ..., 4k\}$ (the set of all possible edge labels for C_{2k+1} cycle).
Since $4k < 4k + 2$ and all edge labels exist for C_{2k+1}, we can say that the labels do not repeat under $mod\,(4k + 2)$.
This contradicts our assumption that f^* is not bijective.
$\therefore$ function defined gives EOH labeling for C_{2k+1}.
Hence, all C_n, $n = 2k + 1$, $k \geq 1$ admit EOH labeling.

The EOH labeling of an odd cycle is given in Figure 3.

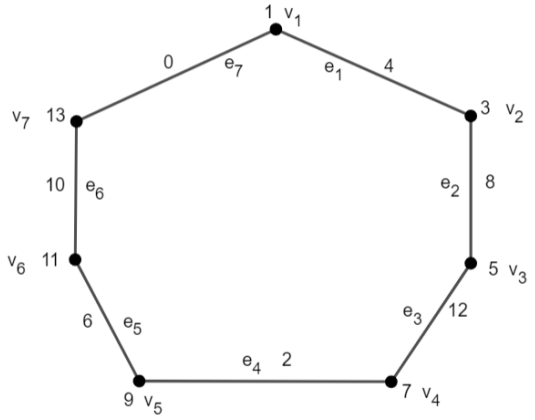

FIGURE 3. EOH labeling of C_7

Definition 3. The Triangular Book graph, denoted by $B_{(3,m)}$ is a graph with m copies of cycle C_3 sharing a common edge. This edge is known as base of the book.

Theorem 2.2. Triangular book graphs $B_{(3,m)}$ admit EOH labeling for $m \geq 2$.

Proof. Consider a Triangular book graph $B_{(3,m)}$ constructed by joining two adjacent vertices to m further vertices with $|V(G)| = m + 2$ and $|E(G)| = 2m + 1$.
Consider $V = \{v_1\} \cup \{v_i : 2 \leq i \leq m + 1\} \cup \{v_{m+2}\}$ be vertex set and $E = \{v_1v_i : 2 \leq i \leq m + 1\} \cup \{v_iv_{m+2} : 2 \leq i \leq m + 1\} \cup \{v_1v_{m+2}\}$ be edge set in $B_{(3,m)}$.
We define a one-one function $f : V \to \{1, 3, ..., 2m + 3\}$ as,
$f(v_1) = 1$
$f(v_i) = 2i - 1,\ 2 \leq i \leq m + 1$
$f(v_{m+2}) = 2m + 3$
The induced function $f^* : E \to \{0, 2, ..., 4m\}$ is given by,
$f^*(e_i) = (f(v_1) + f(v_{i+1}))mod\,(4m + 2)$
$\quad = (2i + 2)[mod\,(4m + 2)],\ 1 \leq i \leq m$
$f^*(e_j) = (f(v_{i+1}) + f(v_{m+2}))mod\,(4m + 2)$
$\quad = (2j + 4)[mod\,(4m + 2)],\ 1 \leq i \leq m,\ j = i + m$
$f^*(e) = (f(v_1) + f(v_{m+2}))mod\,(4m + 2)$
$\quad = (2m + 4)mod\,(4m + 2)$
e_i, e_j and e are edges formed by the vertices v_1, v_{i+1}; v_{i+1}, v_{m+2} and v_1, v_{m+2} respectively.
To show f^* is bijective, we must prove that $f^*(e_i) \neq f^*(e_j) \neq f^*(e)$
Case (i): To show $f^*(e_i) \neq f^*(e)$
For $i = m$, $f^*(e_m) = (2m + 2)mod\,(4m + 2) = 2m + 2$
and,
$f^*(e) = (2m + 4)mod\,(4m + 2) = 2m + 4\ \forall\ m \geq 2$
Also, $2m + 2 < 2m + 4 \implies f^*(e_i) < f^*(e)$
i.e. $f^*(e_i) \neq f^*(e)$
Case (ii): To show $f^*(e_j) \neq f^*(e)$
Suppose, $f^*(e_j) = f^*(e)$
$\implies (2j + 4)mod\,(4m + 2) = (2m + 4)mod\,(4m + 2)$
$\implies j = m$, which is a contradiction as $m + 1 \leq j \leq 2m$
$\therefore f^*(e_j) \neq f^*(e)$
Case (iii): To show $f^*(e_i) \neq f^*(e_j)$
Consider $f^*(e_i)\ \forall\ 1 \leq i \leq m$
i.e. $f^*(e_1) = 4mod\,(4m + 2) = 4$
$f^*(e_2) = 6mod(4m + 2) = 6$
.
.
.
$f^*(e_{m-1}) = (2m)mod\,(4m + 2) = 2m$
$f^*(e_m) = (2m + 2)mod\,(4m + 2) = 2m + 2$
From this we get $2i + 2 < 4m + 2,\ \forall\, i,\ 1 \leq i \leq m$
Hence, no value of $f^*(e_i)$ gets repeated for $1 \leq i \leq m$.

Similarly, consider $f^*(e_j)\ \forall\ j,\ m + 1 \leq j \leq 2m$
i.e. $f^*(e_{m+1}) = (2m + 6)mod\,(4m + 2) = 2m + 6$
$f^*(e_{m+2}) = (2m + 8)mod\,(4m + 2) = 2m + 8$
.
.
.

$f^*(e_{2m-2}) = (4m) mod\,(4m+2) = 4m$
$f^*(e_{2m-1}) = (4m+2) mod\,(4m+2) = 0$
$f^*(e_{2m}) = (4m+4) mod\,(4m+2) = 2$
We see that $2j+4 < 4m+2 \;\; \forall\, j,\, m+1 \leq j \leq m-2$,
$2j+4 = 4m+2$ for $j = 2m-1$
and $2j+4 > 4m+2$ for $j = 2m$.
$\therefore$ no value of $f^*(e_j)$ is being repeated
and $2i+2 < 2j+4\ \forall\, i\,,\ 1 \leq i \leq m,\ j = i+m$
$\implies (2i+2) mod\,(4m+2) \neq (2j+4) mod\,(4m+2)$
$\implies f^*(e_i) \neq f^*(e_j)$
From all three cases we have, $f^*(e_i) \neq f^*(e_j) \neq f^*(e)$
Clearly, f^* is bijective.
$\therefore$ function defined here gives EOH labeling of $B_{(3,m)}$.
Hence, the Triangular book graph $B_{(3,m)}$ admits EOH labeling.

The EOH labeling of the Triangular book $B_{(3,3)}$ is given in Figure 4.

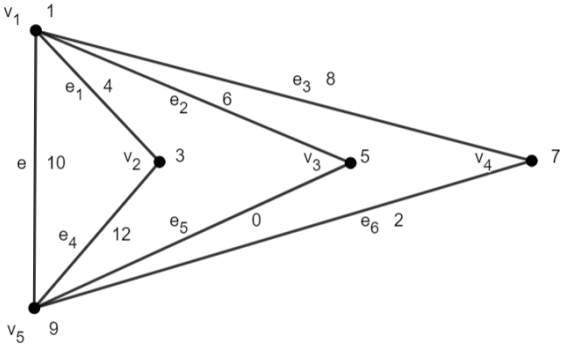

FIGURE 4. EOH labeling of the Triangular book $B_{(3,3)}$

Theorem 2.3. The graph $\langle C_3, K_{1,r}\rangle$ admits EOH labeling for all $r \geq 1$.

Proof. Consider the graph $\langle C_3, K_{1,r}\rangle$ obtained by identifying the central vertex of a star graph $K_{1,r}$ with a single vertex of C_3 .
Here, $|V(G)| = |E(G)| = r+3$
Let $V = \{u_1, u_2, u_3\} \cup \{v_i : 1 \leq i \leq r\}$ be vertex set and $E = \{u_1u_2, u_2u_3, u_1u_3\} \cup \{u_3v_i : 1 \leq i \leq r\}$ be edge set in $\langle C_3, K_{1,r}\rangle$.
We define a one-one function $f : V \to \{1, 3, ..., 2r+5\}$ as,
$f(u_1) = 5,\ f(u_2) = 1,\ f(u_3) = 3$
$f(v_i) = 2i+5,\ \forall\, i, 1 \leq i \leq r$
The induced function $f^* : E \to \{0, 2, ..., 2(r+2)\}$ is given by,
$f^*(e_1) = (f(u_1) + f(u_2)) mod\,(2r+6)$
$\quad = 6 mod\,(2r+6)$
$f^*(e_2) = (f(u_2) + f(u_3)) mod\,(2r+6)$
$\quad = 4 mod\,(2r+6)$
$f^*(e_3) = (f(u_1) + f(u_3)) mod\,(2r+6)$
$\quad = 8 mod\,(2r+6)$

$f^*(e_i^{'}) = (f(u_3) + f(v_i))mod\,(2r+6)$
$\quad = (2i+8)mod\,(2r+6),\ \forall\, i,\ 1 \le i \le r$
e_1, e_2 and e_3 are edges of C_3 and $e_i^{'} = u_3v_i$
For $r \ge 1$
$f(u_1) = 5, f(u_2) = 1, f(u_3) = 3, f(v_1) = 7, f(v_2) = 9, ..., f(v_r) = 2r+5$
$f^*(e_1) = 6mod\,(2r+6) = 6$
$f^*(e_2) = 4mod\,(2r+6) = 4$
$f^*(e_3) = 8mod\,(2r+6) = 8$
$f^*(e_1') = 10mod\,(2r+6) = 10$
.
.
.
$f^*(e_{r-1}') = (2r+6)mod\,(2r+6) = 0$
$f^*(e_r') = (2r+8)mod\,(2r+6) = 2$
Clearly, f^* is bijective
$\therefore$ function defined here gives EOH labeling of $\langle C_3, K_{1,r}\rangle$.
Hence, $\langle C_3, K_{1,r}\rangle$ admits EOH labeling for all $r \ge 1$.

The EOH labeling of $\langle C_3, K_{1,5}\rangle$ graph is given in Figure 5.

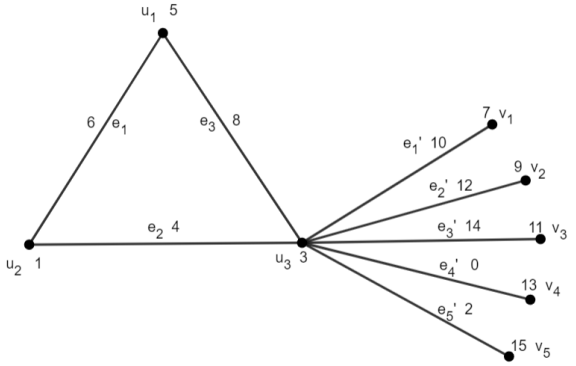

FIGURE 5. EOH labeling of $\langle C_3, K_{1,5}\rangle$

Theorem 2.4. The graph $\langle C_3, 2K_{1,r}\rangle$ admits EOH labeling for all $r \ge 1$.

Proof. Consider the graph $\langle C_3, 2K_{1,r}\rangle$ obtained by identifying the central vertex of a star graph $K_{1,r}$ with two vertices of C_3 where $|V(G)| = |E(G)| = 2r+3$.
Let $V = \{u_1, u_2, u_3\} \cup \{v_{2i-1} : 1 \le i \le r\} \cup \{v_{2i} : 1 \le i \le r\}$ and $E = \{u_1u_2, u_2u_3, u_1u_3\} \cup \{u_2v_{2i-1} : 1 \le i \le r\} \cup \{u_3v_{2i} : 1 \le i \le r\}$
We define a one-one function $f : V \to \{1, 3, ..., 4r+5\}$ as,
$f(u_1) = 3,\ f(u_2) = 5,\ f(u_3) = 1$
$f(v_{2i-1}) = 4i+3,\ \forall\, i,\ 1 \le i \le r$
$f(v_{2i}) = 4i+5,\ \forall\, i,\ 1 \le i \le r$
The induced function $f^* : E \to \{0, 2, ..., 4r+4\}$ is given by,
$f^*(e_1) = (f(u_1) + f(u_2))mod\,(4r+6)$

$= 6mod\,(4r+6)$
$f^*(e_2) = (f(u_2)+f(u_3))mod\,(4r+6)$
$= 4mod\,(4r+6)$
$f^*(e_3) = (f(u_1)+f(u_3))mod\,(4r+6)$
$= 8mod\,(4r+6)$
$f^*(e_i') = (f(u_2)+f(v_{2i-1}))mod\,(4r+6)$
$= (4i+8)mod\,(4r+6)\ \forall\, i,\ 1 \le i \le r$
$f^*(e_i'') = (f(u_3)+f(v_{2i}))mod\,(4r+6)$
$= (4i+6)mod\,(4r+6)\ \forall\, i,\ 1 \le i \le r$
e_1, e_2, e_3 are edges of C_3 and $e_i' = u_2v_{2i-1}$, $e_i'' = u_3v_{2i}$
where, f^* is bijective
$\therefore$ function defined here gives EOH labeling of $\langle C_3, 2K_{1,r}\rangle$.
Hence, $\langle C_3, 2K_{1,r}\rangle$ admits EOH labeling for all $r \ge 1$.

The EOH labeling of $\langle C_3, 2K_{1,4}\rangle$ graph is given in Figure 6.

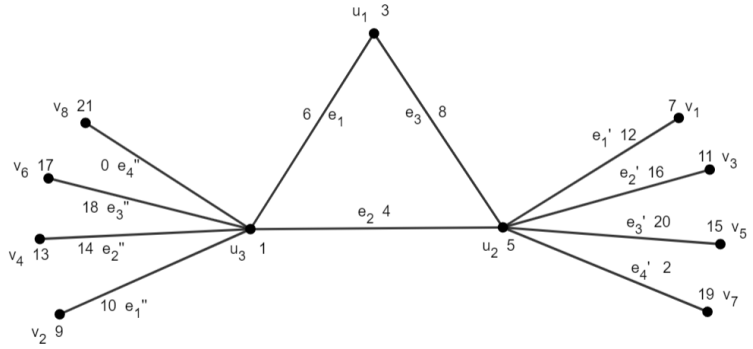

FIGURE 6. EOH labeling of $\langle C_3, 2K_{1,4}\rangle$

Theorem 2.5. The graph $\langle C_3, 3K_{1,r}\rangle$ admits EOH labeling for all $r \ge 1$.

Proof. Consider the graph $\langle C_3, 3K_{1,r}\rangle$ obtained by identifying the central vertex of a star graph $K_{1,r}$ with three vertices of C_3 where $|V(G)| = |E(G)| = 3r+3$.
Let $V = \{u_1, u_2, u_3\} \cup \{v_{3i-2} : 1 \le i \le r\} \cup \{v_{3i-1} : 1 \le i \le r\} \cup \{v_{3i} : 1 \le i \le r\}$ and $E = \{u_1u_2, u_2u_3, u_1u_3\} \cup \{u_1v_{3i} : 1 \le i \le r\} \cup \{u_2v_{3i-2} : 1 \le i \le r\} \cup \{u_3v_{3i-1} : 1 \le i \le r\}$
We define a one-one function $f : V \to \{1, 3, ..., 6r+5\}$ as,
$f(u_1) = 3,\ f(u_2) = 5,\ f(u_3) = 1$
$f(v_{3i-2}) = 6i+1\ \forall\, i,\ 1 \le i \le r$
$f(v_{3i-1}) = 6i+3\ \forall\, i,\ 1 \le i \le r$
$f(v_{3i}) = 6i+5\ \forall\, i,\ 1 \le i \le r$
The induced function $f^* : E \to \{0, 2, ..., 6r+4\}$ is given by,
$f^*(e_1) = (f(u_1)+f(u_2))mod\,(6r+6)$
$= 6mod\,(6r+6)$
$f^*(e_2) = (f(u_2)+f(u_3))mod\,(6r+6)$
$= 4mod\,(6r+6)$

$f^*(e_3) = (f(u_1) + f(u_3))mod\,(6r+6)$
$\quad = 8mod\,(6r+6)$
$f^*(e_i') = (f(u_3) + f(v_{3i-1}))mod\,(6r+6)$
$\quad = (6i+6)mod\,(6r+6)\ \forall\, i,\ 1 \le i \le r$
$f^*(e_i'') = (f(u_2) + f(v_{3i-2}))mod\,(6r+6)$
$\quad = (6i+4)mod\,(6r+6)\ \forall\, i,\ 1 \le i \le r$
$f^*(e_i''') = (f(u_1) + f(v_{3i}))mod\,(6r+6)$
$\quad = (6i+8)mod\,(6r+6)\ \forall\, i,\ 1 \le i \le r$
e_1, e_2, e_3 are edges of C_3 and $e_i' = u_1v_{3i}$, $e_i'' = u_2v_{3i-2}$, $e_i''' = u_3v_{3i-1}$
where, f^* is bijective
$\therefore$ function defined here gives EOH labeling of $\langle C_3, 3K_{1,r}\rangle$.
Hence, $\langle C_3, 3K_{1,r}\rangle$ admits EOH labeling for all $r \ge 1$.

The EOH labeling of $\langle C_3, 3K_{1,4}\rangle$ graph is given in Figure 7.

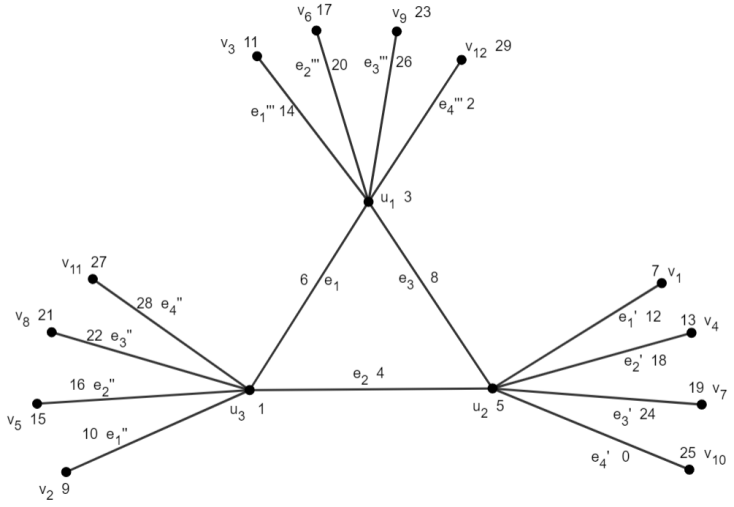

FIGURE 7. EOH labeling of $\langle C_3, 3K_{1,4}\rangle$

3. Algorithm

The following algorithm is used to obtain EOH labeling for a Triangular book graph $B_{(3,m)}$.

Algorithm The algorithm used to obtain EOH labeling of Triangular book $B_{(3,m)}$.

Input: m

$f(v_1) \leftarrow 1$
for $i = 2$ to m **do**
  $f(v_i) \leftarrow 2i - 1$
  $f(v_{m+2}) \leftarrow 2m + 3$
end for
$f^*(e) \leftarrow (f(v_1) + f(v_{m+2}))mod\,(4m + 2)$
for $i = 1$ to m **do**
  $f^*(e_i) \leftarrow (f(v_1) + f(v_{i+1}))mod\,(4m + 2)$
  for $i = m + 1$ to $2m$ **do**
    $f^*(e_i) \leftarrow (f(v_{m+2}) + f(v_{i+1-m}))mod\,(4m + 2)$
  end for
end for

4. Key generation using EOH labeling

We have proved the existence of EOH labeling for a few graphs in the previous section. Now, we apply this labeling technique to generate keys for Columnar transposition and Vigenere cipher.

A **Columnar transposition (CT) cipher** involves writing the plaintext in rows of a rectangular array and obtaining the ciphertext by reading it column-wise one by one in the order formed from a key K.

The **Vigenere cipher** is a poly-alphabetic cryptosystem which uses the following;

(i) The finite set of possible plaintexts, $\mathcal{P}$
(ii) The finite set of possible ciphertexts, $\mathcal{C}$
(iii) The finite set of possible keys, $\mathcal{K}$

Representing the 26 English alphabets by the group $\mathbb{Z}_{26}$, as shown in the Table 1 we have, $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}^m$, where m is the length of the key $K \in \mathcal{K}$. For key $K = (k_1, k_2, ..., k_m)$ the encryption and decryption are carried out as follows;
Encryption: $E_K(p_1, p_2, ...p_m) = (p_1 + k_1,\ p_2 + k_2,\ ..., p_m + k_m)$
Decryption: $D_K(c_1, c_2, ...c_m) = (c_1 - k_1, c_2 - k_2, ..., c_m - k_m)$
where the operations are under *modulo 26.*

Procedure for key generation. The sender sends the following information to the receiver along with the encrypted message:

(i) the number of words n
(ii) the vertex-edge sequence whose labels are the length of words in the plaintext.

(1) The sender removes the space between the words of the plaintext. Both the sender and receiver construct the graph $B_{(3,n)}$ or $B_{(3,n-1)}$ based on whether n is odd or even respectively. They label the graph using the Algorithm in section 3.

(2) Two keys are obtained from the labeled graph. The first key K_1, is the label of the edges taken in the order $e_1, e_2, ..., e_m, e_{m+1}, e_{m+2}, ..., e_{2m}, e$ (e is the edge incident between v_1 and v_{m+2}) which is used in CT cipher. The encryption and decryption techniques of CT cipher using K_1 are denoted by ECT_{K_1} and DCT_{K_1} respectively. The second key K_2 is the label of vertices taken in the order v_1, v_2, ..., v_{m+2} which is used in Vigenere cipher. The encryption and decryption techniques of Vigenere cipher using K_2 are denoted by EVC_{K_2} and DVC_{K_2}.
(3) The key K_1 is converted to its corresponding alphabetical equivalent given in Table 1.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

TABLE 1. Alphabet-number table

(4) At first, the encryption algorithm of CT cipher, namely ECT is applied on the plaintext P with key K_1 to get the CT ciphertext P'. Then encryption algorithm of Vigenere cipher, namely EVT is applied on P' with key K_2 to obtain the Vigenere cipher text C.
i.e. $ECT_{K_1}(P) = P'$ and $EVC_{K_2}(P') = C$,
or $C = EVC_{K_2}(ECT_{K_1}(P))$.
(5) Upon receiving these, the receiver obtains the keys K_1 and K_2 from the EOH labeled $B_{(3,n)}$ or $B_{(3,n-1)}$. The receiver then applies the decryption algorithms in the reverse order with their respective keys. Thus, obtaining $P = DCT_{K_1}(DVC_{K_2}(C))$.
(6) The Vigenere cipher text C, the value of n, the edge sequence corresponding to key K_1, the vertex sequence corresponding to key K_2 and the vertex-edge sequence whose labels correspond to the words in the plaintext delimited by semicolon are sent from the sender to the receiver.

We provide an illustration to describe the encryption decryption process.

Illustration.

Encryption. Suppose "COMPARISON CREATES DESPAIR" is the message. Here $n = 3$ as there are three words. Their lengths are 10, 7 and 7 respectively.

(1) The sender combines these words to form the plaintext P: $COMPARISONCREATESDESPAIR$. Both sender and receiver constructs the $B_{(3,3)}$ graph as n is odd and label it using the Algorithm in section 3. The labeled graph is shown in Figure 8.
(2) The sequence of edges and vertices are $e_1, e_2, e_3, e_4, e_5, e_6, e$ and v_1, v_2, v_3, v_4, v_5. Their labels form the keys $K_1 = 468120210$ and $K_2 = 13579$.

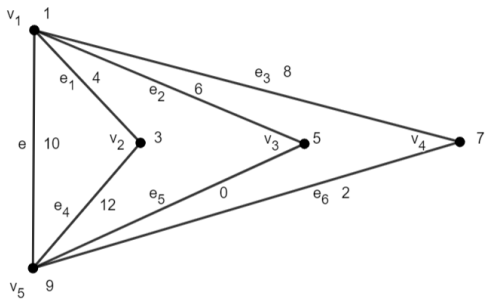

FIGURE 8. Triangular book $B_{(3,3)}$

(3) The next step is to construct the table for CT cipher. The alphabetical equivalent of K_1 is $EGIMACK$ with 7 alphabets, so a table with 7 columns is considered. The key is entered in the first row. The next row gives a numbering to these alphabets in their order of appearance among the English alphabets. For example, A is numbered 1, C is numbered 2 and so on.
(4) Next, the plaintext P is entered through the rows. The blank cells, if any, are filled with a rare letter say Q (which is agreed by both the sender and the receiver prior to communication). The CT cipher table is shown in Table 2.

E	G	I	M	A	C	K
3	4	5	7	1	2	6
C	O	M	P	A	R	I
S	O	N	C	R	E	A
T	E	S	D	E	S	P
A	I	R	Q	Q	Q	Q

TABLE 2. CT cipher table

(5) The letters from Table 2 are read out column-wise according to column numbers obtained in previous step. This gives the CT ciphertext P': $AREQ\,RESQ\,CSTA\,OOEI\,MNSR\,IAPQ\,PCDQ$.
(6) Next the Vigenere encryption algorithm EVC is applied on P' using key K_2. For this the Table 3 is constructed. The CT cipher P' is written in the first row followed by its numerical equivalents x in the second row as given in Table 1. A key stream using $K_2 = 13579$ is formed and this constitutes the third row of the table. The values of $(x + K_2) mod\, 26$ are computed and listed in the fourth row. The alphabetical equivalents of the values in fourth row are written in the fifth row using Table 1. This gives the Vigenere ciphertext C : $BUJX\,AFVV\,JBUD\,TVNJ\,PSZA\,JDUX\,YDGV$.

P'	A	R	E	Q	R	E	S	Q	C	S	T	A	O	O	E	I	M	N	S	R	I	A	P	Q	P	C	D	Q
x	0	17	4	16	17	4	18	16	2	18	19	0	14	14	4	8	12	13	18	17	8	0	15	16	15	2	3	16
K_2	1	3	5	7	9	1	3	5	7	9	1	3	5	7	9	1	3	5	7	9	1	3	5	7	9	1	3	5
$(x+K_2) mod 26$	1	20	9	23	0	5	21	21	9	1	20	3	19	21	13	9	15	18	25	0	9	3	20	23	24	3	6	21
C	B	U	J	X	A	F	V	V	J	B	U	D	T	V	N	J	P	S	Z	A	J	D	U	X	Y	D	G	V

TABLE 3. Encryption using Vigenere cipher

(7) Now the sender sends the encrypted message C, the value of n, edge sequence representing K_1, vertex sequence representing K_2, vertex-edge sequence corresponding to the length of the words in the plaintext delimited by semicolon. For the given example, this is $BUJXAFVVJBUDTVNJPSZAJDUXYDGV$; 3; 468120210; 13579; the last sequence represents 10, 7 and 7, which gives the length of the the three words in the message.

Decryption.

(1) On receiving this, the receiver now forms both keys K_1 and K_2 using the sequences of edges and vertices as $K_1 = 468120210$ and $K_2 = 13579$ from the EOH labeled $B_{(3,3)}$ graph, which is already constructed by both the sender and receiver. The key K_1 is converted to its alphabetical equivalent by the same method described in the encryption section.

(2) Then, the decryption algorithm DVC using key K_2 is applied on the Vigenere ciphertext C to obtain the CT ciphertext P': $AREQRESQ$ $CSTAOOEIMNSRIAPQPCDQ$ as shown in Table 4.

C	B	U	J	X	A	F	V	V	J	B	U	D	T	V	N	J	P	S	Z	A	J	D	U	X	Y	D	G	V
y	1	20	9	23	0	5	21	21	9	1	20	3	19	21	13	9	15	18	25	0	9	3	20	23	24	3	6	21
K_2	1	3	5	7	9	1	3	5	7	9	1	3	5	7	9	1	3	5	7	9	1	3	5	7	9	1	3	5
$(y-K_2) mod 26$	0	17	4	16	17	4	18	16	2	18	19	0	14	14	4	8	12	13	18	17	8	0	15	16	15	2	3	16
P'	A	R	E	Q	R	E	S	Q	C	S	T	A	O	O	E	I	M	N	S	R	I	A	P	Q	P	C	D	Q

TABLE 4. Decryption using Vigenere cipher

(3) The receiver then constructs the CT cipher table using K_1 in similar manner as done in ECT for the first two rows. Next, P' is entered along the columns according to the column numbers, i.e, column with number 1 is filled first followed by 2 till 7, giving Table 2.

(4) The receiver then reads out the letters from Table 2 along the rows and remove the additional letters Q to obtain the plaintext P: COM $PARISONCREATESDESPAIR$.

(5) Now, the receiver uses the labels of the vertex-edge sequence e, v_4, v_4 (10,7,7) to split plain text P by adding spaces at lengths 10, 7 and 7 respectively.

(6) This reverts the plaintext to its initial form as "COMPARISON CREATES DESPAIR" which completes the procedure.

5. Conclusion

Here, we have explored the EOH labeling for a few classes of graphs like cycles C_{2k+1}, Triangular book $B_{(3,m)}$ and $\langle C_3, nK_{1,r}\rangle$ and proved that they admit EOH labeling. We worked on generating keys using EOH labeling and

explained it by using Triangular book $B_{(3,3)}$. The novelty in this work is that we have combined cipher techniques along with EOH labeling to generate keys which makes it difficult for any third party to attack the message. Further studies on proving the existence of certain other families of graphs can be done. Also, various other cryptographic techniques along with EOH labeling can be used to reduce the attack from hackers.

References

[1] B. K. Lavanya and B. R. Pushpa, *Data hiding by means of color cryptography and optimum value transfer method*, Journal of Advanced Research in Dynamical and Control Systems, 10, no. 3(2018).

[2] D. B. West, *Introduction to graph theory*, Prentice Hall (2000).

[3] Dhanyashree, P. Shivapriya, and K. N. Meera, *Key generation in cryptography using graph labeling techniques*, 2022 IEEE 4th PhD Colloquium on Emerging Domain Innovation and Technology for Society (PhD EDITS) (2022).

[4] D. Zala, N. Chotaliya, and M. Chaurasiya, *Even-odd harmonious labeling of some graphs*, International Journal of Innovative Technology and Exploring Engineering, 10 (2021).

[5] K. Jain, P. Krishnan, and V. V. Rao, *A comparison based approach on mutual authentication and key agreement using DNA cryptography*, 2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT) (2021).

[6] M. Kalaimathi and B. J. Balamurugan, *Computation of even-odd harmonious labeling of certain family of acyclic graphs*, J. Engin. Adv. Tech (IJEAT), 9 (2019).

[7] M. Kalaimathi and B. J. Balamurugan, *Even-Odd Harmonious Labeling of Certain Family of Cyclic Graphs* , International Journal of Innovative Technology and Exploring Engineering(IJITEE), 9 (2020).

[8] M. Kalaimathi and B. J. Balamurugan, *Computation of even-odd harmonious labeling of graphs obtained by graph operations*, Recent Trends in Pure and Applied Mathematics, 2177, AIP Publishing (2019).

[9] M. Saraswathi and K. N. Meera, *Radio mean labeled graphs to generate keys in cryptography*, 2nd International Conference on Communication, Computing and Industry 4.0 (C2I4), IEEE (2021).

[10] M.S. Franklin, T. Selvi, and A. Amrutha, *Harmonious labeling of some special classes of graphs*, International Journal of Pure and Applied Mathematics, 118 (2018).

[11] M. Suresh, V. A. Kumar, M. Sethumadhavan, and P. P. Amritha, *Exploitation of http/2 proxies for cryptojacking*, International Symposium on Security in Computing and Communication, Springer (2020).

[12] V. S. Aparna, A. Rajan, I. Jairaj, B. Nandita, P. Madhusoodanan, Ajai A S Remya, *Implementation of aes algorithm on text and image using matlab*, 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) (2019).

Department of Mathematics, Amrita School of Engineering, Bengaluru, Amrita Vishwa Vidyapeetham, India

Email address: bl.sc.r4mat22001@bl.students.amrita.edu

Department of Mathematics, Amrita School of Engineering, Bengaluru, Amrita Vishwa Vidyapeetham, India

Email address: kn_meera@blr.amrita.edu