Encryption System Involving Matrix Associated With Semigraphs

Jyoti Shetty, Sudhakara G*, and Vinay Madhusudanan

***Abstract*—Semigraphs are a generalization of graphs, where an edge is allowed to have two or more vertices. A binomial incidence matrix is an incidence matrix of a semigraph which represents the semigraph uniquely.**

We prove that, the binomial incidence matrix of any semigraph belonging to one of two specific classes of semigraphs, is invertible. Then we note a peculiar property enjoyed by the columns of a submatrix of the adjoint of the binomial incidence matrix of semigraphs under consideration. By making use of this property, we develop an encryption system which uses invertibility of the binomial incidence matrix.

***Index Terms*—semigraph, incidence-matrix, determinant, inverse, cryptography.**

I. Introduction and Preliminaries

This article is divided into four parts. In the first part, the problem is introduced and the necessary basic definitions are given. In the second part, results which are fundamental in developing the algorithm such as the invertibility of binomial incidence matrices and their typical properties are established. The third part contains encryption and decryption algorithms and an example which demonstrates how the algorithms work. Finally, the article is concluded in the fourth part.

Concepts of Graph Theory find natural applications in most of the modern fields, including cryptography. Semigraphs, being a generalization of graphs, are also expected to be useful in all the instances where graphs are.

A. Semigraphs

In this section, we review the basic theory of semigraphs [2] that are required later in the article.

Definition I.1. *A* semigraph G *is a pair* (V, E) *where* V *is a nonempty set whose elements are called vertices of* G*, and* E *is a set of* k*-tuples of distinct vertices, called edges of* G*, for various* $k \geq 2$*, satisfying the following conditions:*

1) *Any two edges of* G *can have at most one vertex in common.*
2) *Two edges* $(a_1, a_2, \ldots, a_p)$ *and* $(b_1, b_2, \ldots, b_q)$ *are said to be equal if and only if*
   - $p = q$ *and*
   - *either* $a_i = b_i$ *for* $1 \leq i \leq p$*, or* $a_i = b_{p-i+1}$ *for* $1 \leq i \leq p$*.*

Manuscript received March 12, 2021; revised March 05, 2022.

Jyoti Shetty was a research scholar in the Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka, India, 576104 (email: jyotishetty.shetty@gmail.com).
Sudhakara G is a Professor and the Head in the Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka, India, 576104 (email: sudhakara.g@manipal.edu).
Vinay M is an Assistant Professor in the Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka, India, 576104 (email: vinay.m@manipal.edu).
*Corresponding author : Sudhakara G.

Note I.2. *Let* E *denote the set of vertices on the edge* e*. Then the number of elements in* E *is called the size of the edge* e *and is usually denoted by* $|e|$*.*

Let $G = (V, E)$ be a semigraph and let $e = (u_1, u_2, \ldots, u_k)$ be an edge of G. Then u_1 and u_k are called the *end vertices* and u_i, $2 \leq i \leq k-1$, are called the *mid vertices* of e. Two vertices of G are *adjacent* if there is an edge containing both of them. An edge is said to be *incident* on every vertex on it. Two edges of G are adjacent if they have a vertex in common. Two vertices are *consecutively adjacent* if they are consecutive on the edge containing them.

Like a graph, a semigraph G also has a geometric representation on the plane. The vertices of G are represented either by dots or by small circles according as whether they are end vertices or mid vertices of the edge containing them, and an edge of G is represented by simple curve passing through all the vertices on it. When a mid vertex v of an edge e_1 is an end vertex of another edge, say e_2, then a small tangent is drawn to the circle representing vertex v where e_2 meets v. A semigraph G and its representation are given in the following example.

Example I.3. *Let* $G = (V, E)$ *be a semigraph with* $V(G) = \{u_1, u_2, \ldots, u_9\}$ *and* $E(G) = \{e_1 = (u_1, u_2, u_3, u_6);\ e_2 = (u_1, u_9, u_4);\ e_3 = (u_4, u_5, u_6, u_7, u_8);\ e_4 = (u_3, u_9);\ e_5 = (u_1, u_8)\}$*. Then* G *can be represented as shown in Figure 1.*

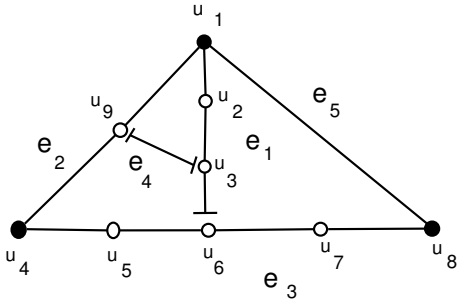

Fig. 1: Semigraph G with vertex set $\{u_1, u_2, \ldots u_8\}$ and edge set $\{e_1 = (u_1, u_2, u_3, u_6);\ e_2 = (u_1, u_9, u_4);\ e_3 = (u_4, u_5, u_6, u_7, u_8);\ e_4 = (u_3, u_9);\ e_5 = (u_1, u_8)\}$.

A *complete semigraph* is a semigraph in which every two vertices are adjacent. In addition, if every vertex is an end vertex of some edge then it is called a *strongly complete semigraph*. For example, a semigraph which consists of a single edge of size $n \geq 3$ is complete but not strongly complete and is denoted by E_n^c. The strongly complete semigraph on $n+1$ vertices with one edge of size n and all other edges of size 2 is denoted by T_n^1. Figure 2 shows the strongly complete semigraph T_5^1.

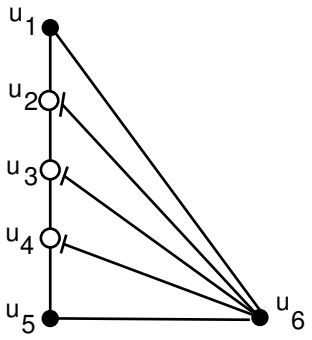

Fig. 2: Strongly complete semigraph T_5^1

Definition I.4. *A semigraph G is said to be a* zig-zag semigraph *if the vertex set $V(G) = \{u_1, u_2, \ldots, u_k, u_{k+1}, u_{k+2}, \ldots, u_{2k-1}\}$ and the edge set $E(G) = \{(u_1, u_2, \ldots, u_k), (u_1, u_{k+1}), (u_2, u_{k+1}), (u_2, u_{k+2}), \ldots, (u_{k-1}, u_{2k-2}), (u_{k-1}, u_{2k-1}), (u_k, u_{2k-1})\}$. In this article we denote it by Z_k^{k-1}. Figure 3 shows the zig-zag semigraph Z_6^5.*

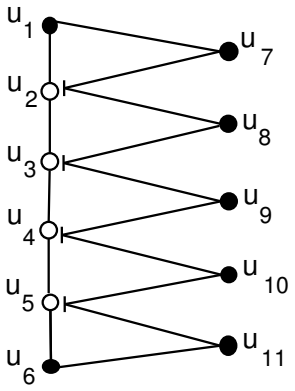

Fig. 3: Zig-zag semigraph Z_6^5

The concept of semigraphs was introduced and initially developed by E Sampathkumar [2]. Later, several authors have explored concepts such as matrix representation, domination, and graph energy in the case of semigraphs. We refer the interested readers to [4], [5], [6], [8], [11], [12], [15], [16].

B. Cryptography

A standard cryptographic system has the following components.

1) The original intelligible message or data that is fed into the encryption algorithm as input. This is called *plaintext*.
2) A transformed version of the plaintext message, called *ciphertext*, which is difficult for an unintended reader to understand. The alphabet used and the size of the ciphertext may be same as those of the plaintext or different.
3) A mathematical procedure that transforms the plaintext into ciphertext, called *encryption algorithm*. The input to this algorithm is the plaintext and a *secret key*.
4) A *decryption key* and a *decryption algorithm*, using which the ciphertext can be transformed back into the original plaintext.

A cryptographic system in which the encryption key is the same as the decryption key, the decryption algorithm is the step-by-step reversal of the encryption algorithm, and both the sender and receiver know the encryption key, is called a *symmetric* cryptographic system. Otherwise, it is an *asymmetric* cryptographic system.

In a symmetric cryptographic system, one must hide the encryption key. But in an asymmetric cryptographic system, the encryption key can be made public [3].

Applications of graph theory in cryptography can be found in the survey article [7]. Samid [3] patented an encryption method in which the key is a graph. In the article entitled "Development of public key cryptographic algorithm using matrix pattern for tele-ultrasound applications" [9], a public key cryptographic algorithm using a matrix pattern is developed. Cryptography has also gained a newfound importance due to the growing usage of cloud storage and computing, where privacy requires the usage of strong cryptographic algorithms such as the one developed in [17].

C. Matrices

We use some results from matrix theory given in [13], described below.

If A is an $n \times n$ matrix, then $\operatorname{cof} A$ will denote the sum of all cofactors of A. Note that if A is nonsingular, then

$$\operatorname{cof} A = (\det A)(\mathbf{1}' A^{-1} \mathbf{1})$$

where $\mathbf{1}$ is a all 1s vector.

Lemma I.5. *Let A be an $n \times n$ matrix. Let B be the matrix obtained from A by subtracting the first row from all the other rows and then subtracting the first column from all the other columns. Then*

$$\operatorname{cof} A = \det B(1|1)$$

where, $B(1|1)$ denotes the submatrix obtained by deleting the first row and the first column of the matrix B.

II. Binomial Incidence Matrix of a Semigraph

The incidence matrix of a semigraph, as defined by E. Sampathkumar [2], does not represent the semigraph uniquely. C. M. Deshpande, Yogeshri Gaidhani and B. P. Athawale [2], came up with a new definition of incidence matrix of a semigraph which represents the semigraph uniquely. But none of the above incidence matrices reveals the fact that $(v_1, v_2, \ldots, v_n)$ and $(v_n, v_{n-1}, \ldots, v_1)$ represent the same edge. We achieve this by making use of the property of the binomial coefficient that ${}^nC_r = {}^nC_{n-r}$.

In [4], the authors have obtained a new incidence matrix of a semigraph which not only represents a semigraph uniquely but also has the following property. The (i, j)-entry of the matrix gives information about position of the vertex u_i from either end vertex on the edge e_j and also size of the edge e_j.

The incidence matrix with binomial coefficients, called the binomial incidence matrix is defined formally as follows.

Definition II.1. *Let $G = (V, E)$ be a semigraph with $V(G) = \{u_1, u_2, \ldots, u_n\}$ and $E(G) = \{e_1, e_2, \ldots, e_m\}$. Let the size of the edge e_j be $n_j + 1$, $1 \le j \le m$. The* binomial incidence matrix *of G, denoted by $\mathscr{B}(G)$, is a $n \times m$ matrix, whose rows are indexed by the vertex set and columns are indexed by the edge set of G. The column corresponding to e_j in the binomial incidence matrix consists of entries $0, {}^{n_j}C_0, \ldots, {}^{n_j}C_{n_j}$, where nonzero entries correspond to the vertices on the edge. The entries ${}^{n_j}C_0$ and ${}^{n_j}C_{n_j}$ correspond to the end vertices of the edge e_j. The (i, j)-entry of $\mathscr{B}(G)$ is given by,*

$$b_{ij} = \begin{cases} {}^{n_j}C_r, & \begin{array}{c} u_i \text{ is incident with } e_j \text{ and is the } r^{th} \\ \text{vertex from the end vertex of } e_j \\ \text{with entry } {}^{n_j}C_0,\ 0 \le r \le n_j \end{array} \\ 0, & u_i \text{ is not incident with } e_j\ . \end{cases} \tag{1}$$

In the next two theorems, (II.2 and II.5), we show that the binomial incidence matrices of T_n^1 and Z_n^{n-1} are invertible, and find their inverses. Throughout this section,

C represents $({}^{n-1}C_0, {}^{n-1}C_1, \ldots, {}^{n-1}C_{n-1})^T$.

$\mathbf{1}_n$ represents the column vector of length n in which every entry is 1.

I_n represents the identity matrix of order n.

Theorem II.2. *Let $\{u_1, u_2, \ldots, u_n\}$ be the set of vertices of the complete semigraph E_n^c. Then inverse of $\mathscr{B}(T_n^1)$ is given by*

$$\left(\mathscr{B}(T_n^1)\right)^{-1} = \frac{1}{2^{n-1}} \begin{bmatrix} \mathbf{1}_n^T & -1 \\ W & C \end{bmatrix} \tag{2}$$

where $W = 2^{n-1} I_n - C\mathbf{1}_n^T$.

Proof: The semigraph T_n^1 has $n+1$ vertices and $n+1$ edges. Let $e_1 = (u_1, u_2, \ldots, u_n)$ and let $e_i = (u_{i-1}, u_{n+1})$, $2 \le i \le n+1$ be the $(n+1)$ edges. Then the binomial incidence matrix of T_n^1 takes the form

$$\mathscr{B}(T_n^1) = \begin{array}{c} \\ u_1 \\ u_2 \\ u_3 \\ \vdots \\ u_n \\ u_{n+1} \end{array} \begin{array}{c} \begin{array}{ccccccc} e_1 & e_2 & e_3 & e_4 & \cdots & e_n & e_{n+1} \end{array} \\ \begin{bmatrix} {}^{n-1}C_0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ {}^{n-1}C_1 & 0 & 1 & 0 & \cdots & 0 & 0 \\ {}^{n-1}C_2 & 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ {}^{n-1}C_{n-1} & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 1 & 1 & \cdots & 1 & 1 \end{bmatrix} \end{array}$$

and can be written in block form as

$$\mathscr{B}(T_n^1) = \begin{bmatrix} C & I_n \\ 0 & \mathbf{1}_n^T \end{bmatrix}.$$

Let $\mathscr{B}(i|j)$ denote the $n \times n$ submatrix of $\mathscr{B}(T_n^1)$ obtained by deleting its i^{th} row and j^{th} column. Let b_{ij} be the (i, j)-entry of $\mathscr{B}(T_n^1)$ and M_{ij} the minor of the element b_{ij}. Then, by expanding $\det \mathscr{B}(T_n^1)$ along the first column, and noting that $b_{n+1,1} = 0$, we get,

$$\det \mathscr{B}(T_n^1) = \sum_{i=1}^{n} (-1)^{i+1} b_{i1} M_{i1}.$$

We show that $M_{i1} = (-1)^{n-i}$, $1 \le i \le n$.

Consider the matrix $\mathscr{B}(i|1)$, $1 \le i \le n$, which is a square matrix of order n. Subtracting the sum of the first $(n-1)$ rows from the n^{th} row, we get a permutation matrix P_i, which becomes I_n after $(n-i)$ row-interchanges. Hence, $\det P_i = M_{i,1} = (-1)^{n-i}$, $1 \le i \le n$. This implies that $\det \mathscr{B}(T_n^1) = (-2)^{n-1}$ and hence $\mathscr{B}(T_n^1)$ is invertible.

We claim that the adjoint of $B(T_n^1)$, in block form, is

$$\operatorname{adj}(\mathscr{B}(T_n^1)) = (-1)^{n-1} \begin{bmatrix} \mathbf{1}_n^T & -1 \\ W & C \end{bmatrix}$$

where $W = 2^{n-1} I_n - C\mathbf{1}_n^T$. Then observe that

$$\begin{bmatrix} C & I_n \\ 0 & \mathbf{1}_n^T \end{bmatrix} \left(\frac{1}{2^{n-1}} \begin{bmatrix} \mathbf{1}_n^T & -1 \\ W & C \end{bmatrix} \right) = I_{n+1}.$$

The above proves that

$$\frac{1}{2^{n-1}} \begin{bmatrix} \mathbf{1}_n^T & -1 \\ W & C \end{bmatrix}$$

is the inverse of $\mathscr{B}(T_n^1)$. ■

We are interested in the particular submatrix $W = 2^{n-1} I_n - C\mathbf{1}_n^T$ of inverse of $B(T_n^1)$. In the next Note, we observe some of the properties of W that are very useful in our encryption and decryption method.

Note II.3. *1) In W, sum of the entries along i^{th} column is equal to zero, $\forall$ i.*

2) The (i, i) entry of W is given by $2^{n-1} - {}^{n-1}C_{i-1}$, $1 \le i \le n$ and the other entries of i^{th} column are $-{}^{n-1}C_0$, $-{}^{n-1}C_1$, …, $-{}^{n-1}C_{i-2}$, $-{}^{n-1}C_i$, …, $-{}^{n-1}C_{n-1}$.

3) When the column vector C is added to the i^{th} column of W,resulting column has only one non zero entry (equal to 2^{n-1}) which is in the i^{th} row. This can be used to determine the column of W under consideration.

The following example illustrates $\mathscr{B}(T_4^1)$, its inverse and the properties given in Note II.3.

Example II.4. *Consider T_4^1.*

The binomial incidence matrix of T_4^1 is as follows.

$$\mathscr{B}(T_4^1) = \begin{array}{c} \\ u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \end{array} \begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 3 & 0 & 1 & 0 & 0 \\ 3 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix} \end{array}.$$

Clearly, $\det \mathscr{B}(T_4^1) = (-2)^3$, *and*

$$(\mathscr{B}(\mathbf{T_4^1}))^{-1} = \tfrac{1}{8} \begin{bmatrix} 1 & 1 & 1 & 1 & -1 \\ 7 & -1 & -1 & -1 & 1 \\ -3 & 5 & -3 & -3 & 3 \\ -3 & -3 & 5 & -3 & 3 \\ -1 & -1 & -1 & 7 & 1 \end{bmatrix}$$

where,

$$W = \begin{bmatrix} 7 & -1 & -1 & -1 \\ -3 & 5 & -3 & -3 \\ -3 & -3 & 5 & -3 \\ -1 & -1 & -1 & 7 \end{bmatrix}.$$

Theorem II.5. *Let $\{u_1, u_2, \ldots, u_{2n-1}\}$ be the set of vertices of the complete semigraph Z_n^{n-1}. Then inverse of $\mathscr{B}(Z_n^{n-1})$ is given by*

$$(\mathscr{B}(Z_n^{n-1}))^{-1} = \frac{1}{2^{n-1}} \begin{bmatrix} \mathbf{1}_n^T & -\mathbf{1}_{n-1}^T \\ X & -XP_0 \\ -X & XL_0 \end{bmatrix} \tag{3}$$

where X is a $(n-1) \times n$ matrix $[x_1, x_2, \ldots, x_n]$, where $x_1 = \sum_{j=1}^{n-1} \left[\sum_{k=j}^{n-1} {}^{n-1}C_k(\gamma_j) \right]$, $x_{k+1} = x_1 - (2)^{n-1} \left(\sum_{j=1}^{k} \gamma_j \right)$, $1 \leq k \leq n-1$ *with γ_j denoting the j^{th} column of the $(n-1 \times n-1)$ identity matrix, and* $L_0 = \begin{bmatrix} I_{n-1} \\ \mathbf{0}_{1\times n-1} \end{bmatrix}$, $P_0 = \begin{bmatrix} \mathbf{0}_{1\times n-1} \\ I_{n-1} \end{bmatrix}$.

Proof: The semigraph Z_n^{n-1} has $(2n-1)$ vertices $u_1, u_2, \ldots, u_n, u_{n+1}, u_{n+2}, \ldots, u_{2n-1}$ and $(2n-1)$ edges given by, $e_1 = (u_1, u_2, \ldots, u_n)$, $e_i = (u_{n+i-1}, u_{i-1})$ and $e_i' = (u_{n+i-1}, u_i)$, $2 \leq i \leq n$.

The binomial incidence matrix of Z_n^{n-1}, $\mathscr{B}(Z_n^{n-1})$ is

$\mathscr{B}(Z_n^{n-1}) =$

$$\begin{array}{c} \\ u_1 \\ u_2 \\ u_3 \\ \vdots \\ u_{n-1} \\ u_n \\ u_{n+1} \\ u_{n+2} \\ \vdots \\ u_{2n-1} \end{array} \begin{array}{c} \begin{array}{ccccccccc} e_1 & e_2 & e_3 & \cdots & e_n & e_2' & e_3' & \cdots & e_n' \end{array} \\ \left[\begin{array}{ccccc|ccccc} {}^{n-1}C_0 & & & & & 0 & 0 & \cdots & 0 \\ {}^{n-1}C_1 & & & & & & & & \\ {}^{n-1}C_2 & & I_{n-1} & & & & & & \\ \vdots & & & & & & I_{n-1} & & \\ {}^{n-1}C_{n-1} & & & & & & & & \\ {}^{n-1}C_{n-1} & 0 & 0 & \cdots & 0 & & & & \\ 0 & & & & & & & & \\ 0 & & & & & & & & \\ \vdots & & I_{n-1} & & & & I_{n-1} & & \\ 0 & & & & & & & & \end{array}\right] \end{array}.$$

and $\mathscr{B}(Z_n^{n-1})$ has block form

$$\mathscr{B}(Z_n^{n-1}) = \begin{bmatrix} C & L_0 & P_0 \\ O & I_{n-1} & I_{n-1} \end{bmatrix}$$

where $L_0 = \begin{bmatrix} I_{n-1} \\ \mathbf{0}_{1\times n-1} \end{bmatrix}$, $P_0 = \begin{bmatrix} \mathbf{0}_{1\times n-1} \\ I_{n-1} \end{bmatrix}$.

Let b_{ij}' be the (i,j)-entry of $\mathscr{B}(Z_n^{n-1})$ and M_{ij}' the minor of the element b_{ij}'. By expanding $\det \mathscr{B}(Z_n^{n-1})$ along the first column and observing that $b_{i1}' = 0$, for all i with $n+1 \leq i \leq 2n-1$, we get

$$\det \mathscr{B}(Z_n^{n-1}) = \sum_{i=1}^{n} (-1)^{i+1} b_{i1}' M_{i1}'.$$

We have $M_{i1}' = \det \mathscr{B}(i|1) = \begin{vmatrix} A & B \\ E & D \end{vmatrix}$ where A, B, E, and D are blocks of order $(n-1 \times n-1)$, and E and D are identity matrices.

We have $M_{i1}' = \det \mathscr{B}(i|1) = \det(AD - BE) = \det(A - B)$. Observe that, $A - B$ is a lower triangular matrix with $n-i$ entries equal to -1 and $i-1$ entries equal to $+1$. Hence, $M_{i1} = (-1)^{n-i}$. Then $\det \mathscr{B}(Z_n^{n-1})$ becomes $(-2)^{n-1}$. Thus $\mathscr{B}(Z_n^{n-1})$ is invertible.

We proceed to find the inverse of $\mathscr{B}(Z_n^{n-1})$. We claim that the adjoint of $\mathscr{B}(Z_n^{n-1})$, in block form, is

$$\operatorname{adj}(\mathscr{B}(Z_n^{n-1})) = (-1)^{n-1} \begin{bmatrix} \mathbf{1}_n^T & -\mathbf{1}_{n-1}^T \\ X & -XP_0 \\ -X & XL_0 \end{bmatrix}$$

where X is the $(n-1) \times n$ matrix $\begin{bmatrix} x_1 & x_2 & \ldots & x_n \end{bmatrix}$, with $x_1 = \sum_{j=1}^{n-1} \left(\sum_{k=j}^{n-1} [{}^{n-1}C_k]\gamma_j \right)$, $x_{k+1} = x_1 - (2)^{n-1} \left(\sum_{j=1}^{k} \gamma_j \right)$ $1 \leq k \leq n-1$, where γ_j denotes the j^{th} column of the $(n-1 \times n-1)$ identity matrix.

Observe that

$$\begin{bmatrix} C & L_0 & P_0 \\ 0 & I_{n-1} & I_{n-1} \end{bmatrix} \left(\frac{1}{2^{n-1}} \begin{bmatrix} \mathbf{1}_n^T & -\mathbf{1}_{n-1}^T \\ X & -XP_0 \\ -X & XL_0 \end{bmatrix} \right) = I_{2n-1}$$

which proves that

$$\frac{1}{2^{n-1}} \begin{bmatrix} \mathbf{1}_n^T & -\mathbf{1}_{n-1}^T \\ X & -XP_0 \\ -X & XL_0 \end{bmatrix}$$

is the inverse of $\mathscr{B}(Z_n^{n-1})$. ■

Before proceeding to the example, we make a note of some properties of the $2(n-1) \times n$ matrix $\begin{bmatrix} X \\ -X \end{bmatrix}$, which is a submatrix of the inverse of $\mathscr{B}(Z_n^{n-1})$.

Note II.6. *1) In $\begin{bmatrix} X \\ -X \end{bmatrix}$, the sum of the entries of each column is zero.*

2) In X, the i^{th} column has exactly $(i-1)$ negative entries, for $1 \leq i \leq n$.

This helps in identifying the position of the column of X under consideration.

The following example illustrates the $\mathscr{B}(Z_4^3))^{-1}$ and the properties given in Note II.6.

Example II.7. *Consider Z_4^3.*

The binomial incidence matrix of Z_4^3 is

$$\mathscr{B}(Z_4^3) = \begin{array}{c} \\ u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ u_6 \\ u_7 \end{array} \begin{array}{c} \begin{array}{ccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 1 & 0 & 1 & 0 & 0 \\ 3 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \end{array}.$$

Clearly, $\det \mathscr{B}(Z_4^3) = (-2)^3$, *and*

$$(\mathscr{B}(Z_4^3))^{-1} = \frac{1}{8} \left[\begin{array}{cccc|ccc} 1 & 1 & 1 & 1 & -1 & -1 & -1 \\ \hline 7 & -1 & -1 & -1 & -1 & 1 & 1 \\ 4 & 4 & -4 & -4 & -4 & 4 & 4 \\ 1 & 1 & 1 & -7 & -1 & -1 & 7 \\ -7 & 1 & 1 & 1 & 7 & -1 & -1 \\ -4 & -4 & 4 & 4 & 4 & 4 & -4 \\ -1 & -1 & -1 & 7 & 1 & 1 & 1 \end{array}\right]$$

where $X = \begin{bmatrix} 7 & -1 & -1 & -1 \\ 4 & 4 & -4 & -4 \\ 1 & 1 & 1 & -7 \end{bmatrix}$, $L_0 = \begin{bmatrix} I_{n-1} \\ \mathbf{0}_{1\times n-1} \end{bmatrix}$, *and* $P_0 = \begin{bmatrix} \mathbf{0}_{1\times n-1} \\ I_{n-1} \end{bmatrix}$.

III. Encryption Scheme using Binomial Incidence Matrix associated with a Semigraph

Invertibility of matrices is very effectively used in the case of Hill Cipher encryption. In the method of encryption and decryption that we develop, we consider the invertibility of binomial incidence matrix of semigraphs. The binomial incidence matrix of a semigraph G is of order $n \times m$, where n is the number of vertices and m is the number of edges in G, and the entries along any column are binomial coefficients (Definition II.1). For our purpose, we have chosen the semigraphs E_n^c and Z_n^{n-1}, both of which are invertible for all values of n.

We observe that the matrix W (as defined in (2)) and the matrix $\begin{bmatrix} X \\ -X \end{bmatrix}$ (as defined in (3)), both have the property that the sum of the entries along any column is equal to zero. This special property is extensively used in both encryption and decryption in the method we propose. The plaintext, which is assumed to be a sequence of letters from the English alphabet, is divided into groups of three consecutive letters starting from the leftmost letter of the sequence. These groups are called *trigraphs*. Each letter in the trigraph is encrypted by a column of either W or $\begin{bmatrix} X \\ -X \end{bmatrix}$ according to whether the letter is one of the first thirteen letters or one of the last thirteen letters, respectively, of the English alphabet.

Both the matrices W and $\begin{bmatrix} X \\ -X \end{bmatrix}$ are sufficiently large, having several columns. So, three columns can be chosen to represent three letters in the trigraph in several different ways. The information, about which three columns are used in the encryption system, is given as the first three digits in the secret key.

In this encryption method, a plaintext will be converted into a sequence of positive and negative integers where each letter in the plaintext corresponds to a sequence, the sum of the entries of which is equal to zero. So, while deciphering, we always start from the left and choose the first r (say) integers, the sum of which equals zero.

To further strengthen the algorithm, we add the following two steps:

1) Once the letters in any trigraph are encrypted as three sequences, we permute the sub sequences in one of the six possible permutations. By Notes II.3 and II.6, using the first three digits of the secret key, the receiver can decipher the sequence in the correct order.
2) The fourth letter n_4 in the secret key represents $N = \operatorname{cof} A$, where A is the binomial incidence matrix of the semigraph that is associated with n_4 by the encryption scheme. We add N to every element in the sequence representing the message. This prevents any unintended reader from discovering the pattern of the string of numbers adding up to zero.

Key Generation:

The secret key in our method consists of an association of semigraphs, taken from two particular classes of semigraphs, to the letters of the English alphabet, and a sequence $s = (n_1, n_2, n_3, n_4)$ of positive integers satisfying the following conditions.

1) n_1, n_2, and n_3 are three positive integers indicating the position of the column to be selected corresponding to the letters l_1, l_2, and l_3 of any trigraph, respectively.
2) $1 \le n_1, n_2, n_3 \le \min \left\{ \begin{matrix} \text{min. no. of columns in } W, \\ \text{min. no. of columns in } \begin{bmatrix} X \\ -X \end{bmatrix} \end{matrix} \right\}$.
3) $1 \le n_4 \le 26$.

In the following encryption and decryption procedures, we consider the plaintext to be a sequence of English letters written as trigraphs. The encryption function f converts a plaintext message into ciphertext in the following steps.

★ **Step 1.** To each letter in the plaintext, associate a semigraph as follows. If the letter is in the i^{th} position in the English alphabet and if $1 \le i \le 13$, then the associated semigraph is T^1_{i+2} and if the letter is in the j^{th} position, where $14 \le j \le 26$, then the associated semigraph is Z^{j-12}_{j-11}.

★ **Step 2.** Consider the binomial incidence matrix $\mathscr{B}(G)$ and its adjoint.

★ **Step 3.** Consider the submatrix W of the adjoint if the letter is one of the first 13 letters or the submatrix $\begin{bmatrix} X \\ -X \end{bmatrix}$ of the adjoint if the letter is one of the last 13 letters in the English alphabet.

★ **Step 4.** Let $l_1 l_2 l_3$ be any trigraph. Then the sequence associated to the letter in the trigraph is given by the $n_1{}^{\text{th}}$, $n_2{}^{\text{th}}$, and $n_3{}^{\text{th}}$ columns of either W or $\begin{bmatrix} X \\ -X \end{bmatrix}$ according to whether $1 \le l_i \le 13$ or $14 \le l_i \le 26$, respectively, where n_1, n_2 and n_3 are the 1^{st} three digits in the secret key.

★ **Step 5.** Let $N = \operatorname{cof} \mathscr{B}(S)$, where $\mathscr{B}(S)$ is the binomial incidence matrix of the semigraph S which is associated with n_4 by the encryption scheme, where n_4 is the 4^{th} digit in the secret key. Add N to each entry of the sequence, starting from the 5^{th} entry.

★ **Step 6.** First, arrange the sequences corresponding to the letters in the same order as they appear in the plaintext and respective trigraph. Then, to each trigraph, apply a random permutation of the sequences associated with the letters inside the trigraph.

Note III.1. *After dividing into trigraphs, if one or two letters are left out in the plaintext, they are also represented by the $n_1{}^{th}$ column or the $n_1{}^{th}$ and $n_2{}^{th}$ columns of either the matrix W or $\begin{bmatrix} X \\ -X \end{bmatrix}$, accordingly.*

Now, the ciphertext contains a sequence and it is not true that sum of some r consecutive elements is equal to zero.

The encrypted message, in the above method, is a sequence of integers. The first four integers constitute a secret key where the first three integers n_1, n_2, and n_3, inform the column numbers corresponding to the 1^{st}, 2^{nd} and 3^{rd} letters in any trigraph. The fourth integer n_4 gives information about the integer $N = \operatorname{cof} \mathscr{B}(S)$ where S is the semigraph associated with n_4 by the encryption function. The deciphering procedure is explained below.

⧫ **Step 1.** The receiver gets the encrypted message in the form of a sequence. First, consider the 1^{st} four integers, say, n_1, n_2, n_3, n_4, which is the secret key. The integer n_4 is the most important one, using which the receiver gets the semigraph to be considered. In fact, the semigraph, say S, is the one which is associated with n_4 by the encryption function. Next, compute $N = \operatorname{cof} \mathscr{B}(S)$. Then subtract N from every entry in the encrypted text, starting from 5^{th} entry.

⧫ **Step 2.** Now consider the sequence starting from the 5^{th} entry in the encrypted sequence. Add the consecutive entries, one by one, till the sum obtained equals zero for the first time. That corresponds to one letter of the

first trigraph. Continue this procedure, starting from the first entry after the sum zero. The three letters obtained correspond to the first trigraph.

- **Step 3.** For each sequence in the trigraph, there are two possibilities. The sequence may contain one positive entry, and all other entries are negative, where the sum of negative entries equals to, in magnitude, to the positive entry. In this case, the sequence corresponds to a column of the submatrix W. To this column vector, add the vector $({}^{n-1}C_0, {}^{n-1}C_1, \ldots, {}^{n-1}C_{n-1})^T$ (when W is of order n). If the only nonzero entry in the sequence is in the $n_i{}^{\text{th}}$ position, then the letter corresponds to position i in the trigraph, $1 \leq i \leq 3$. The other possible type of sequence is one in which entries in the second half are negatives of the entries in the first half. In this case, the sequence corresponds to a column of the matrix $\begin{bmatrix} X \\ -X \end{bmatrix}$ and the letter is in the j^{th} position of the trigraph, if X is the part containing $(n_j - 1)$ negative entries. Thus the receiver can get the correct trigraph.
- **Step 4.** Now, if the sequence corresponding to a letter in the trigraph is a column of W and it is of length k, then it is the $(k-2)^{\text{th}}$ letter in the English alphabet. On the other hand, if the sequence is a column of $\begin{bmatrix} X \\ -X \end{bmatrix}$ and is of length $2k$ then it is the $(12+k)^{\text{th}}$ letter in the English alphabet.
- **Step 5.** Repeat the Steps 2, 3, and 4 for the immediate next trigraph, starting from the immediate next letter. Continue until all the sequences in the encrypted message are deciphered. This gives the actual message.

Example III.2. *In the following example we take the plaintext "CAP IS HIGH".*

We consider the first trigraph "CAP" of the plaintext and illustrate how it is encrypted and decrypted using the proposed encryption system.

As secret key we use $n_1 = 1$, $n_2 = 2$, $n_3 = 3$, $n_4 = 1$.

Encryption:

1) The characters of the considered trigraph are associated with the semigraphs T_5^1, T_3^1 and Z_5^4, respectively, which are shown in Figure 4.

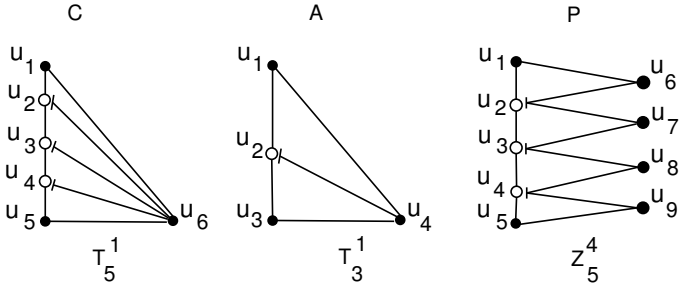

Fig. 4: semigraphs associated with first trigraph

2) The binomial incidence matrices of the above three semigraphs are as follows.

$$\mathscr{B}(T_5^1) = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 4 & 0 & 1 & 0 & 0 & 0 \\ 6 & 0 & 0 & 1 & 0 & 0 \\ 4 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\mathscr{B}(T_3^1) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

$$\mathscr{B}(Z_5^4) = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 6 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 4 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Their inverses are given below.

$$(\mathscr{B}(T_5^1))^{-1} = \frac{1}{16}\left[\begin{array}{ccccc|c} 1 & 1 & 1 & 1 & 1 & -1 \\ \hline 15 & -1 & -1 & -1 & -1 & 1 \\ -4 & 12 & -4 & -4 & -4 & 4 \\ -6 & -6 & 10 & -6 & -6 & 6 \\ -4 & -4 & -4 & 12 & -4 & 4 \\ -1 & -1 & -1 & -1 & 15 & 1 \end{array}\right]$$

$$(\mathscr{B}(T_3^1))^{-1} = \frac{1}{4}\left[\begin{array}{ccc|c} 1 & 1 & 1 & -1 \\ \hline 3 & -1 & -1 & 1 \\ -2 & 2 & -2 & 2 \\ -1 & -1 & 3 & 1 \end{array}\right]$$

$$(\mathscr{B}(Z_5^4))^{-1} =$$

$$\frac{1}{16}\left[\begin{array}{ccccc|cccc} 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ \hline 15 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ 11 & 11 & -5 & -5 & -5 & -11 & 5 & 5 & 5 \\ 5 & 5 & 5 & -11 & -11 & -5 & -5 & 11 & 11 \\ 1 & 1 & 1 & 1 & -15 & -1 & -1 & -1 & 15 \\ -15 & 1 & 1 & 1 & 1 & 15 & -1 & -1 & -1 \\ -11 & -11 & 5 & 5 & 5 & 11 & 11 & -5 & -5 \\ -5 & -5 & -5 & 11 & 11 & 5 & 5 & 5 & -11 \\ -1 & -1 & -1 & -1 & 15 & 1 & 1 & 1 & 1 \end{array}\right]$$

3)

$$W_C = \begin{bmatrix} \mathbf{15} & -1 & -1 & -1 & -1 \\ \mathbf{-4} & 12 & -4 & -4 & -4 \\ \mathbf{-6} & -6 & 10 & -6 & -6 \\ \mathbf{-4} & -4 & -4 & 12 & -4 \\ \mathbf{-1} & -1 & -1 & -1 & 15 \end{bmatrix}$$

$$W_A = \begin{bmatrix} 3 & \mathbf{-1} & -1 \\ -2 & \mathbf{2} & -2 \\ -1 & \mathbf{-1} & 3 \end{bmatrix}$$

$$\begin{bmatrix} X \\ -X \end{bmatrix}_P = \left[\begin{array}{ccccc} 15 & -1 & \mathbf{-1} & -1 & -1 \\ 11 & 11 & \mathbf{-5} & -5 & -5 \\ 5 & 5 & \mathbf{5} & -11 & -11 \\ 1 & 1 & \mathbf{1} & 1 & -15 \\ \hline -15 & 1 & \mathbf{1} & 1 & 1 \\ -11 & -11 & \mathbf{5} & 5 & 5 \\ -5 & -5 & \mathbf{-5} & 11 & 11 \\ -1 & -1 & \mathbf{-1} & -1 & 15 \end{array}\right].$$

4) *The trigraph is "CAP". Now associate the first column of W_C to C, the second column of W_A to A, and the third column of $\begin{bmatrix} X \\ -X \end{bmatrix}_P$ to P. We get the sequence to be*

$$15, -4, -6, -4, -1, -1, 2, -1, -1, -5, 5, 1, 1, 5, -5, -1.$$

5) *The fourth digit of the secret key is $n_4 = 1$. Computing $N = \operatorname{cof} \mathscr{B}(T_3^1)$ as explained in Lemma I.5, $N = \operatorname{cof} \mathscr{B}(T_3^1) = 6$.*
Adding $N = \operatorname{cof} \mathscr{B}(T_3^1)$, i.e. 6, to each entry of the above resulted sequence we have,

$$21, 2, 0, 2, 5, 5, 8, 5, 5, 1, 11, 7, 7, 11, 1, 5.$$

6) *Introducing the secret key in the beginning of the sequence and shuffling within the trigraph limit, the ciphertext is*

$$1, 2, 1, 1, 5, 8, 5, 5, 1, 11, 7, 7, 11, 1, 5, 21, 2, 0, 2, 5.$$

Decryption:

Consider the ciphertext of the first trigraph with the secret key attached to it,

$$1, 2, 1, 1, 5, 8, 5, 5, 1, 11, 7, 7, 11, 1, 5, 21, 2, 0, 2, 5.$$

1) *Clearly, $n_1 = 1$, $n_2 = 2$ and $n_3 = 1$.*
The fourth digit in the secret key, i.e. $n_4 = 1$, represents the semigraph associated with the first letter in the English alphabet, i.e. A. So, $N = \operatorname{cof} \mathscr{B}(T_3^1) = 6$.
Subtracting $\operatorname{cof} \mathscr{B}(T_3^1)$, i.e., 6 from each entry after 4^{th} entry of the sequence, we get,

$$1, 2, 1, 1, -1, 2, -1, -1, -5, 5,$$
$$1, 1, 5, -5 - 1, 15, -4, -6, -4, -1.$$

2) *Start with the fifth entry from the left most position, go on adding the consecutive entries, one by one, until the sum becomes equal to zero for the first time. Continue the procedure to cover all the entries of the sequence.*

$$(-1, 2, -1)(-1, -5, 5, 1, 1, 5, -5 - 1)$$
$$(15, -4, -6, -4, -1).$$

3) *Consider, $-1, 2, -1$.*
   a) *The sequence has one positive integer and all other entries negative. Hence the underlying submatrix is W.*
   b) *The sequence is of length $k = 3 \implies (k-2)^{th}$ letter in the English alphabet i.e., A.*
   c) *Add the vector $({}^2C_0, {}^2C_1, {}^2C_2)^T$ to $(-1, 2, -1)^T$. The resulting sequence $(0, 2^2, 0)$ has only one nonzero element, which is in the second position.*
   d) *Hence A is the second character of the trigraph.*

   Consider, $-1, -5, 5, 1, 1, 5, -5 - 1$.
   a) *The second half of the sequence is numerically the same as the first half of the sequence but opposite in sign, and hence the underlying submatrix is $\begin{bmatrix} X \\ -X \end{bmatrix}$.*
   b) *The sequenc is of length $2k = 8 \implies (12 + k)^{th}$ letter in the English alphabet i.e 16^{th} letter, i.e., P.*
   c) *In $\begin{bmatrix} X \\ -X \end{bmatrix}$, the part X has two negative entries.*
   d) *Hence, P is the third character of the trigraph.*

   Consider, $15, -4, -6, -4, -1$
   a) *The sequence have one positive integer and all other integers negative, and hence the underlying submatrix is W.*
   b) *The sequence is of length $k = 5 \implies (k-2)^{th}$ letter in the English alphabet i.e C.*
   c) *Add the vector $({}^4C_0, {}^4C_1, {}^4C_2, {}^4C_3, {}^4C_4)^T$ to $(15, -4, -6, -4, -1)^T$. The resulting sequence $(2^4, 0, 0, 0, 0)$ has only one nonzero element, which is in first position.*
   d) *Hence C is the first character of the trigraph.*

   Therefore the trigraph is"CAP".

Note III.3. *1) At this juncture, we want to emphasize on the following point. Since security or confidentiality is the main goal of the above development, other aspects like computational complexity are not considered to be too important.*

2) To add further randomness in the procedure of encryption, we suggest the following modification. In the procedure given above, the 26 letters of the English alphabet are mapped to the semigraphs (either Z_n^{n-1} or T_n^1) as follows. For the n^{th} letter, the semigraph associated is T_1^n if $1 \le n \le 13$ and Z_{n-1}^n if $14 \le n \le 26$. Instead, select a collection of 26 graphs G_i, $1 \le i \le 26$ at random, where each G_i is either Z_n^{n-1} or T_n^1 for some n. This defines a bijection f from the letters of the English alphabet to the collection of semigraphs $\{G_1, \ldots, G_{26}\}$. Add this function f to the secret key and share it with the receiver. The advantage is that an unintended reader, without knowing f, can never decipher the encrypted message.

IV. Conclusions

This is a symmetric encryption system where both the sender and the receiver are supposed to know both the methods of encryption as well as decryption. The secret key is exchanged between them periodically, possibly with several changes. We assumed here that the message is a sequence of English alphabets, without any punctuation marks. In a situation where these symbols appear in the message, the same algorithm can be used by considering a few more semigraphs corresponding to those symbols.

There is a very large member of options for associating the semigraphs to characters. The information about which semigraph is associated with which symbol is to be shared between the sender and the receiver, and the association can be changed periodically.

Moreover, the indices of the columns of either W or $\begin{bmatrix} X \\ -X \end{bmatrix}$ used to represent the letters in the message can be changed periodically, and it is the first part of the secret key shared between sender and receiver.

The sequence corresponding to a letter, say S, in the k^{th} position of the trigraph is different from the sequence corresponding to the same letter S in the r^{th} position of the trigraph, when $k \neq r$.

As decryption depends on information about the semigraphs, or correspondingly their binomial incidence matrices, their inverses, and the sum of the entries in these inverses, we believe that it is difficult for a third party to decipher the encrypted message.

REFERENCES

[1] C. Boyd, and Mathuria, *A Protocols for Authentication and Key Establishment*. Vol. 1, Heidelberg: Springer, 2003.

[2] E. Sampathkumar, C. M. Deshpande, B. Y. Bam, L. Pushpalatha and V. Swaminathan, *Semigraphs and their applications*, 1st ed., India: Academy of Discrete Mathematics and Applications, 2019.

[3] G. Samid, *Denial cryptography based on graph theory*, U.S. Patent 6,823,068, 2004.

[4] J. Shetty and G. Sudhakara,"Binomial incidence matrix of a semigraph", *Discrete Mathematics, Algorithms and Applications,* pp. 2150017, 2020.

[5] J. Shetty, G. Sudhakara and M. Vinay, "On the existence of semigraphs and complete semigraphs with given parameters," *Ain Shams Engineering Journal https://doi.org/10.1016/j.asej.2021.04.002,* 2021.

[6] J. Shetty, K. Arathi Bhat and G. Sudhakara, "Addition Operation in Semigraphs", *Applied Mathematics E Notes*, 2021 (accepted).

[7] P. L. K. Priyadarsini, "A survey on some applications of graph theory in cryptography," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 18, no. 3, pp. 209-217, 2015.

[8] S. Gomathi, R. Sundareswaran, and V. Swaminathan, "(m, e)-domination in semigraphs," *Electronic Notes in Discrete Mathematics,* vol. 33, pp. 75-80, 2009.

[9] S. H. Shin, W. S. Yoo, and H. Choi, "Development of public key cryptographic algorithm using matrix pattern for tele-ultrasound applications," *Mathematics,* vol. 7, no. 8, pp. 752-752, 2019.

[10] S. S. Kamath and R. S. Bhat, "Domination in semigraphs," *Electronic Notes in Discrete Mathematics,* vol. 15, pp. 106-111, 2003.

[11] S. S. Kamath and S. R. Hebbar, "Strong and weak domination, full sets and domination balance in semigraphs," *Electronic Notes in Discrete Mathematics,* vol. 15, pp. 112-112, 2003.

[12] S. S. Kamath, and S. R. Hebbar, "Domination critical semigraphs," *Electronic Notes in Discrete Mathematics,* vol. 15, pp. 113-113, 2003.

[13] R. B. Bapat, *Graphs and Matrices*, 2nd ed. London :Springer, 2010.

[14] W. Stallings, *Cryptography and Network Security*, 4/E. India: Pearson Education, 2006.

[15] Y. S. Gaidhani, C.M. Deshpande, and B. P. Athawale, "Adjacency matrix of a semigraph," *Electronic Notes in Discrete Mathematics*, vol. 63, pp. 399-406, 2017.

[16] Y. S. Gaidhani, C. M. Deshpande, and S. Pirzada, "Energy of a semigraph," *AKCE International Journal of Graphs and Combinatorics*, vol. 16, no. 1, pp. 41-49, 2019.

[17] Z. Kartit and M. E. Marraki, "Applying Encryption Algorithm to Enhance Data Security in Cloud Storage," *Engineering Letters*, vol. 23, no. 4, pp. 277-282, 2015.

Jyoti Shetty received her B.Sc. from Karnataka University, Dharwad, India, in 2009 and M.Sc. degree in Mathematics from Mangalore University, Mangalore, India, in 2013. She then received her Ph.D. from Manipal Academy of Higher Education, Manipal, in 2021. This author became a Member (M) of IAENG in 2020.

Sudhakara G. received his B.Sc. and M.Sc. degrees in Mathematics from Mangalore University, Mangalore, India, in 1984 and 1986, respectively. He is a Professor and Head of the Department of Mathematics, Manipal Institute of Technology, Manipal, India, where he is working as a faculty in the department since 1987. His research interests include Graph Theory, Combinatorics, and Number theory.

Vinay Madhusudanan received his M.Sc. degree in Applied Mathematics and Computing from Manipal Institute of Technology, Manipal, India, and is an Assistant Professor at the Department of Mathematics, Manipal Institute of Technology, Manipal, India, since 2011. He is pursuing his Ph.D. under the guidance of Dr. Sudhakara G. His research interests include Algebra, Graph Theory, and Combinatorics.