International Journal of Applied Mathematics

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

GRAPH THEORY REVOLUTIONIZES MATRIX REPRESENTATION IN ENCRYPTION AND DECRYPTION USING ALPHANUMERIC SERIES

P. Divya [1] , Prof. Dr. R. Nagarathinam [2]

[1] P.Divya - Dr. M.G.R Educational and Research Institute

Maduravoyal, Chennai - 600095.

e-mail: divya.math@drmgrdu.ac.in

(or)

divyaparanthaman1997@gmail.com

[2] Prof. Dr. R. Nagarathinam - Dr. M.G.R Educational and Research Institute

Maduravoyal, Chennai - 600095.

e-mail: nagarathinam.hs@drmgrdu.ac.in

Abstract

This study introduces a groundbreaking method that merges graph theory with cryptographic techniques to develop an innovative encryption and decryption algorithm through key generation. The combination of cryptography and graph theory to design encryption and decryption algorithms involves several structured steps. This provided security and computational effectiveness. In this approach, the confidential information of three people was transformed into numerical objects in a graph. These objects are often vertices and edges, which are linked to form certain types of graphs such as complete graphs or Hamiltonian graphs. These graphs form the foundation for constructing adjacency matrices or other algebraic representations, wherein the underlying information is concealed through weights or unique graph labels. This key makes it possible to safely manipulate patterns and guarantees that the encryption may only be inverted if one is in possession of the key. For example, to encrypt information, the algorithm can transform text characters into numbers, incorporate them into the weights or structure of the graph, and alter the adjacency matrix through algebraic operations based on the secret key. The decrypted data resemble an altered graph or a sophisticated matrix that is not easily understandable unless the key is present. During decryption, the reverse occurs, and the encrypted matrix or graph goes through the inverse of the operations based on the key, gradually rebuilding the graph and then extracting the original characters or data. The system is secure because it is difficult for any intruder to re-establish the same connections between the original data and its graph-based encryption without a key. The application of graph-theoretic techniques provides strong security against typical attacks such as frequency analysis, brute force, and structural inference. This is because the patterns involved in the underlying mechanisms are heavily dependent on the secret structure and the transformations applied. The technique can also be used to protect different types of personal or digital information in a flexible way, laying a sound basis for

Received: August 12, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

practical and effective multi-person secure communication. Now a days the Security is one of the important challenges to secure the data. This research paper discusses graph theory in matrices, using the key generation from this methodology, which can be applied to both encryption and decryption approaches. Even without knowing the key value, the third -eye person is not easier to access. The key emerges through complex derivation from multiple matrix types which serve as foundational elements in graph theory. Unauthorized individuals find themselves unable to access confidential messages or personal information due to the algorithm's design which makes it highly resilient against cyber-attacks.

Math. Subject Classification: ...

Key Words and Phrases: Graph theory, Adjacency matrix, Incident matrix, Alphanumeric, Cryptography, Encryption, Decryption.

1 Introduction

1.1 Graph theory

The beginning of graph theory is often linked to the work of the 18th century mathematician Leonhard Euler. He is a mathematician, physicist, astronomer, engineer, etc.; he found the great solution for the famous Seven Bridges of Konigsberg problem in the year 1736. He is one first inverted the graph theory using the Seven Bridges of Konigsberg problem. Crossing the seven bridges is done one time; don't cross any bridge twice laid. A graph (V, E) contains the vertices V and edges E. Two vertices are connected by the line, which is an edge. From that starting point, so many graphs are established, e.g., directed, undirected, weighted graphs, etc. Some applications of graph theory are applied for various fields of application of graph theory, which play a crucial vital role in computer science, social science, architecture, natural science, pharmaceutical science, etc. The next one is the matrix representation of graph theory, which is most widely used in the adjacency matrix and incidence matrix. And also, some matrices are there, like path matrix, circuit matrix, cut-set matrix, etc.

1.2 Background and Motivation :-

The nexus between cryptography and graph theory represents a paradigm shift in the design and analysis of secure systems for traditional and new digital realms. With global threats to confidential data and services increasing in scope and complexity, from Internet bank fraud to cyber-attacks against critical infrastructure, tradtional models of security are becoming increasingly evident. Traditional cryptography techniques tend to fail to reflect the dynamic interlinking of contemporary digital systems. In response, graph theory offers a strong abstraction that models entities and relations with great power, enabling researchers and engineers to analyze, design, and optimize security mechanisms with more accuracy. The impetus for such integration revolves around some of the distinctive strengths of graph theory. First, it presents computationally intractable problems—graph isomorphism, Hamiltonian paths, and graph coloring—to form a foundation for constructing robust

Received: August 12, 2025

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

encryption schemes, authentication protocols, and zero-knowledge proofs. These issues continue to be challenging to address, even with quantum computing technologies serving as future-proof cryptographic systems against new algorithmic threats. In addition, graph-theoretic frameworks naturally capture intricate network topologies and threat diffusion, enabling sophisticated methodologies in attack graph analysis, trust modeling, and secure routing for wireless sensor networks and blockchain systems. Recent developments such as quantum-safe protocols and AI-based threat analysis attest to the malleability of graph theory in cryptographic studies. For instance, the spectral graph theory leverages graph matrix eigenvalues and eigenvectors to securely and compactly encode messages, and attack graphs enhance intrusion detection situational awareness. Hypergraphs and temporal models further allow multiagent trust dynamic and temporal system behavior to be represented, advancing the limits of what can be theoretically and practically achieved in security. Overall, the interplay between graph theory and cryptography is motivated by the demand for mathematically sound, scalable, and future-resistant solutions, which seize the richness of graph-theoretic abstractions to enhance data protection and resilience in a world of constantly shifting digital threats.

1.3 Cryptography

Cryptography is in the field of computer science for securing in- formation and confidential messages or personal information from one person to the other person. The history of cryptography spans thousands of years. It is in the secure form of the traditional day onwards. Traditional cryptography is easier for a hacker to attack. From that modern cryptography, so many new techniques, algorithms, formulas, and methods are used to make it very tough to access for unauthorized people. It is readable text formed into un- readable text; it is protected from the unknown person attacking, and the reverse process is for known persons or users. In the Greek work it is “hidden writing.” The uses are securing the online trans- actions, digital certificates and signatures, etc. There are some types of cryptography: symmetric, asymmetric, and hash function. In symmetric cryptography, in simple words, the same key for both encryption and decryption is known as private key cryptography, a basic example of which is AES and DES. Asymmetric cryptography pairs of keys are different to encrypt and decrypt and are called public key cryptography. Examples are RSA and ECC.

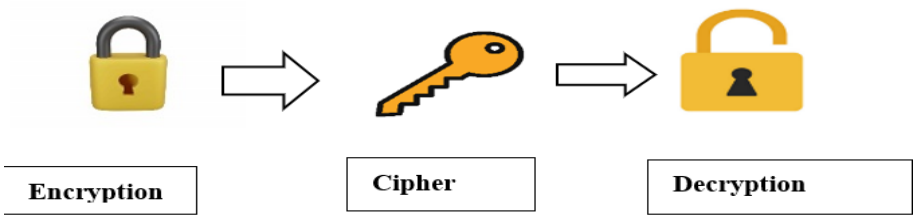
1.4 Connection in graph theory and cryptography

Graph theory is an area of research in mathematics, engineering, and computer science that focuses on the examination of graphs, which has composed of nodes connected by edges. A vital role is played by this discipline in cryptography, where data is rep- resented as graphs by encryption algorithms, thereby facilitating secure transmission and reception of messages. In cryptography having data, encryption data and decryption data. Convert the data into graph it is easy to understand instead of long text. The foundation were laid by Shannon in 1949, initially employed for military or army purpose. From the algorithm can make use of graph theory likes spanning trees, weighted graph, Hamiltonian graph etc., Furthermore, cipher can be transformed into graphs for convert communication

Received: August 12, 2025

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and many cryptographic applications make advantage of graph theory feature like connectedness. Sensitive information has been transformed into encoded for- mats for secure transmission by cryptography, a field dedicated to this purpose, which has undergone substantial evolution throughout history. The development of innovative cryptographic techniques aimed at tackling challenges such as confidentiality, privacy, authentication, password protection, digital signatures, identity verification, and electronic currency has been led by the rise of digital communication. In contemporary society, critical issues, including identity verification, digital signatures, and electronic currency, are addressed by cryptography. As protective measures advance, secure communication is continually being compromised by new methods that are identified.



2 Basic Definition

2.1) Definition 1 (Graph)**.** Let G be a graph with the vertices V and edges E. Vertices are nothing but the nodes or points, and similarly, the edges are lines. For simple understanding, the two nodes joined by the one line are called the graph.

2.2) Definition 2 (Matrix)**.** The matrix is represented in the form of a rectangular array represented by symbols, numbers, alphabets, etc., and also the arrangement of the rows and columns. A row is arranged in the horizontal direction (i.e., it goes from left to right of the matrix). A column is the arrangement of the vertical direction (i.e., it goes from top to bottom).

2.3) Definition 3 (Adjacent Matrix)**.** An adjacency matrix is a simple way to represent the graph using a square matrix. Every row and each column are represented by nodes or points. If the edge is connecting in between the two vertices. The edge and vertices are connected; the value is given by 1. If there is no connection in vertices and edges, the value is given by 0.

2.4) Definition 4 (Incident Matrix)**.** The incidence matrix is a graph representation of a matrix. It shows the columns are indi- cated by the nodes or points and the rows indicate the edges or lines. In the graph, is there any connection between the vertices and edge where the values are given as 1 or otherwise 0.

2.5) Definition 5 (Plain Text)**.** The two people are sending the message or information. Sharing the message from sender to re- ceiver. That text is called the plain text or readable text.

Received: August 12, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2.6) Definition 6 (Cipher Text)**.** The ciphertext is nothing. The readable text form is changed as the unreadable form is known as ciphertext.

2.7) Definition 7 (Encryption)**.** The readable text form, or plain text, is converted into the cipher text, which is known as encryption.

2.8) Definition 8 (Decryption)**.** The cipher text is converted into the readable form, or plain text, which is known as the decryption.

3 Preliminaries

- ✓ **Fundamental Concepts in Graph Theory**

The core concepts of graph theory create a universal language and mathematical tools to describe and reason about relational structures in any discipline. A graph G consists of a set of vertices V and a set of edges E connecting pairs of vertices, frequently with further structures represented by direction, weights, or labels. The vertices, or nodes, represent the objects of the system, and the edges represent the relationships, or interactions, between those objects. Edges may be undirected, indicating a symmetric relationship, or directed, indicating asymmetry of interaction. Weights specify a volume associated with an edge, providing the ability to make values such as cost, distance, or capacity. Degrees of vertices clarify the involvement of a vertex in a graph, where the degree of a vertex in an undirected graph is the number of incident edges, and for directed graphs the degree is the sum of the in-degree and out-degree. A subgraph, a path, and a cycle are terms that define increasingly complex, connected structures in a graph, where the path consists of a series of consecutive edges, and a cycle or circuit refers to a closed walk that returns to the initial vertex. Standard classes of graphs include trees (acyclic connected graphs), bipartite graphs (graphs whose vertex sets are partitioned such that edges cross between the two partitions), and planar graphs (graphs that can be drawn consecutively such that no edges cross).

4 Literature Review

Dharmendra Kumar Gurjar [1] is used to graph labelled concept in cryptography for to increase security, the labelled path graphs presented the method of encryption and decryption. The concept of permutation & Combination also used to enhance the hiding message. Dr. Gurusharan Kaur [2] proposed the new algorithm for encryption and decryption using some basic graphs, it is also safe guard from the unauthorised person. R. Jegan et. al.,[3] is using the two types of graphs labelled (Super-edge antimagic total labelling for ladder graph and super-edge antimagic total la- belling for comb graph) use for the encryption techniques combine the cryptography algorithm like Affine-Cipher and RSA Algorithm. P. Amudha et.al [4], proposed the new technique where each char- acter of data to encrypted the Euler graphs. Hamiltonian circuit is used for key generation. Reverse for decrypt. Wael Mahmoud AI Etaiwi et.al [5], proposed the algorithm for new encryption and decryption using the graph theory properties, the new symmetric encryption algorithm use the concept of cycle graphs, complete graph and minimum spanning tree to generate the cipher text using the key. P.A.S.D. Peera [6] is proposed the methodology first con- verts the original message into several graphs and further matrix finally, obtain the

Received: August 12, 2025

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

cipher text by multiplying these matrices with the secret key. M. Giridaran [7] is applied the concept of the super magic labelling to encrypt and decrypt a secure message. S. Vani Shree [8] is proposed an edge bi magic mean labelling approach for latitude graph and slanting ladder graph is used to analyse both the encryption and decryption processes of a text using the affine cipher.

- **Related Work in Graph-Based Cryptography**

Graph-based Cryptography is the study of how we might leverage graph structures and their mathematical properties to build secure cryptographic primitives, protocols, and key management schemes. The fundamental goal is to apply graph representations (e.g., adjacency matrices, incidence structures, graph spectra) to instantiate hard problems, build efficient encoding schemes, or securely represent communication processes. This section describes some example topics, techniques, and trends that have characterized recent activity in the field.

Graphs are used in cryptography:

There are many works that represent data and computations as graphs or graph abstractions, such as adjacency or Laplacian matrices, graph complements, and certain classes of special graphs. These representations are useful in developing new encryption/decryption pipelines, as well as paving the way for security analyses in graph theory.

Cryptography based on matrices:

Based on adjacency, incidence, and other graph-derived matrices, we can create linear or non-linear mappings used for key generation, encryption, and decryption processes. These mappings are aligned with several matrix properties (inverted, sparse, and spectral properties) to create good security and performance trade-offs.

Graph labeling and magic sums: Labeling schemes (edge magic total labeling, antimagic labeling, and cordial labeling) label graph elements with algebraic restrictions. Labeling schemes can lead directly to cryptographic encodings or inspire such encodings, as the labels generate structured, often computationally infeasible-to-invert mappings.

- **Existing Encryption and Decryption Methods:-**

In general, encryption techniques can be characterized as symmetric and asymmetric schemes, with a mixture of both applied in practice. Symmetric schemes use one shared key for both encryption and decryption, while asymmetric schemes use a public key for encryption and a private key for decryption. Research papers typically contrast algorithms with respect to a security proof, performance metrics, and factors related to implementation, while clearly recognizing a distinction between cryptographic objectives (confidentiality, integrity, authenticity) and the operational context (data-at-rest, data-in-transit, or end-to-end). In general, do not restate the original verbatim; nevertheless, paraphrase terms in your writing and cite original standards and peer-reviewed publications for each technique.

- ✓ **Symmetric Encryption:-**

A definition is a single secret key for encryption and decryption. Desirable for high-speed

Received: August 12, 2025

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

protection of data if the exchange of keys is done securely.

Algorithms:- Some popular algorithms would be AES (Advanced Encryption Standard), ChaCha20-Poly1305, Blowfish, Twofish, Triple DES (play old algorithms in most systems). Describe these algorithms in context of key size, modes of operations, and security guarantees**.**

Modes of operation: ECB, CBC, CFB, OFB, GCM, and XTS. Describe affect of modes on confidentiality, integrity, and error propagation; note how authenticated encryption with associated data (AEAD) modes like GCM and ChaCha20-Poly1305 provide both confidentiality and integrity in one primitive.

Security concerns: Key management, IV/randomness, potential against chosen-plaintext and known-plaintext attacks, and side-channel issues related to implementation.

Common use cases: Protecting data-at-rest e.g. encrypting databases, files, and large volumes of stream data that are optimized for high-throughput.

Paper evaluation criteria: use the most significant key length, the famility of the algorithm, potential against current attack vectors, performance benchmarks, and footprint in memory/CPU for a target platform.

- ✓ **Assymmetric Encryption:-**

Definition: Utilizes a pair of keys: a public key for encryption and a private key for decryption. Enables secure exchange of keys, digital signatures, and identity verification without any prior sharing of secrets.

Main algorithms: RSA, Elliptic Curve Cryptography (ECC), Diffie-Hellman (used in key establishment), and lattice-based schemes coming from post-quantum thinking.

Security basis: integer factorization in the case of RSA, problems based on discrete logarithms for values that apply to Diffie-Hellman and ECC, and quantum-resistance thinking concerning post-quantum algorithms.

Standard applications: secure exchanges of messages, digital signatures, certificate-based authentication, and some hybrid protocols (e.g., TLS) that use asymmetric cryptography to derive a session key for a symmetric encryption session.

Filter for papers: implications related to the size of the key, their proof of security or reduction, performance to establish their efficacy in modes commonly called handshake, and impacts with latency related to the established secure channel.

- **Research Gaps :-**

There is good research about the combination of current graph-structural labeling methodologies and matrix cryptographic constructions in the context of producing efficient, usable, and verifiable solutions where current versions resist quantum and classical attacks. Specifically, there are gaps in systematic and rigorous connections between high-level graph matrix representations (such as adjacency, Laplacian, and normalized) and primitives; systematic and rigorous security reductions relating graph matrix representations to hardness

Received: August 12, 2025

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

assumptions; and systematic and reproducible evaluation to quantify protocol security and performance using real-world data as well as standard image/media formats, and be free of plagiarized methodology.

5 Table Value

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	2	3	4	5	6	7	8	9	10	11	12	13	14

SPACE	.	Z	Y	X	W	V	U	T	S	R	Q	P	O
28	27	26	25	24	23	22	21	20	19	18	17	16	15

Example

A = 28	B= 27	M = 16
SPACE = 1	2 = DOT	13 = P
N = 15	C = 26	L = 17
O= 14	Z= 3	Q = 12

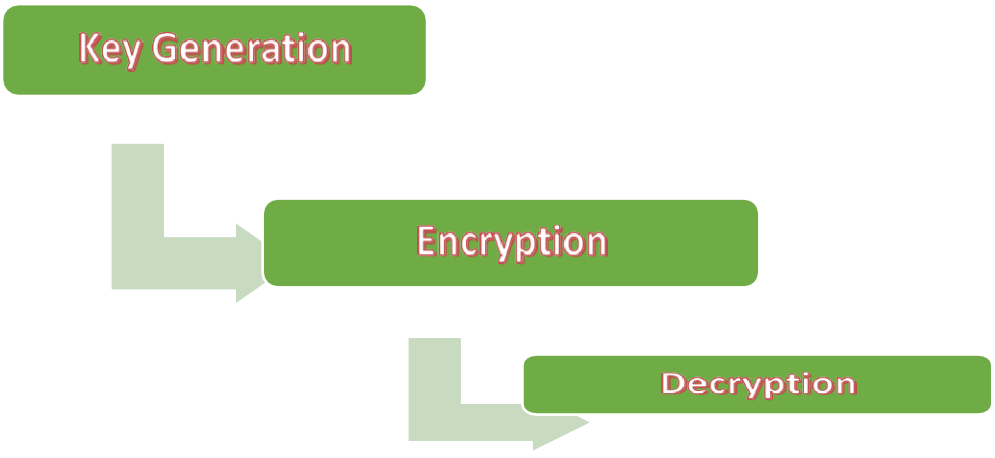
6 Proposed Methodology

6.1 Key generation

The generation of keys is one of the most important areas in which encryption and decryption focus. First, we will establish the graph using the matrix; we get key values according to what we calculated. Additionally, you may also want to be mindful of any modifiers that may apply when responding to a question. From the graph, draw the adjacent matrix, and we get the key.

Figure 1

Encryption Algorithm



Received: August 12, 2025

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

In encryption, the plain text is converted into the cipher text.

Step 1: Take the example of plain text.

Step 2: Change the text into the alphanumeric alternative letter and numbers using the encoding table.

Step 3: Now, using the key K1, format the matrix arranged in the row-wise

Step 4: From these row-wise matrix using the adjacent matrix key K1 and written in the column wise matrix

Step 5: Using the adjacent matrix key, split the values in the matrix form.

Step 6: Read off the message row by row.

Step 7: Using the key, change the column-by-column change in row by row.

Step 8: Write the matrix again and read row by row. Repeat the five times matrix format.

Step 9: Finally, we obtain the ciphertext after reading each row.

Step 10: End

6.2 Decryption Algorithm

The purpose of this method is to translate encryption into plain text.

Step 1: Receiver cipher text convert into plain text

Step 2: Arrange the cipher text in the matrix form column by col- umn using key K1.

Step 3: Now take it into the row-by-row format.

Step 4: From row-by-row format change into the matrix

Step 5: Again, take into the row by row.

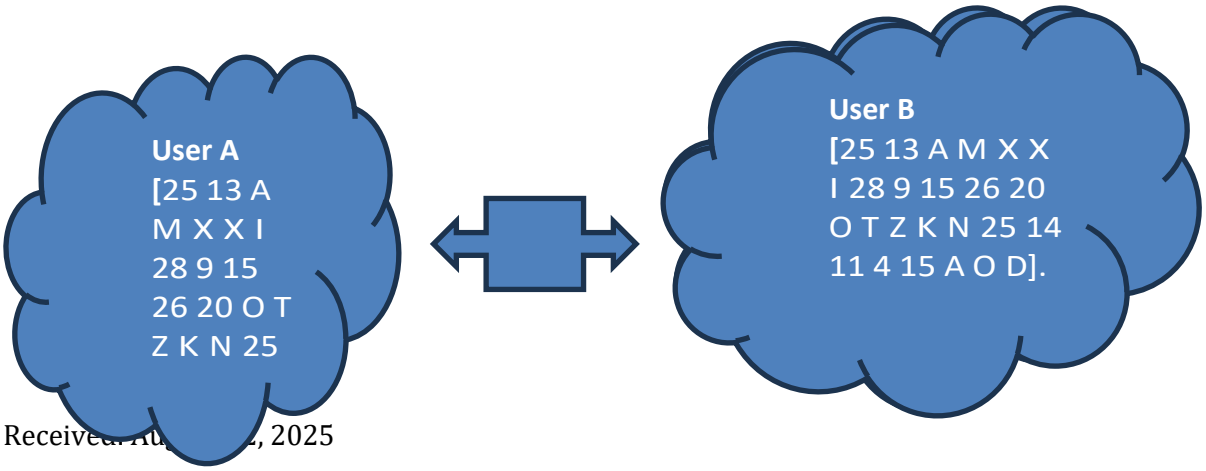
Step 6: It is in the alternate alphanumeric series change into alphabet and numbers.

Step 7: Now decrypt the message

Step 8: Finally, we get plain text.

Step 9: End.

Illustration:-



Received: Au , 2025

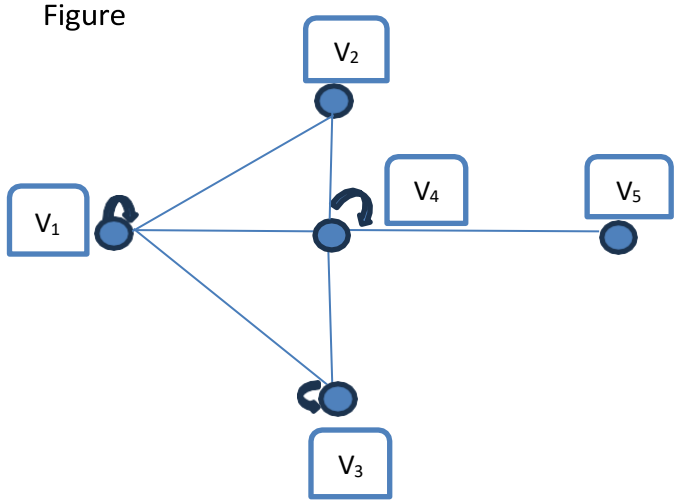
International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Result Outcomes

6.3 Key Generation

Multigraph A graph with two vertices connected with edges is a parallel edge. It is a not a simple graph. And it also has a self-loop is known as a multigraph.

Figure



6.4 Adjacent Matrix

	$V1$	$V2$	$V3$	$V4$	$V5$
$V1$	1	1	1	1	0
$V2$	1	0	0	1	0
$V3$	1	0	1	1	0
$V4$	1	1	1	1	1
$V5$	0	0	0	1	0

Therefore, key $K1 = 4\ \ 2\ \ 3\ \ 5\ \ 1$

6.5 Encryption Algorithm

1) **Example: Encryption and Decryption**

2) Change the example sentence into the alphanumeric take oppo- site letter.

3) Encryption and decryption

$X\ 15\ Z\ 11\ D\ 13\ I\ 20\ N\ 15\ A\ 28\ O\ 25\ A\ 25\ X\ 26\ K\ 4\ M\ 9\ T\ 14\ O$

Step 1: Now, using the key K1, format the matrix arranged in the row-wise

Received: August 12, 2025

International Journal of Applied Mathematics

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

X	15	*Z*	11	*D*
13	*I*	10	*N*	15
A	28	O	25	*A*
25	*X*	26	*K*	4
M	9	*T*	14	O

Step 2: Using the key, change into column-by-column change into row-by-row

D	15	*A*	4	*O*
15	*I*	28	*X*	9
Z	20	O	26	*T*
X	13	*A*	25	*M*
11	*N*	25	*K*	14

Step 3: Read off the message row by row.

O	9	*T*	*M*	14
15	*I*	20	13	*N*
A	28	O	*A*	25
D	15	*Z*	*X*	11
4	*X*	26	25	*K*

Step 4: Using the key, change the column-by-column change in row by row

14	*N*	25	11	*K*
9	*I*	28	15	*X*
T	20	*O*	*Z*	26
O	15	*A*	*D*	4
M	13	*A*	*X*	25

Step 5: Write the matrix again and read row by row.

K	*X*	26	4	25
N	*I*	20	15	13
25	28	*O*	*A*	*A*
14	9	*T*	*O*	*M*
11	15	*Z*	*D*	*X*

Finally, we obtain the ciphertext after reading each row.

Now, we get Cipher Text

Received: August 12, 2025

International Journal of Applied Mathematics

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

25 13 *A M X X I* 28 9 15 26 20 *O T Z K N* 25 14 11 4 15 *A O D*.

6.6 Decryption Algorithm

Receiver cipher text convert into plain text Cipher text

25 13 *A M X X I* 28 9 15 26 20 *O T Z K N* 25 14 11 4 15 *A O D*

Step 1: Arrange the cipher text in the matrix form column by column using key.

K	*X*	26	4	25
N	*I*	20	15	13
25	28	*O*	*A*	*A*
14	9	*T*	*O*	*M*
11	15	*Z*	*D*	*X*

Step 2: Now take it into the row-by-row format. From row-by-row format change into the matrix form column by column using the key.

*14	*N*	25	11	*K*
9	*I*	28	15	*X*
T	20	*O*	*Z*	26
O	15	*A*	*D*	4
M	13	*A*	*X*	25

Step 3: Again, take into the row by row.

O	9	*T*	*M*	14
15	*I*	20	13	*N*
A	28	O	*A*	25
D	15	*Z*	*X*	11
4	*X*	26	25	*K*

Step 4: Repeat until the final matrix is received.

D	15	*A*	4	*O*
15	*I*	28	*X*	9
Z	20	O	26	*T*

Received: August 12, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

X	13	*A*	25	*M*
11	*N*	25	*K*	14

Step 5: Repeat the process.

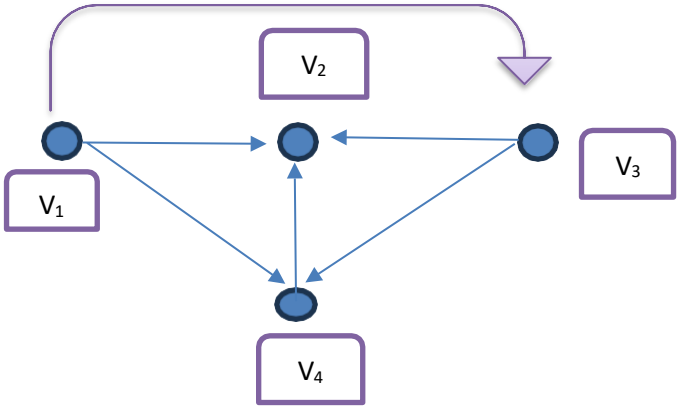
X	15	*Z*	11	*D*
13	*I*	10	*N*	15
A	28	O	25	*A*
25	*X*	26	*K*	4
M	9	*T*	14	O

It is in the alternate alphanumeric series change into alphabet.

X 15 *Z* 11 *D* 13 *I* 20 *N* 15 *A* 28 *O* 25 *A* 25 *X* 26 *K* 4 *M* 9 *T* 14 *o*

Now decrypt the message. Finally, we get plain text. Encryption and Decryption.

7 Incident Matrix



7.1 Key Generation – Incident Matrix

The generation of keys is one of the most important areas in which encryption and decryption focus. First, we will establish the graph using the matrix; we get key values according to what we calculated. Additionally, you may also want to be mindful of any modifiers that may apply when responding to a question. From the graph, draw the adjacent matrix, and we get the key.

7.2 Encryption Algorithm – Incident Matrix

In encryption, the plain text is converted into the cipher text.

Step 1: Take the example of plain text.

Received: August 12, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Step 2: Change the text into the alphanumeric alternative letter and numbers using the encoding table.

Step 3: Now, using the key $K2$, format the matrix arranged in the row-wise

Step 4: From these row-wise matrix using the adjacent matrix key

$K2$ and written in the column wise matrix.

Step 5: Using the adjacent matrix key, split the values in the matrix form.

Step 6: Read off the message row by row.

Step 7: Using the key, change the column-by-column change in row by row.

Step 8: Write the matrix again and read row by row. Repeat the five times matrix format.

Step 9: Finally, we obtain the ciphertext after reading each row. Step 10: End.

7.3 Decryption Algorithm – Incident Matrix

The purpose of this method is to translate encryption into plain text.

Step 1: Receiver cipher text convert into plain text

Step 2: Arrange the cipher text in the matrix form column by col- umn using key $K2$.

Step 3: Now take it into the row-by-row format.

Step 4: From row-by-row format change into the matrix form col- umn by column using the key $K2$.

Step 5: Again, take into the row by row.

Step 6: It is in the alternate alphanumeric series change into alpha- bet and numbers.

Step 7: Now decrypt the message Step 8: Finally, we get plain text. Step 9: End.

8 Proposed Methodology for Incident Matrix

In this process, the incident matrix is used for the cryptography process of key generation, encryption & decryption.

8.1 Key Generation

$V1$	$V1$	$V1$	$V1$	$V1$	$V1$
$V1$	$V1$	$V1$	$V1$	$V1$	$V1$
$V1$	$V1$	$V1$	$V1$	$V1$	$V1$
$V1$	$V1$	$V1$	$V1$	$V1$	$V1$

Received: August 12, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$V1$	$V1$	$V1$	$V1$	$V1$	$V1$

Incident matrix Key $K2$: 3021

8.2 Encryption Process

Take the example of plain text.

Example I Love Daughter.

Change the text into the alphanumeric alternative letter or num- bers using the encoding table.

T 1 Q 14 G 24 A 25 $SPACE$ 8 V 21 I 24 K 2

Step 1: Now, using the key $K2$, format the matrix arranged in the row-wise.

T	1	Q	14
G	24	A	25
Space	8	V	21
I	24	K	2

Step 2: From these row-wise using the adjacent matrix key $K2$ in the column.

1	24	8	24
14	25	21	2
Q	A	V	K
T	G	Space	I

Step 3: Using the adjacent matrix key, split the values in the ma- trix form.

24	25	A	G
24	2	K	I
8	21	V	Space
1	14	Q	T

Step 4: Read off the message row by row. Using the key, change the column-by-column change in row by row.

25	2	21	14

Received: August 12, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

G	*I*	Space	*T*
A	*K*	*V*	*Q*
24	24	8	1

Step 5: Write the matrix again and read row by row.

2	*I*	*K*	24
14	*T*	*Q*	1
21	Space	*V*	8
25	*G*	*A*	24

Finally, we obtain the ciphertext after reading each row.

Cipher Text

2 *I K* 24 14 *T Q* 1 21 Space *V* 8 25 *G A* 24.

8.3 Decryption Process – Incident Matrix

The purpose of this method is receiver cipher text convert into plain text

Cipher Text

2 *I K* 24 14 *T Q* 1 21 Space *V* 8 25 *G A* 24

Step 1:

2	*I*	*K*	24
14	*T*	*Q*	1
21	Space	*V*	8
25	*G*	*A*	24

Step 2: Arrange the cipher text in the matrix form column by column using key.

25	2	21	14
G	*I*	Space	*T*
A	*K*	*V*	*Q*

Received: August 12, 2025

International Journal of Applied Mathematics

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

24	24	8	1

Step 3: Now take it into the row-by-row format. Again take into the row by row.

24	25	*A*	*G*
24	2	*K*	*I*
8	21	*V*	Space
1	14	*Q*	*T*

Step 4: From row-by-row format change into the matrix form column by column using the key.

1	24	8	24
14	25	21	2
Q	*A*	*V*	*K*
T	*G*	Space	*I*

Step 5: Again, take into the row by row.

T	1	*Q*	14
G	24	*A*	25
Space	8	*V*	21
I	24	*K*	2

It is in the alternate alphanumeric series change into alphabet.

T 1 *Q* 14 *G* 24 *A* 25 SPACE 8 *V*21 *I* 24 *K* 2

Now decrypt the message. Finally we get plain text.

Final Plain Text: I Love Daughter.

9 Conclusion

The final conclusion of the paperwork introduces a new innovative cryptographic method with the use of graph theory, some basic graphs using the adjacency and incident matrices to create keys, and organized encryption and decryption of the proposed algorithm. It is more safeguarded information in the modern crypto graphic methods, presenting the difficulties for unauthorized at- tacks or access. Even the traditional cipher, modern cipher, brute force attack, etc., is not easy to attack. Future enhancements include using the new trending graph theory integrated with cryptography for authentication or pure graph theory connected with public key cryptography using some algorithms like Playfair cipher or stream cipher.

Received: August 12, 2025

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

References

[1] Dharmendra Kumar Gurjar, Auparajita Krishnaa, Labeled Paths in Cryptography, *Advances in Mathematics Research*, ISBN: 978-1-53619-759-4 (2021).

[2] Dr. Gurusharan Kaur, Dr. Namrata Tripathi, Applying Graph Theory to Secure Data by Cryptography, *International Jour- nal of Linguistics and computational Applications (IJLCA)*, **8**(Issue 1) (2021).

[3] R. Jegan et. al, Encryption A Word using Super- Edge An- timagic and Super -Edge Magic Total Labeling of Extended Duplicate Graphs, *Indian Journal of Computer Science and Engineering (IJCSE)*, **13**(5) (2022).

[4] P. Amudha et. al, An Application of Graph Theory in Cryp- tography, *International Journal of Pure and Applied Mathe- matics*, **119**(13) (2018).

[5] Wael Mahmoud AI Etaiwi, Encryption Algorithm using Graph Theory, *Journal of Scientific Research & Reports* (2014), Doi: 10.9734/JSRR/2014/11804.

[6] P.A.S.D. Perera, G.S. Wijesiri, Encryption and Decryption Al- gorithms in Symmetric Key Cryptography Using Graph the- ory, *Psychology and Education Journal* (2021).

[7] M. Giridaran, Application of Super Magic Labeling in Cryp- tography, *International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)*, **9**(Issue 6) (2020).

[8] S. Vani shree, S. Dhanalakshmi, Application of Edge Bimagic Mean Labeling in Data Security.

[9] D.A. Angel Sherin, V. Maheswari, Encryption and Decryp- tion Process Using Edge Magic Labeling, International Con- ference on Physics and Photonics Processes in Nano Sciences,

J. Phys. Conf. ser., 1362 012024 (2019), doi:10.1088/1742- 6596/1362/1/012024.

[10] Dharmendra Kumar Gurjar, Auparajita Krishnaa, Various Antimagic Labeled Graphs from Graph Theory for Cryptogra- phy Applications, *International Journal of Scientific Research in Mathematical and Statistical Sciences*, **9**(Issue 3), 11–18, June (2022), E-ISSN: 2348-4519.

[11] Sangeetha Nandigam, perumali sundarayya, Graph theory for data cryptography security, *International Journal of Mathe- matics in Operational Research*, **30**(2), April 9 (2025).

[12] I.W. Sudarsana et. al., An application of super mean and magic graphs labelling on cryptography system, *Jour- nal of Physics: Conference Series* (2020), doi:10.1088/1742- 6596/1763/1/012052.

[13] Abhishek, Dr. Vandana, A study on Modified RSA Algorithm in Network Security, *International Research Journal of Mod- ernization in Engineering Technology and science*, **4** (2022).

[14] S. Vani Shree, S. Dhanalakshmi, Information Security by em- ploying RSA Algorithm

Received: August 12, 2025

Volume 38 No. 12s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and Graph Labeling, *IAENG Inter- national Journal of Applied Mathematics*, **54**(Issue 12), Dec (2024).

[15] N.K. Geetha, and V. Ragavi, Graph Theory Matrix Approach in Cryptography and Network Security, *Algorithms, Comput- ing and Mathematics Conference (ACM)* (2022), Doi: 10. 1109/ACM57404.2022.00025.

[16] Auparajita Krishnaa, On Antimagic labelling of some cycle related graphs, *Journal of Discrete Mathematical Sciences and Cryptography*, **15**(4 & 5), 225–235, 2012.

Received: August 12, 2025