iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XII **Month of publication:** December 2021

DOI: https://doi.org/10.22214/ijraset.2021.39048

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XII Dec 2021- Available at www.ijraset.com

Employing Graph Theory on Social Networks by Data Encryption to Enhance Privacy

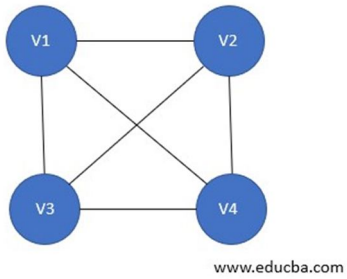
P. Shalini[1], K. M. Manikandan[2]
[1]*M.Sc, Mathematics,* [2]*Head and Assistant Professor Of Mathematics, Departent of Mathematics, Dr. S N S Rajalakshmi college of arts and science, Coimbatore, TamilNadu, India.*

Abstract: ***Now a day's users of Online Social Network have been increased by the Internet usage. As huge number of online social Network users, it becomes more and more interactive and privacy becomes a matter of increasing concern. To solve this problem, graph structure, Proposed Algorithm, Encryption Algorithm used, which excludes the users which combine the information of the status of privacy users. By using these methods, the experiment can be done which helps to show how the server works in between the sender and receiver and to receive their information without knowing third parties. And it would be easier by using graph that shows it can be efficiently helps the users to improve their privacy disclosure.***
Keywords: Graph theory, social network, Privacy, Data Encryption, end to end encryption, Encryption Algorithm.

I. INTRODUCTION

A. *Graph Theory*

The paper written by Leonhard Euler on the Seven Bridges of Konigsberg and published in 1736 is regarded as the first paper in the history of graph theory. A graph G=(V,E) consists of a set of objects V={v_1,v_2....}called vertices and another set E={e_1,e_2,….},whose element is called edges. Graph theory is nothing but is study of graph



1) *Vertices:* We have 4 elements in the set {v1, v2, v3, v4} where V is the set of vertices
2) *Edge:* A edge uniquely identified by its two endpoints. We have two types of edges
- Directed edge
- Undirected edges

B. *Social Network*

A social network is a website which connects peoples with various interests to come together and share information, photos, and videos. The most usable definition is derived from graph theory that is, a set of vertices (or nodes, units, points) representing social entities or objects and a set of lines representing one or more social relations among them.

Networks can be divided into two major parts:

1) *Social and Economic Network:* It consists of a group of people connected with some sort of interactions or pattern of communication. e.g. - Facebook, Twitter, business relation between companies and clients, interrelationship between families involved in a marriage etc.
2) *Information Network:* The connection between• information objects e.g. – Semantic (links between various words and symbols), World Wide Web (link between various web pages; new page connecting to another through hyperlinks)

©IJRASET: All Rights are Reserved

C. Graph using Social Network

A social network graph is a graph where the nodes represent people and the lines between nodes, called edges, a social network is a website which connects peoples with various interest to come together and share information, videos, photos and it represent social connections between them, such as friendship or working together on a project. These graphs can be either undirected or directed. Let us have some of the interesting example:

D. Facebook

A social network like Facebook can be represented as an undirected graph. A user would be vertices in the graph and if 2 users are friends, there would be an edge connecting them.A real social network would have millions and billions of vertices. Lots of problem can be easily solved by applying standard algorithm. Like here in this social network, Let us say we want to do something like suggest friends to a user.

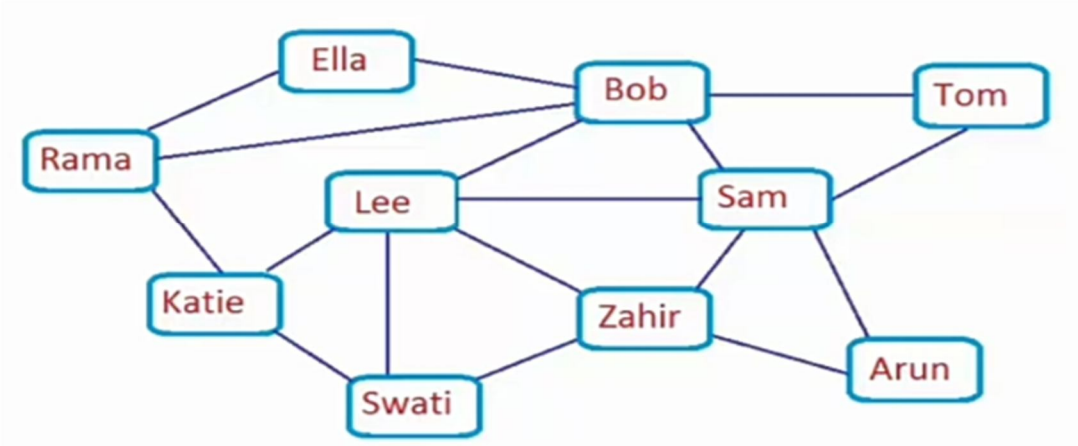


Fig:2

In this fig 2 we can suggest some connections to Rama. There is only one possible approach to do can be suggesting friends of friends who are not connected already

In this fig 2: Rama has 3 friends Ella, Bob and Katie and friends of 3 that are not connected to Rama already can be suggested. There is no friend of Ella who is not connected to Rama already. Bob however, has 3 friends Tom, Sam and Lee that are not friends with Rama so they can be suggested and Katie has 2 friends' lee and Swati who is not connected to Rama. We have counted Lee already so in all we can suggest these 4 users to Rama. Now even though we described this problem in context of a social network this is a standard graph problem .The problem is pure graph term to finding all vertices having length of shortest path from a given vertices equal to 2.From this the social network like Facebook is an undirected graph.

E. Application of Graph Theory in Social Network

The concept of graph theory is extensively used in social media. Usually here the users or the people involved are considered as the vertices. And any relation between the users due to common likes or mutual friendship is considered as edges.

1) *Graph Theory in Facebook:* Majority are familiar with Facebook these days. You can click 'like' if you find something likeable, 'tag' your friends in various 'posts', put comments in posts and most importantly befriend someone whom you know and also someone whom you don't know! The concept of graph theory is used in Facebook with each person as nodes and every like, share, comment, tag as edges.
2) *Graph Theory in Twitter:* Here the persons are considered as nodes and if one person follows another then that is considered as the edge between the two.

II. PRIVACY

Privacy is state of being free from public security. Internet Privacy involves the right of personal privacy concerning the storing, repurposing, provision to third parties and displaying of information to the user via internet.

A. Purpose Of Privacy In Social Network

This privacy which helps not to share passwords to your friends , relations, etc… setting your profile to private and not accepting unknown friend requests are good standard practices.

©IJRASET: All Rights are Reserved

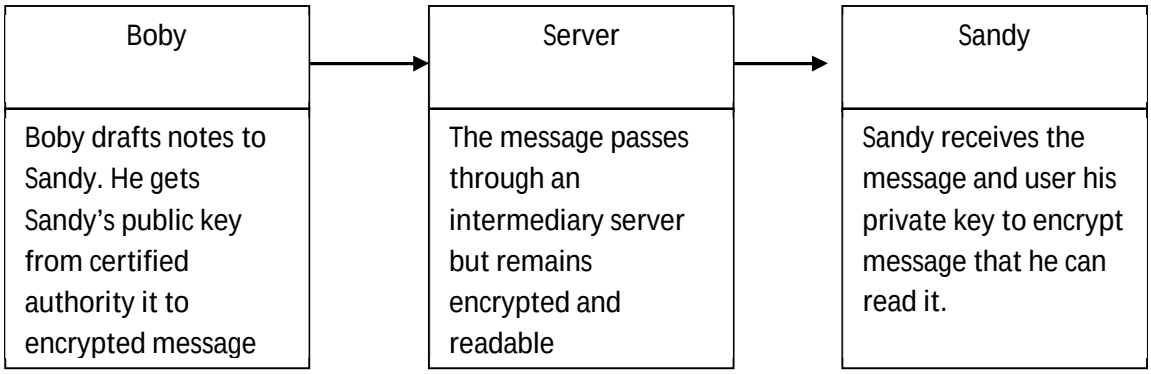
B. Data Encryption

Data encryption is nothing that which translates data into another form of code so that will be easier for the user to maintain secret code. This data is usually referred as cipher text and the unencrypted data is refers as plain text.

C. End –End Encryption

End to end Encryption which secure information that prevents from third-parties while transforming from one person to another.

For example,



This figure shows that Boby sends Sandy a message using end to end encryption.

1) Advantages of End-To-End Encryption

The main advantage of end-to-end encryption is a high level of data privacy, provided by the following features:

a) Security in Transit: End-to-end encryption uses public key cryptography, which stores private keys on the endpoint devices. Messages can only be decrypted using these keys, so only people with access to the endpoint devices are able to read the message.

b) Tamper-proof: With E2EE, the decryption key does not have to be transmitted; the recipient will already have it. If a message encrypted with a public key gets altered or tampered with in transit, the recipient will not be able to decrypt it, so the tampered contents will not be viewable.

c) Compliance: Many industries are bound by regulatory compliance laws that require encryption-level data security. End-to-end encryption can help organizations protect that data by making it unreadable.

D. Secure Data Transfer: Graph $C_n \odot K_1$ by Proposed Algorithm

1) In this algorithm, which represents a vertices in then Graph, each character represented by a vertex ,when all the adjacent character is represented as adjacent edge it keeps adding until it form cyclic graph (some number of vertices connected in a closed chain).

2) Every letter in data has its unique numeric representation, mentioned in encoding table, which is used to encode each alphabetic character.

3) Then, each digit is transmuted up to n-place, through shift type of cipher. Now, new numeric values are obtained.

4) Randomly, some positive integers b_1 are selected which are relatively prime with a_i.

5) By taking inverse of that a_i in the modulus of b_i , graph $C_n \odot K_1$ is considered according to length of simple text with specified outward vertices and allocates the resulting inverses to suspended outward vertices, while main vertices are labeled with b_i

6) The final labeled graph $C_n \odot K_1$ is the encrypted data, in which the recipient receives to get required information.

©IJRASET: All Rights are Reserved

E. Encryption Algorithm

1) Add a special character to indicate the starting character (Let A).
2) Add vertex for each character in the plain text to the graph.
3) Link vertices together by adding an edge between each sequential character in the plain text until we form a cycle graph.
4) Weight each edge using the encoding table. Each edge's weight represents the distance between the connected two vertices from the encoding table.
5) Give the numerical values to the alphabets of plain-text word and apply shift cipher; en Give the numerical values to the alphabets of plain-text word and apply shift cipher; $e_n(x) = x + n(\text{mod}26)$, to each numerical value obtained before and get new numerical values, say $a_1, a_2, a_3 \ldots\ldots\ldots a_n$
6) Find a sequence; $b_1, b_2, b_3 \ldots b_n$ of positive integers in increasing order such that $\gcd(b_i, a_i) = 1$ and $b_i > 26$.
7) Consider a graph $C_n \odot K_1$ with 2n vertices and allot weights; $b_1, b_2, b_3 \ldots b_n$ to the vertices, adjacent to pendent vertices randomly.
8) Find the inverse of a_i $(\text{mod}b_i)$ for all i and denote them by c_i, i.e., $c_i = (a_i)^{-1}$ $(\text{mod}b_i)\forall i$.
9) Give numeric values $c_1, c_2, c_3 \ldots c_n$ to pendent vertices.
10) Send this graph $C_n \odot K_1$ to the receiver

F. Decryption Algorithm

1) The receiver receives the graph, and following steps are applied to transform the information and get original data
2) Arrange those vertices which are adjacent to the pendent vertices, in increasing order as $b_1 < b_2 < b_3 < \cdots < b_n$.
3) Find the inverse of the weights of pendent vertices c_i modulus their adjacent vertices b_i and denote them by a_i for each i
4) Compute $w_i = a_i - (\text{order of graph}/2)\text{mod}26, \forall i$. Convert the numeric value w_i for each I, to relate specific letters,

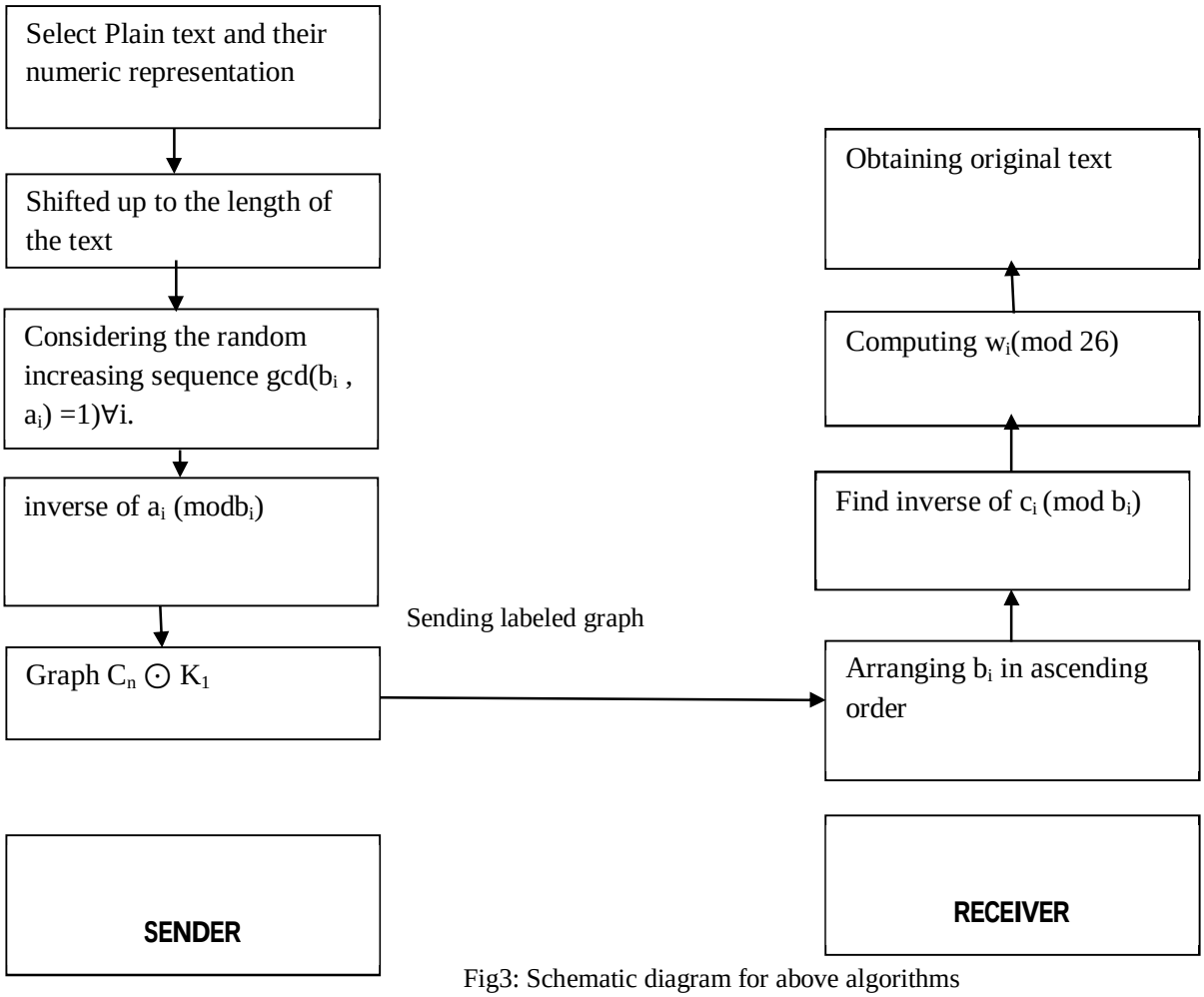


Fig3: Schematic diagram for above algorithms

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XII Dec 2021- Available at www.ijraset.com

Let us suppose we have to transform information, I.e., FILE, encrypting it and then sending it to the recipient.

The starting point is to convert the alphabets into number of their respective positions through the encoding table

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

F I L E

6 9 12 5

Here, length of the word n=4, Applying shift cipher $e_n(x) = x + n(\text{mod}26)$, we get

$06+4=10= a_1$
$09+4=13= a_2$
$12+4=16= a_3$
$05+4=09= a_4$

Given word “FILE” is encrypted in the form

J M P I

Selecting random increasing method b_i, such that the value of $b_i > 26$.

Gcd $(b_1,a_1)=(29,10)=1$
Gcd $(b_2,a_2)=(31,13)=1$
Gcd $(b_3,a_3)=(35,16)=1$
Gcd $(b_4,a_4)=(40,9)=1$

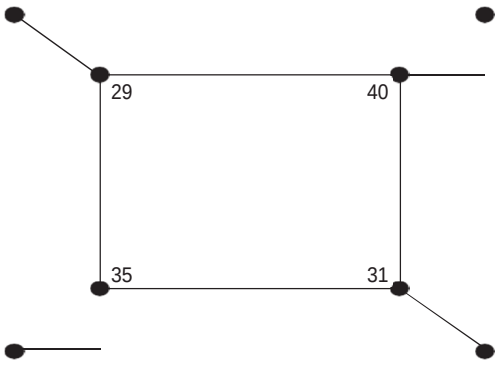


Fig 4

Constructing the graph (C_n is dot product of K_1) $C_n \odot K_1$and put the value of b_i to main vertices randomly as shown in the above fig 4

Now, through the below mentioned step, $c_i = (a_i)^{-1} (\text{mod}b_i)$

We get,
$C_1 = (a_1)^{-1} (\text{mod}b_1) = (10)^{-1} (\text{mod } 29) = 3$
$c_2 = (a_2)^{-1} (\text{mod}b_2) = (13)^{-1} (\text{mod } 31) = 12$
$c_3 = (a_3)^{-1} (\text{mod}b_3) = (16)^{-1} (\text{mod } 35) = 11$
$c_4 = (a_4)^{-1} (\text{mod}b_4) = (09)^{-1} (\text{mod } 40) = 9$

©IJRASET: All Rights are Reserved

The inverse values are given to the adjacent vertices of fig 4 as shown in fig

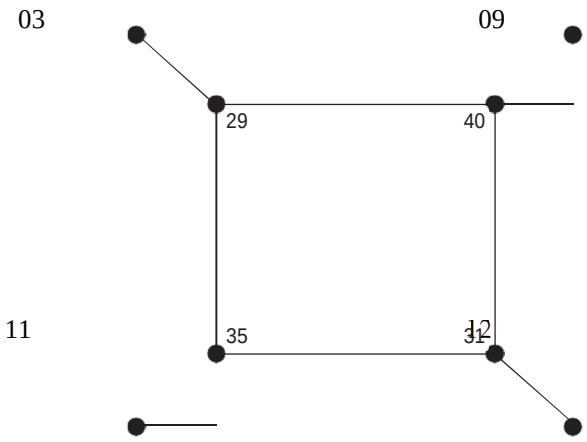


Fig 5

Send this labeled graph (Figure 5) to the receiver.

The recipient, after receiving that labeled graph, arranges the main vertices in ascending o

29<31<35<40

And consider the number as values of b_i such that;

$b_1 < b_2 < b_3 < b_4$

Taking inverse of corresponding vertices with respect to the value of each b_i as shown in fig 5 we get,

3^{-1} (mod 29) =10

12^{-1} (mod 31) =13

11^{-1}(mod 35) =16

9^{-1}(mod 40) =9

Now, for w_i,

$w_i=a_i – (2n/2)$ mod 26

Now let us find the value of a_1, a_2, a_3, a_4

$w_1=a_1 – (2(4)/2)$ mod 26 =6 =F

$w_2=a_2 – (2(4)/2)$ mod 26=9=I

$w_3=a_3 – (2(4)/2)$ mod 26=12=L

$w_4=a_4 – (2(4)/2)$ mod 26=5=E

Finally, we got the original text.

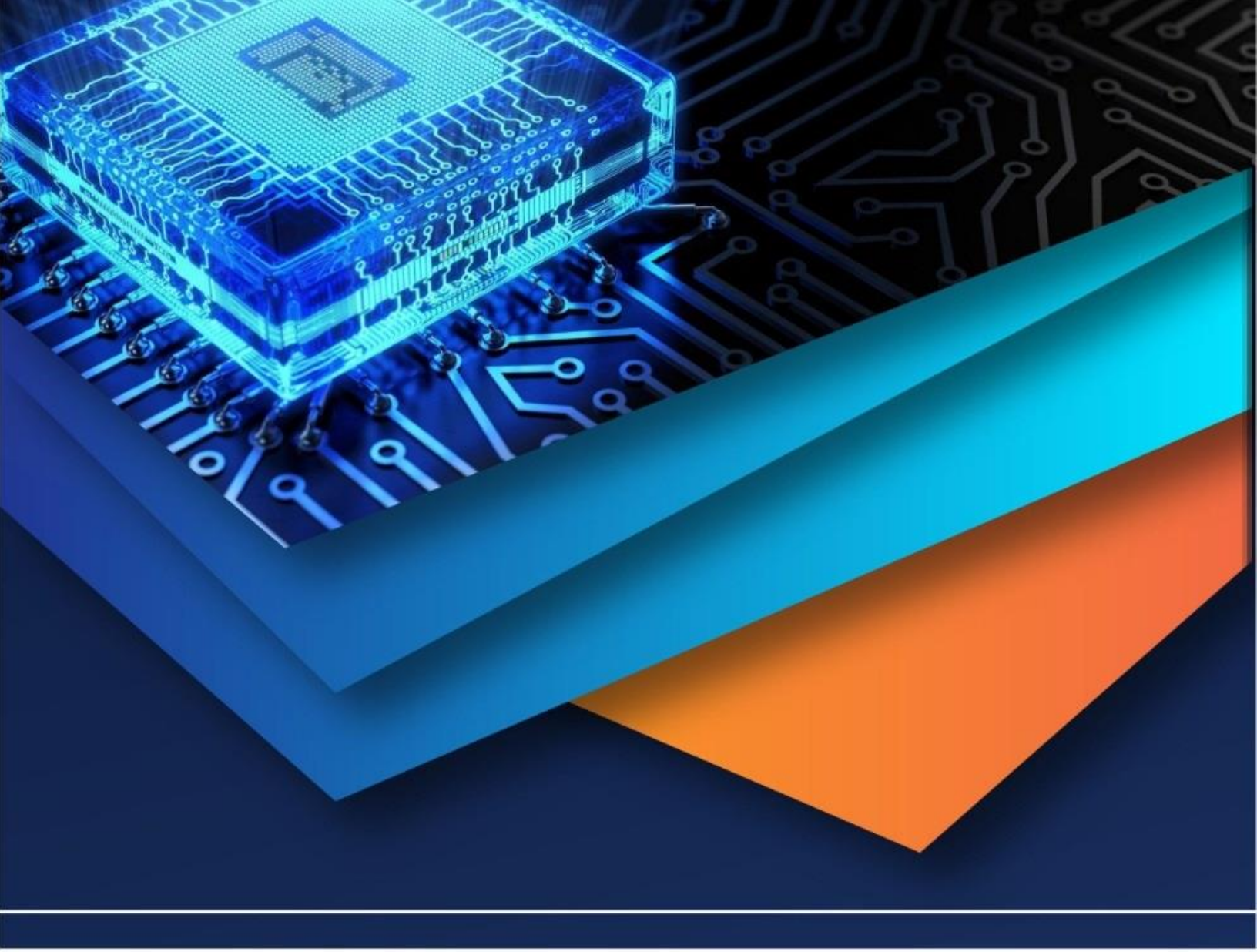
III. CONCLUSION

In this paper we present a graph theory using social network to encrypt the privacy by implanting proposed algorithm, Encryption algorithm and decryption algorithm, This algorithm used to encrypt the data transmitted using an encoding table and Congruence modulo properties in Number theory and minimum spanning tree. The Examples are showed how they receive their information from sender to receiver.

REFERENCES

[1] Graph Theory with Applications to Engineering and Computer Science by Deo (Author), Narsingh (Author).
[2] Social network analysis,Book by John Scott. ,
[3] Corman TH, Leiserson CE, Rivest RL, Stein C. Introduction to algorithms 2nd edition, McGraw-Hill.
[4] Yamuna M, Meenal Gogia, Ashish Sikka, Md. Jazib Hayat Khan. Encryption using graph theory and linear algebra. International Journal of Computer Application. ISSN:2250-1797; 2012.
[5] Encryption Algorithm Using Graph Theory, Wael Mahmoud Al Etaiwi, Information Technology Directorate, Jordan Customs Department, Amman, Jordan.
[6] Some Graph-Based Encryption Schemes, Baizhu Ni, Rabiha Qazi, Shafiq Ur Rehman , and Ghulam Farid Mathematics Science Department, Normal University of Mudanjiang, Mudanjiang, Heilongjiang, China 2 Department of Mathematics, COMSATS University, Islamabad, Attock Campus, Pakistan

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)