International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Encryption Algorithm - Detecting Chemical Structures using Graph Theory

R.Tamizharasi, M.Yamuna

Abstract: ***Security is the matter of great importance when the confidential/important information is stored and transferred across the insecure channel such as an internet where the possibility of protection of information is at high risk. Cryptography is a powerful tool to ensure the secure communication between different operators by transferring the protected information and only the authorized receiver can access the information. Though there are many encryption algorithms available in literature, the requirement of new encryption algorithms also receives importance to prevent any traditional opportunity to sniff data. In this paper, we have proposed a new algorithm to encrypt and decrypt information of interest, using graph theoretical approach.***

Keywords : ***cryptography, decryption, edge, encryption, graph, weight***

I. INTRODUCTION

Most of the products we see around us are made up of atoms. In fact, atoms make up all the matter in the universe. They rarely stay as individual structures and they form molecules instead. Based on their distinct properties and structures, molecules can be categorized and further sub-categorized. Most of the human made products possess a unique molecular formula and hence a unique molecular structure. The most important class of biomolecules are DNA and RNA. These are involved in storage of genetic information.

The drugs around us have a basic molecular structure. Drug overdose creates serious troubles like accidental death. Many times it is due to wrong prescription. The reason for this severe outcome is because of the 3-D structure of drugs dictates where the drug goes in the body and how quickly it does.

Herbicides belong to a group of chemicals, known as pesticides, that is used specifically to kill weeds. We know that these herbicides have specific molecular structures. In most of the food products we see around us food coloring and dyes are used. We know that most of the food colors and dyes are manufactured and have molecular structures.

Revised Manuscript Received on November 30, 2019.
* Correspondence Author
R.Tamizharasi*, Department of Mathematics, Vellore Institute of Technology, Vellore, Tamil Nadu, India.Email: tamizharasi.r@vit.ac.in
M.Yamuna*, Department of Mathematics, Vellore Institute of Technology, Vellore, Tamil Nadu, India.Email: myamuna@vit.ac.in

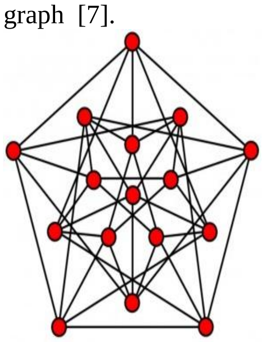
So safety of these molecular formulae is important. Researchers have developed multiple techniques for safety of these formulae.

The security facets and processes associated in the design and implementation of increasingly being used encryption algorithms are examined by [1].

The usage of graph theory in cryptography has been studied by [2]. Encryption using various concepts of graph theory is done by several researchers such as [3]-[6].

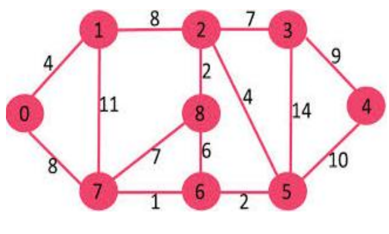
In this article, we propose a method of encrypting the molecular structure using graph theory.

Preliminary: **Graph**: $G = (V, E)$ is defined as a graph where V = set of vertices in G (shown in red color) and E = set of edges (link between vertices) in G. Snapshot 1, gives an example of a graph [7].



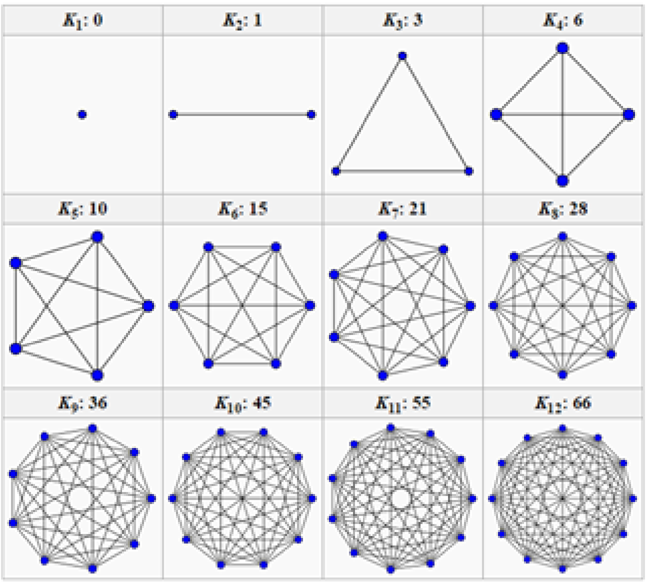
Snapshot:1

Weighted graph: Assigning numbers to the edges of a graph G is a weighted graph. An example for a weighted graph is displayed in snapshot 2 [8].



Snapshot:2

Complete graph: A graph G is said to be complete if there exists an edge between every pair of vertices. A complete graph with n vertices is denoted by K_n and number of edges in $K_n = \frac{n(n-1)}{2}$. Snapshot 3 illustrates an example of complete graph [9].



Snapshot: 3

Relatively prime: Two integers are relatively prime if they share no common positive divisors except 1.

(e.g) 12 and 13 are relatively prime, but 12 and 14 are not.

II. PROPOSED METHOD

Molecular graph: Consider any molecular formula and hence its molecular structure. These molecular structures are made of atoms and bonds between them. We shall construct a molecular graph by choosing atoms as vertices and bonds between them as edges. Fig.1 gives an example of a chemical formula of Benzoic acid, its molecular structure and its graph structure.

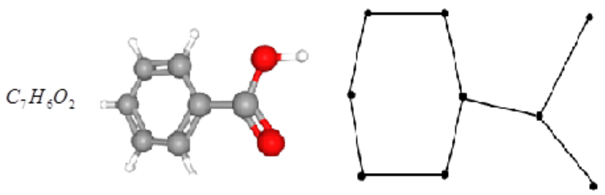
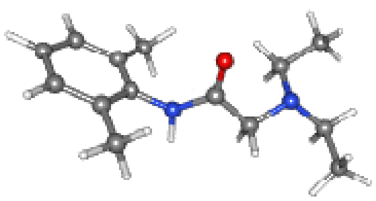


Fig.1. chemical formula, molecular structure and graph structure of Benzoic acid.

The chemical structures used in this paper are taken from "PUBCHEM". While constructing the graph hydrogen bonds are not considered for ease of representation. If required the graph can also be constructed along with the hydrogen bonds.

Encryption algorithm

Step 1 Consider the molecular formula to be encrypted. We shall choose the local anesthetic Lidocaine as an example. The molecular formula of Lidocaine is $C_{14}H_{22}N_2O$. Its molecular structure is shown in snapshot 4.



Snapshot 4: Molecular structure of Lidocaine

Step 2 Construct the molecular graph from the molecular structure. Label the graph as G_1. The molecular graph of Lidocaine is seen in fig.2.

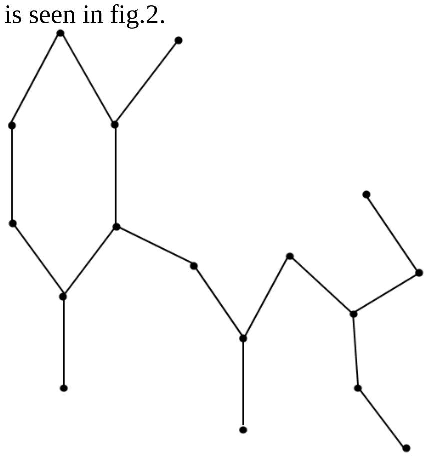


Fig.2. Molecular graph (G_1) of Lidocaine

Step 3 Add random edges between random pair of vertices. We can include any number of edges until the molecular graph becomes a complete graph. That is the number of additional edges added is $\leq \frac{n(n-1)}{2}$ – number of edges in the molecular graph, where n denotes the number of vertices in the molecular graph. Label the resulting graph as G_2. For our example, let us include 7 random edges. The resulting graph is seen in fig.3., in which the newly added edges are highlighted in blue color.

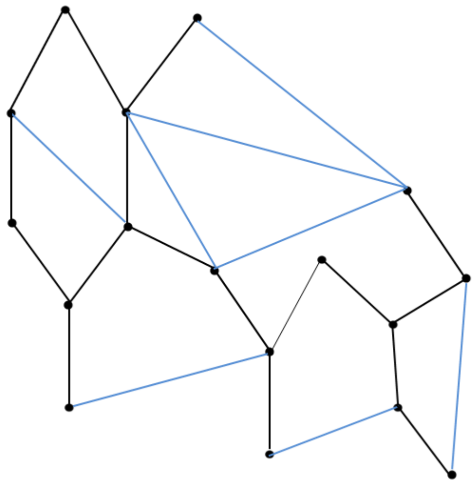


Fig.3. Molecular graph (G_2) of Lidocaine with additional edges

Step 4 Let $e_1, e_2, \ldots e_m$ be the edges in G_1. Assign weights $w_1, w_2, \ldots w_m$ to these edges. Let $w_i = (x_{i1}\ x_{i2})$ where x_{i1}, x_{i2} are integers, $i = 1, 2, \ldots m$. We choose $(x_{i1}\ x_{i2})$ as follows.

$$(x_{i1}\ x_{i2}) = \begin{cases} (y_{i1}\ \ y_{i2}),\ y_{i1} \text{ relatively prime to } y_{i2} \text{ if } e_i \text{ is not an edge in } G_1 \\ (y_{i1}\ \ y_{i2}),\ y_{i1} \text{ not relatively prime to } y_{i2} \text{ if } e_i \text{ is an edge in } G_1 \end{cases}$$

Label the resulting graph as G_3. For the graph seen in fig.3,

Retrieval Number: A4693119119/2019©BEIESP
DOI: 10.35940/ijitee.A4693.119119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

by assigning random weights to the edges, the resulting graph is portrayed in fig.4. Note that the edges in blue color have received a pair of integers as weights, which are relatively prime.

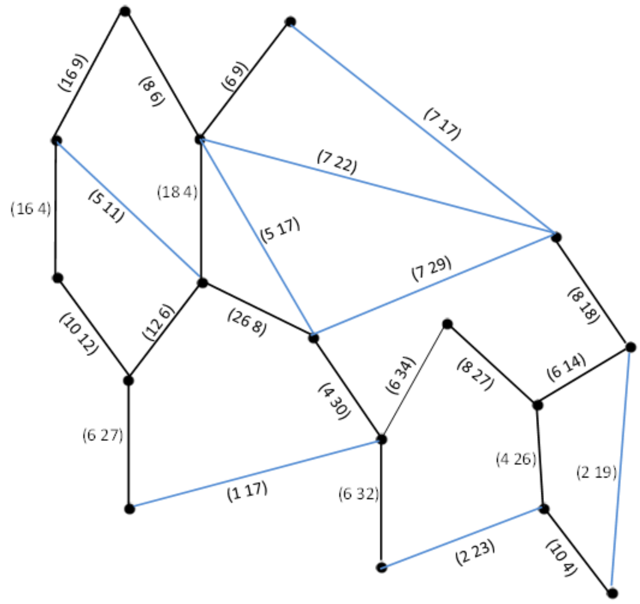


Fig.4. Encrypted molecular graph (G_3) of Lidocaine

Step 5 Send the graph to the receiver.

Decryption is done by reversing the procedure. Suppose the received graph is as illustrated in fig.5.

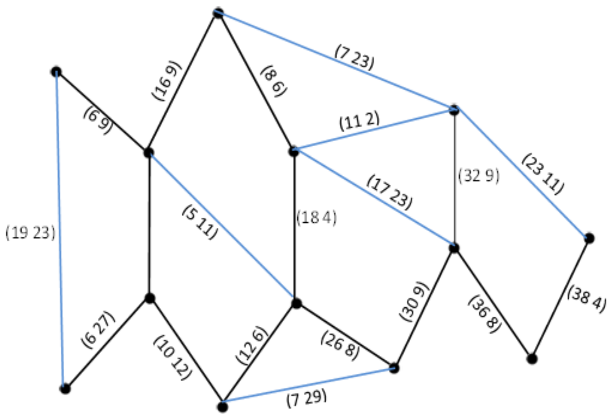


Fig.5. Encrypted molecular graph of Propanil

We choose the edges with relatively prime weights. There are 7 edges with weights (19 23), (5 11), (7 23), (11 2), (17 23), (7 29) and (23 11). Remove these edges from the graph and the graph obtained is as displayed in fig.6.

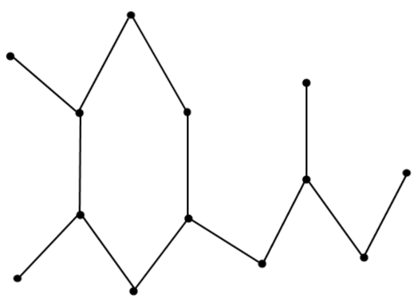
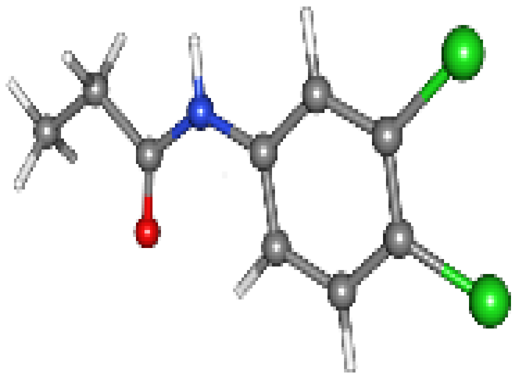


Fig.6. Molecular graph of Propanil after decryption

The molecular structure representing fig.6 is seen in snapshot 5. This molecular structure represents the herbicide Propanil, whose molecular formula is $C_9H_9Cl_2NO$.



Snapshot 5: Molecular structure of Propanil

The proposed method can be used to encrypt any product that has a molecular formula**.** In order to validate the present method, two more commodities such as a sweetening agent and Caffeine are considered for discussion. The graph representations, molecular structures and the encrypted graphs are seen in Table I.

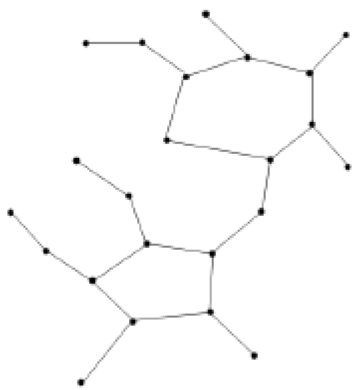
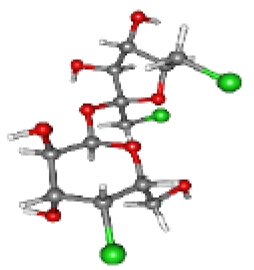
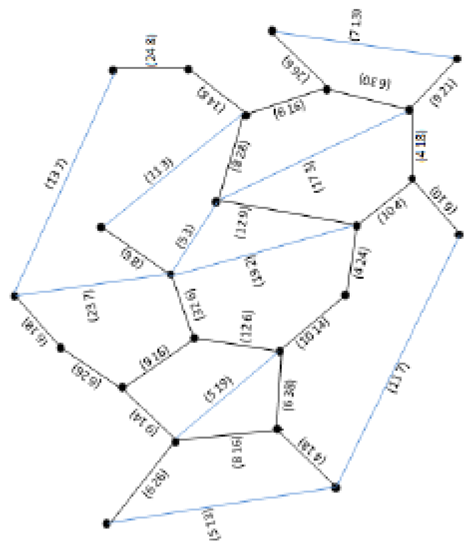
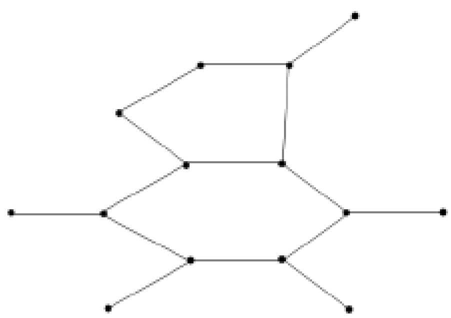
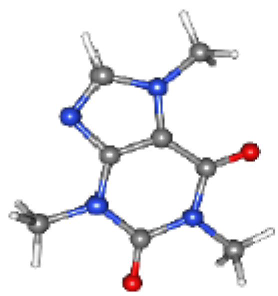
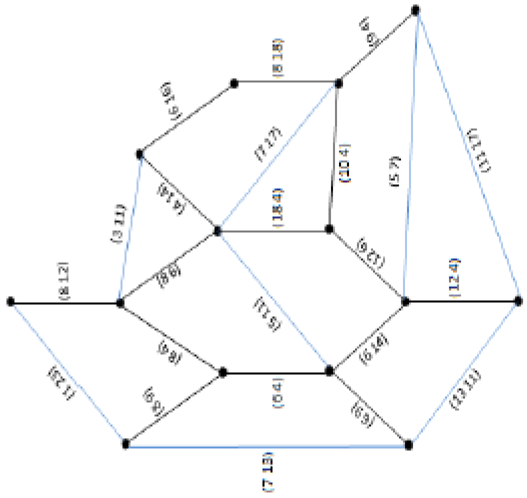
III. CONCLUSION

In developing society, discovery of any new product is expensive. Many new discoveries are of use for society and need to be approved by government appointed institutions or both. Before patenting, security of the new discoveries is in risk with modern communication methods. The proposed method helps to transfer the molecular formula of any new finding. This method

- Uses double encryption once by adding edges and again by assigning weights.
- Unless the property of relatively prime is known, decryption is almost impossible.
- Even if, a relatively prime property is decrypted, it is tough to guess the resulting graph representing the molecular graph.
- As in a complete graph, nC_2 edges are possible, if the number of additional edges added is increased in number, the encryption will really be very effective.
- A large number of graphs is available in public domain. Hence the encrypted graph can be transmitted in public domain. It would be tough to differentiate the normal and the encrypted graphs.

Hence we conclude that the present method is safe and reliable for encrypting any molecular structure.

Table I: Molecular graph, molecular structure and encrypted graph of Sucralose and Caffiene

S.No.	Molecular graph	Ball and stick diagram	Encrypted graph
1.		 Sucralose $C_{12}H_{19}Cl_3O_8$	
2.		 Caffeine $C_8H_{10}N_4O_2$	

Retrieval Number: A4693119119/2019©BEIESP
DOI: 10.35940/ijitee.A4693.119119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

REFERENCES

1. Muhammad Faheem Mushtaq, Sapiee Jamal, Abdulkadir Hassan Disina, Zahraddeen A. Pindar, Nur Shafinaz Ahmad Shakir, Mustafa Mat Deirs, “A survey on the cryptographic encryption algorithms”, Int.J. Adv. Comp. Sci. Appl., Vol:8, (11) , 2017, pp.333-344.
2. P. Amudha, A.C. Charles Sagayaraj, A.C. Shantha Sheela, “An application of graph theory in cryptography”, Int. J. Pure Appl. Math. Vol:119 (13), 2018, pp. 375-383.
3. Wael Mahmoud Al Etaiwi, “Encryption algorithm using graph theory”, J.Scientific Res.Reports, 3(19), 2014, pp. 2519-2527.
4. M. Yamuna and K. Karthika, “Data transfer using Bipartite graphs”, Int.J.Adv.Res.Sci.Engg., Vol:4(2), 2015, pp.
5. Shubham Agarwal and Anand Singh Uniyal, “Prime weighted graph in cryptographic system for secure communication”, Int.J. Pure Appl. Math., Vol: 105(3), 2015, pp. 325-338.
6. J. Dharani, V. Maheeswari and V. Balaji, “Encryption approach on Graph theory”, J. Comp. Matha., Vol:2(1), 2018, pp. 59-65.
7. 7.http://momath.org/wp-content/uploads/2013/10/graph_theory-300x292.jpeg
8. https://encryptedtbn1.gstatic.com/images
9. 9.http://mathworld.wolfram.com/CompleteGraph.html