ENCRYPTION THROUGH MOLECULAR GRAPHS

L. Shobana[1], J. Baskar Babujee[2]
[1]*Department of Mathematics*
SRM Institute of Science and Technology
Kattankulathur - 603 203, India
[2]*Department of Mathematics, Anna University*
MIT Camps, Chennai- 600 044, India.
shobanal@srmist.edu.in, baskarbabujee@yahoo.com

Abstract

Encryption and decryption mostly emerge from mathematical discipline. Molecular graphs are models of molecules in which atoms are represented by vertices and chemical bonds by edges of a graph. Graph invariant numbers reflect certain structural features of a molecule that are derived from its molecular graph, known as topological indices. A topological index is a numerical descriptor of a molecule, based on a certain topological features of the corresponding molecular graph. One of the most widely known topological descriptor is the Wiener index. Wiener number is employed to predict boiling point, molar volumes and large number of physico-chemical properties of alkenes. In this paper a new technique is employed to encrypt and decrypt message through the topological index of molecular graph using the linear congruence equations.

Mathematics Subject Classification: 05C12, 92E10

Keywords: wiener index, congruence modulo, encryption, decryption, molecular compound

1 Introduction

1.1 Chemical Graph Theory

Chemical graph theory is the topology branch of mathematical chemistry which applies graph theory to mathematical modelling of chemical phenomena. The main goal of chemical graph theory is to use algebraic invariants to reduce the topological structure of a molecule to a single number which characterizes either the energy of the molecule as a whole or its orbital's, its molecular branching, structural fragments, and its electronic structures, among others. A molecular graph G = (V, E) is a simple graph having $n = |V|$ nodes and $m = |E|$ edges. The nodes $v_i \in V$ represent non-hydrogen atoms and the edges $(v_i, v_j) \in E$ represent covalent bonds between the corresponding atoms. In particular, hydrocarbons are formed

only by carbon and hydrogen atoms and their molecular graphs represent the carbon skeleton of the molecule.

Graph invariant numbers reflect certain structural features of a molecule that are derived from its molecular graph, known as topological indices. It is also defined as those "Numerical values associated with chemical contribution for correlation of chemical structure with various physical properties, chemical reactivity or biological activity". The topological distance between a pair of vertices v_i and v_j denoted by $d(v_i, v_j)$, is the number of edges of the shortest path joining v_i and v_j. The simplest topological indices do not recognize double bonds and atom types (C, N, O etc.) and ignore hydrogen atoms ("hydrogen suppressed") and defined for connected undirected molecular graphs only.

Among the various types of topological indices, Wiener index is the oldest topological index related to molecular branching named after Harry Wiener, who introduced it in 1947. The Wiener index $W(G)$ of a graph G is defined as the sum of distances between all vertices of the graph G [1].

$$W(G) = \sum_{i<j} d(v_i, v_j)$$

Example 1.1.1 The molecular graph representing 2,2 diethyl propanol is isomorphic to star graph $K_{1,4}$. The Wiener Index of $k_{1,4}$ is 16.

Figure 1. 2,2 diethyl propanol

1.2 Cryptology

Cryptography is the art and science of concealing the meaning of confidential communications from all except the intended recipients. It starts with the unencrypted data, referred to as plaintext. Plaintext is encrypted into cipher text, which will in turn be decrypted back into usable plaintext. Cryptanalysis deals with breaking secret messages. The encryption and decryption is based upon the type of cryptography scheme being employed and some form of key. An authorized user can only decrypt data since decryption requires a secret key

or password. It is most closely associated with the development and creation of the mathematical algorithms used to encrypt and decrypt messages, whereas cryptanalysis is the science of analyzing and breaking encryption schemes. Cryptology is the term referring to the broad study of secret writing, and encompasses both cryptography and cryptanalysis.

1.2.1 Affine Ciphers

An affine cipher (like a shift cipher), is an example of a substitution cipher. Shift ciphers belong to a large family of affine ciphers defined by the formula $C \equiv aP + k (\mathrm{mod}\, 26)$ where a is a positive integer ≤ 25 and (a, 26) = 1. The condition that (a, 26)=1 guarantees that as P runs through the least residues modulo 26, so does C, it ensures that congruence $C \equiv aP + k (\mathrm{mod}\, 26)$ has a unique solution for P, $P \equiv a^{-1}(C - k) (\mathrm{mod}\, 26)$.

In this paper, we use the technique of finding the Weiner index for the graph structure from its corresponding molecular compound which in turn is used to encrypt and decrypt the message using affine ciphers.

2. Main Results

In this section, we proposed a new technique to encrypt the original message using a molecular compound. Convert the molecular compound to its corresponding graph and then finding the wiener index of the graph. Using the congruence relation $C \equiv aP + k (\mathrm{mod}\, 26)$ where a is the wiener index of G modulo 26 and k is the number of vertices of G modulo 26, we obtain sequence of encrypted numbers. Converting these numbers to letters using the normal chart, results in the encrypted message. The encrypted message contains five letters in a block. Consider the relation $P \equiv a^{-1}(C - k) (\mathrm{mod}\, 26)$ to decrypt the message. While decrypting the message, combine the letters to obtained the meaningful words as the letters in the encrypted message are arranged five in a block.

Consider the following normal chart to encrypt and decrypt the given message.

letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Ordinal number	00	01	02	03	04	05	06	07	08	09	10	11	12
letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ordinal number	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 1. Normal Chart

2.1 Algorithm for Encryption

Input: The original message *M* and a molecular compound.

Output: The encrypted message *E*.

Begin

Step 1: Convert the letters in the original message *M* to its ordinal number using the above normal chart. Let us assume the obtained sequence of ordinal numbers to be P.

Step 2: Construct the graph *G*, for the given molecular compound.

Step 3: Calculate *W*, the Wiener Index of *G* using the formula, $W(G) = \sum_{i<j} d(v_i, v_j)$.

Step 4: Compute $C \equiv aP + k \pmod{26}$ where a is the Wiener Index of *G* modulo 26 and *k* is the number of vertices of *G* modulo 26.

Step 5: From step 4, we obtain the sequence of encrypted numbers as C.

Step 6: Convert the encrypted numbers in to its corresponding letters from the normal chart, resulting in the encrypted message.

2.2 Algorithm for Decryption

Input: The encrypted message *E*

Output: The original message *M*

Step 1: From step 4, we have $P \equiv a^{-1}(C - k) \pmod{26}$.

Step 2: Solve the above linear congruence relation by varying the values of *C*, preserving the order.

Step 3: For each value of C, we obtained finite number of solutions for P. Among the finite number of solutions for *P*, we assign the initial solution to *P*.

Step 4: Convert the sequence of numbers obtained in to its corresponding letters using normal chart, which in turn result in the original message.

3. Illustration for Encryption and Decryption

3.1 Encryption

Input: The original message ***FIRE GREEN VALLEY*** and a molecular compound – Benzoic acid.

Output: The encrypted message ***TKJWQ JWWVX IBBWO*.**

- Convert the letters in the original message ***FIRE GREEN VALLEY*** to its ordinal numbers 5, 8, 17, 4, 6, 17, 4, 4, 13, 21, 0, 11, 11, 4, 24. Let us assume the obtained sequence of ordinal numbers to be *P*.
- The Molecular compound – 2 propylpentane is represented as a graph *G* with eight vertices and seven edges, whose Wiener Index is given by *W(G)= 75*.

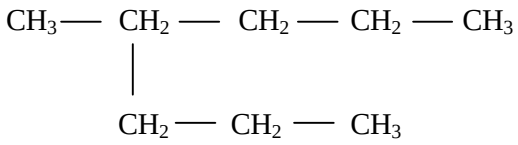

Figure 2. 2 propyl pentane

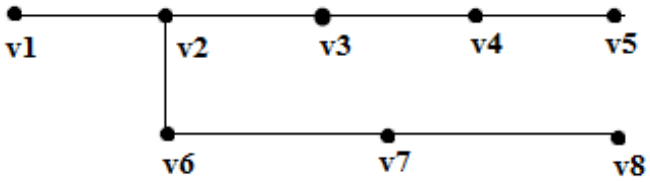

Figure 3. The graph G

- Compute $C = 23P + 8 \bmod 26$.
- We obtain the sequence 19,10,9,22,16,9,22,22,21,23,8,1,1,22,14 of encrypted numbers as *C*.
- The encrypted numbers are converted in to its corresponding letters ***TKJWQ JWWVX IBBWO***, resulting in the encrypted message.

3.2 Decryption

Input: The encrypted message ***TKJWQ JWWVX IBBWO***

Output: The original message ***FIRE GREEN VALLEY***

- Solve the linear congruence relation $23P \equiv C - 8 \bmod 26$ - (1) by varying the values of C, preserving the order.
- For each value of *C*, we obtain the finite number of solutions for *P*. Among the finite number of solutions for *P*, we assign the initial solution to *P*. For example, substitute *C* = 19 in (1), we have $23P \equiv 11 \bmod 26 -$ (2). On solving for *P*, we get *P*= 5.

- Convert the sequence of numbers 5, 8, 17, 4, 6, 17, 4, 4, 13, 21, 0, 11, 11, 4, 24 obtained in to its corresponding letters ***FIRE GREEN VALLEY***, which is the required original message.

4. Conclusion

There are so many emerging methods to encrypt and decrypt the given message. In this paper, a new idea is used to encrypt and decrypt the message through topological index especially the Wiener index of a chemical compound using congruence equations. Using different topological indices for a molecular graph of a chemical compound along with the congruence relations for encryption and decryption of a message is our future work. A new labeling technique can be used to encrypt pin numbers(secret numbers) using various graph structures to complicate the encryption which can used in ATMs, banks and military for sharing the secret data.

5. References

1. J. Baskar Babujee , "On Graph coding", The Mathematics Education, Vol XXXIX, No.3, 2005.
2. J. Baskar Babujee and J. Senbagamalar, Wiener Index of Graphs using Degree Sequence, Applied Mathematical Sciences, Vol. 6, 2012, no. 88, 4387 – 4395.
3. J. Baskar Babujee and S. Babitha, Encrypting and Decrypting Number using Labeled Graphs, European Journal of Scientific Research, Vol. 75, No. 1, 2012, pp. 14–24.
4. D. Bonchev and D.H. Rouvray, Chemical Graph Theory, Introduction and Fundamentals, Mathematical Chemistry Series, Abacus Press/Gordon & Breach Science Publishers, 1991.
5. J. A. Bondy and U. S. R. Murthy, Graph Theory with Applications, Elsevier Science Publishing. Co.Inc,1982.
6. J.A. Gallian, A dynamic survey of graph labeling, The Electronic Journal of Combinatorics, #DS6, 2019.
7. Nenad Trinajstic, Chemical Graph theory, Vol II, CRC Press, Inc. Boca Raton, Florida, 115–116.
8. A. Rosa, On certain valuations of the vertices of a graph, Theory of Graphs

Internet. Symposium, Rome, Gordon and Breach, NY (1967), Dunod, Paris , 1966, pp. 349–355.

9. S.G. Telang, Number Theory, Tata McGraw-Hill Publishing company limited, 1996.
10. Thomas Kohsy, Elementary Number Theory with Applications, Second Edition, Academis Press,Elsevier, 2007.
11. W.D.Wallis, Magic Graphs, 2001, Birkhauser.
12. H. Wiener, Structural determination of paraffin boiling points, J. Amer. Chem. Soc., 69, 1947, 17-20.