Proceedings of the Jangjeon Mathematical Society
23 (2020), No. 4, pp. 503 - 507

www.jangjeon.or.kr
http://dx.doi.org/10.17777/pjms2020.23.4.503

# A NEW CRYPTOGRAPHIC METHOD BY MEANS OF MOLECULAR GRAPHS

L. SHOBANA, J. BASKAR BABUJEE, AND ISMAIL NACI CANGUL

Abstract. Encryption and decryption, the two steps of cryptography, mostly emerge from mathematics. Both operations are done by means of several mathematical methods making use of number theory, elliptic curves, affine transformations, modular arithmetic, matrices, functions, etc. Graph theory has been in interaction with Chemistry since 1947 when Wiener used a mathematical formula, later called as Wiener index, to compare the boiling points of some alkane isomers. Since than, many mathematical methods have been used to determine the chemical and physical properties of molecular structures. In this work, a new technique has been proposed to encrypt and decrypt a secret message using a topological index of a selected molecular graph to avoid the interference of adversaries.

2010 Mathematics Subject Classification. 05C12, 92E10. 20G40, 94B05.

Keywords and phrases. Wiener index, congruence, encryption, decryption, molecular compound.

## 1. Introduction

1.1. **Chemical graph theory.** Chemical graph theory is the topological 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 modelling a chemical molecule. 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. For general notions related to chemical graph theory, see e.g. [1, 2].

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 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 $G$, [3], as

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

**Example 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.*

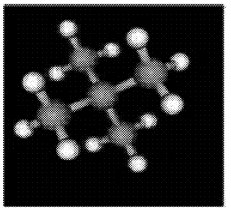

***Figure 1*** *2,2 diethyl propanol*

1.2. **Cryptology.** Cryptography is the art and science of concealing the meaning of confidential communications from all except the intended recipients. The data before encryption is referred as plaintext. It is encrypted into a ciphertext, which will in turn be decrypted back into usable plaintext. Cryptanalysis deals with breaking secret messages. The encrypting and decrypting the message is based upon the type of cryptography scheme being employed and some form of key. A secret key or password is required for the authorized user to decrypt the data. 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 $C \equiv aP + k \pmod{26}$ where $a$ is a positive integer $\leq 25$ 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 the congruence $C \equiv aP + k \pmod{26}$ has a unique solution for $P$, $P \equiv a^{-1}(C - k) \pmod{26}$.

In this paper, we use the technique of finding the Wiener 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. Graphs have been used in coding, see e.g. [4, 6, 5]. We convert the molecular compound to its corresponding graph and then find the Wiener index of the graph. Using the congruence relation $C \equiv aP + k \pmod{26}$ where $a$ is the Wiener index of $G$ modulo 26 and $k$ is the number of vertices of $G$ modulo 26, 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 $P \equiv a^{-1}(C - k) \pmod{26}$ 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** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **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** |
| **Number** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** | **25** |

**Normal chart**

2.1. **Algorithm for encryption. Input**: The original message $M$ and a molecular compound.
**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 $G$ and $k$ is the number of vertices of $G$ such that $gcd(a, k) = 1$.
**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.
**Output:** The encrypted message $E$.

2.2. **Algorithm for decryption. Input:** The encrypted message $E$
**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.

**Output**: The original message $M$

## 3. Illustration for encryption and decryption

3.1. **Encryption. Input**: The original message ***FIRE GREEN VALLEY*** and a molecular compound, Benzoic acid.
**Step 1:** 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 $P$.
**Step 2:** The molecular compound, 2 propylpentane, is represented as a graph $G$ with eight vertices and seven edges, whose Wiener index is given by $W(G) = 75$.

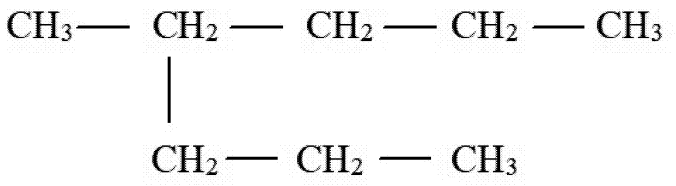


**Figure 2** 2-propyl-pentane

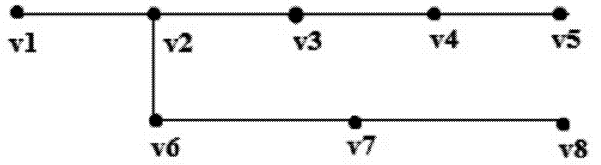


**Figure 3** The graph $G$

**Step 3:** Compute $C = 23P + 8 \mod 26$.
**Step 4:** We obtain the sequence $19, 10, 9, 22, 16, 9, 22, 22, 21, 23, 8, 1, 1, 22, 14$ of encrypted numbers as $C$.
**Step 5:** The encrypted numbers are converted in to its corresponding letters ***TKJWQ JWWVX IBBWO*** resulting in the encrypted message.
**Output:** The encrypted message ***TKJWQ JWWVX IBBWO.***

3.2. **Decryption. Input:** The encrypted message ***TKJWQ JWWVX IBBWO***
**Step 1:** Solve the linear congruence relation

$$23P \equiv C - 8 \mod 26 \tag{1}$$

by varying the values of $C$, preserving the order.
**Step 2:** 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 Eqn. (1), we have

$$23P \equiv 11 \mod 26. \tag{2}$$

On solving for $P$, we get $P = 5$.
**Step 3:** Convert the sequence of numbers $5, 8, 17, 4, 6, 17, 4, 4, 13, 21, 0, 11, 11, 4, 24$ to its corresponding letters to get ***FIRE GREEN VALLEY*** which is the

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

## 4. Conclusion

There are so many emerging methods to encrypt and decrypt a given secret message. In this paper, a new idea is used to encrypt and decrypt a message by a topological graph index, especially the Wiener index of a selected chemical compound using congruence equations. Using different topological indices of a molecular graph of a chemical compound by means of some linear congruence relations for encryption and decryption of a message is our future work. The similar operations can be applied by using any topological graph index and any molecular structure. A new labeling technique can be used to encrypt pin numbers (secret numbers) using various graph structures to complicate the encryption which can be used in ATMs, banks and military services for sharing the secret data securely. An open problem is to compare the topological graph indices and molecular structures to find the most advantegous couple.

## References

[1] Bonchev, D and Rouvray, DH. Chemical Graph Theory, Introduction and Fundamentals. Chemistry Series, Abacus Press/Gordon and Breach Science Publishers, New York, 1991.
[2] Trinajstic, N. Chemical Graph Theory. 2nd ed. CRC Press Inc. Boca Raton, Florida, 2019.
[3] Wiener, H. Structural determination of paraffin boiling points. J. Amer. Chem. Soc., 1947;69:17-20.
[4] Babujee, JB. On Graph Coding. The Mathematics Education, 2005;39(3):138-141.
[5] Babujee, JB and Senbagamalar, J. Wiener Index of Graphs using Degree Sequence. Applied Mathematical Sciences, 2012;88(6):4387-4395.
[6] Babujee, JB and Babitha, S. Encrypting and Decrypting Number using Labeled Graphs. European Journal of Scientific Research, 2012;75(1):14-24.

Dept. of Mathematics, SRMIST Kattankulathur-603203 India
*Email address*: shobanal@srmist.edu.in

Dept. of Mathematics, Anna University, MIT Campus, Chennai- 600044 India
*Email address*: baskarbabujee@yahoo.com

Dept. of Mathematics, Bursa Uludag University, 16059 Bursa, Turkey
*Email address*: cangul@uludag.edu.tr