Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 4, pp. 1175–1182
DOI : 10.47974/JDMSC-1564

More secure on the symmetric encryption schemes based on triple vertex path graph

Muhaimen Khudhair Shathir *
Ghassan Ezzulddin Arif †
Department of Mathematics
Education College for Pure Sciences
University of Tikrit
Tikrit
Iraq

Ruma Kareem K. Ajeena §
Department of Mathematics
Education College for Pure Sciences
University of Babylon
Babil
Iraq

Abstract

A triple vertex (TV) and triple vertex path (TVP) graph are defined as new concepts. These concepts consider the main point of this work to modify the symmetric encryption (SE) schemes and increase the security level in comparison with the previous ES schemes. In proposed ES schemes, the ciphertexts of the plaintexts are sent to the receiver entity as the TVP graph. Two study cases of the proposed TVPG-SE schemes are presented as new experimental results. The security issues of the proposed TVPG-SE schemes have been determined. The TVPG-SE schemes consider new insights for more secure communications.

Subject Classification: *68P25, 05E10.*

Keywords: *Cryptography, SE schemes, Graph theory, TV graph, TVP graph, Security.*

* *E-mail:* **muheiman.k.shathir@st.tu.edu.iq (Corresponding Author)**
† *E-mail:* **pure.ruma.k@uobabylon.edu.iq**
§ *E-mail:* **ghasanarif@tu.edu.iq**

1. Introduction

Several mathematical problems are solved using the fundamental concepts of Graph theory by creating the models of relations. Many mathematician researchers employed the graph theory as an influence in cryptography [1].

In 2019, Jaya Shruthy, and V. Maheswari [2] proposed a double encryption process of secret text by using the different labeling of signed graphs and Vigenere cipher. In 2020, Wei Zhang et al [3], proposed an approach for creating a random Hamiltonian path for an image encryption algorithm. In 2021, Ruma Ajeena [4] presented the soft graphic ISD (SG-ISD) method by employing the connected sub-graphs of an undirected simple graph, which formed a soft graph (F, A) generated by a set-valued function F. Also, in the same year, Karrar Aljamaly and Ruma Ajeena [5] presented a new graph based on the scalar multiplication operation on an elliptic curve defined over a prime field which is considered a key point to design a new version of an asymmetric encryption scheme. In 2022, H. Ibrahim, et al [6] provided an algorithm for a new triple system, called a Butterfly triple system which developed a starter of cyclic near-resolvable (v-1/2)-cycle system of a complete graph.

In this work, two graphs triple vertex (TV) and triple vertex path (TVP) graphs are defined as the main point to design new versions of the symmetric encryption schemes. The outline of this work includes: Section 2 introduces new definitions of the graphs which are called the triple vertex (TV) and triple vertex path (TVP) graphs with examples to explain them. Section 3 discusses the symmetric encryption schemes using the proposed graphs based on the English alphabet values in the first scheme and based on the ASCII values in the second scheme. Section 4 introduces the study cases of these encryption schemes. Furthermore, in Section 5, the security considerations of the proposed encryption schemes are determined. Finally, Section 6 presents the conclusions.

2. The Proposed Triple Vertex Graph

The triple vertex graph is defined as the main point for this work this graph is called a tripe vertex graph (TVG) that is presented as follows:

Definition 1L (TVG). Let G(V,E) be a simple graph. The order of G is equal n with n ≥ 3. The triple vertex $TVG_3(G)$ is a graph whose vertex set V such that two vertices {x,y,z} and {u,v,t} are adjacent if and only if $|\{x,y,z\} \cap \{u,v,t\}| = 2$ and if x= u and y= v then z and t are adjacent in G.

Example 1: (The $TVG_3(G)$). Let G be a simple graph that has 5 vertices and 7 edges as shown in Figure 1 (a). The $TVG_3(G(5,7))$ of G(5,7) is given in Figure 1 (b).

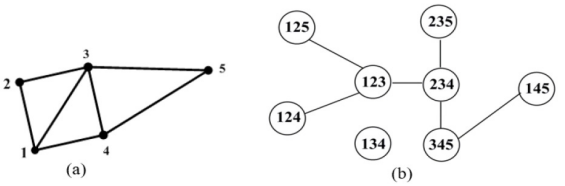

Figure 1

(a) A simple graph G (5,7), (b) The TVG_3 (G (5, 7)).

Based on definition (1), one can propose another new definition, when a graph G is a path graph P_n. This definition is given by

Definition 2: (TVGP) Let P_n be a path graph of order n. This means, that this path has n vertices 1,2,…,n such that the edges of it are (i,i+1) where i=1,2,…,n-1 The triple vertex graph of the path is denoted by $TVG_3(P_n)$.

Example 2: Let P_5 be the path that has 5 vertices and 4 edges, as shown in Figure 2.

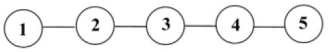

Figure 2

The path graph P_5.

The $TVG_3(P_5)$ is given in Figure 3.

3. The Triple Vertex Path Graph for Symmetric Encryption Schemes

In this section, two symmetric encryption schemes are proposed. One of them depends on the English Alphabet values (EAVs) and another one is based on the ASCII values table. These schemes are employed the TVPG to

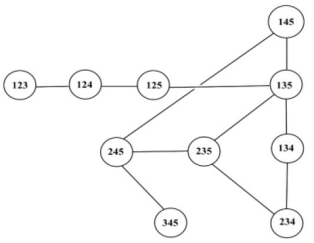

Figure 3

The $TVG_3(P_5)$ of path graph P_5.

Compute the ciphertext of the plaintext as a TVPG which is sent to the receiver. The discussion of these schemes is done as follows:

3.1 *The TVPG for Encryption Scheme Based on the EAVs*

Suppose $M=\{m_1,m_2,\ldots,m_n\}$ is a plaintext given as an English word or English sentence. A shared secret key K between two users, sender and receiver, is computed using the Diffie-Hellman key exchange [7]. The ciphertext C is computed by $C_i \equiv m_i + K \ (mod\ 26)$, with $i=1,2,\ldots,n$. A path graph P_{C_i} is formed based on the components of the ciphertext C_i for $i=1,2,\ldots,n$. In other words, $P_{C_i} = \{C_1, C_2, ..., C_n\}$. The triple vertex path graph $\mathrm{TVG}_3(P_{C_i})$ of a path graph P_{C_i} is computed and sent to the receiver as a ciphertext of M by the sender. After the second user (receiver) receives the $\mathrm{TVG}_3(P_{C_i})$, he/ she wants to decrypt the ciphertext and recover the original plaintext. He/ She first determines the label vertices of the TVG_3 (P_{C_i}). Later on, he/she takes the path graph into numbers. And since a key is a shared secret key between sender and receiver, so the second user (receiver) can recover the original plaintext only the letters from vertices (the encrypted letters) without repeating to form the correct path P_{C_i}. The English alphabetic values (EAVs) are used to convert the encrypted letters of the correct easily by $m_i \equiv C_i - K \ (mod\ 26)$, with $i=1,\ldots,n$. In other words, $\{m_1,\ldots,m_n\} = M$.

3.2 *The TVPG for Encryption Scheme Based on the ASCII Values*

The same idea of the TVPG scheme that uses EAVs can be applied to encrypt the plaintext m using the ASCII values. Using ASCII, the number of the allowed letters that can be chosen is 127. The ciphertext C of a message M is computed by $C_i \equiv m_i + K \ (mod\ 127)$, with $i=1,2,\ldots,k$ and sent to the receiver as $\mathrm{TVPG}_3(P_{C_i})$. Upon the second user receives the TVPG_3 (P_{C_i}), he/she determines the label vertices of a graph $\mathrm{TVG}_3(P_{C_i})$. Later on, he/she takes only the letters from vertices (the encrypted letters) without repeating to form correct path P_{C_i}. Using ASCII values table to convert the encrypted letters in the correct path graph into numbers. And since a key is a shared secret key between sender and receiver, so the second user (receiver) can recover the original plaintext easily by $m_i \equiv C_i - K \ (mod\ 127)$, with $i=1,\ldots,k$. In other words, $\{m_1,m_2,\ldots,m_k\} = M$.

4. The Computational Results on Proposed Symmetric Encryption Schemes

This section discusses two study cases of the proposed encryption schemes as follows:

4.1 *Study Case on the TVPG for Encryption Scheme Based on the EAVs*

Suppose a plaintext M is given by the word "**WORLD"**. Now, M is converted into numbers by $W \rightarrow 22$, $O \rightarrow 14$, $R \rightarrow 17$, $L \rightarrow 11$, $D \rightarrow 3$. With a shared secret key $K = 5$. The ciphertext C is computed by C = {B,T,W,Q,I} and it forms a path graph as shown in Figure 4.

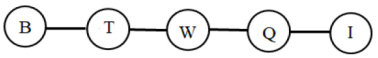

Figure 4

The path P_5 of the ciphertext BTWQI.

The TVG of P_5 is given in Figure 5 and sent to the receiver by the sender.

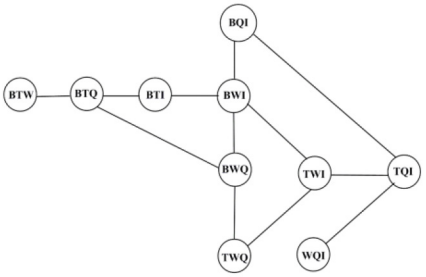

Figure 5

The TVPG of the path P_5 of the ciphertext BTWQI.

The second user (receiver) receives a ciphertext as a triple vertex graph. He/ She first determines the label vertices BTW, BTQ, BTI, BWQ, BWI, BQI, TWQ, TWI, TQI, and WQI of the TVG(P_5) graph. Later on, he/ she takes only the letters from vertices without repeating them to form a path graph of the ciphertext. There are many cases to determine the correct path graph. The correct one is BTWQI. Now, based on ASCII values table, the encrypted letters are converted into numbers $B \rightarrow 1$, $T \rightarrow 19$, $W \rightarrow 22$, $Q \rightarrow 16$, $I \rightarrow 8$. Since the shared secret key K is equal to 5, so, the original message is WORLD.

4.2 *Study Case on the TVPG for Encryption Scheme Based on the ASCII Values*

Suppose M is the plaintext that is given by the word **Matrix**. Based on the ASCII Table, the plaintext M is converted into numbers by $M \rightarrow 77$, $a \rightarrow 97$, $t \rightarrow 116$, $r \rightarrow 114$, $i \rightarrow 105$, $x \rightarrow 120$. Since a shared secret key K is equal to 6, so the ciphertext of M is $C = Sgzxo\sim$. A path graph of the cipher text is created as shown in Figure 6.

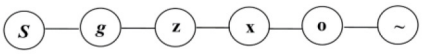

Figure 6

The path P_6 of the ciphertext *Sgzxo~*.

The TVPG(P_6) of a path graph is created as shown in Figure 7 which is sent to the receiver by the sender.

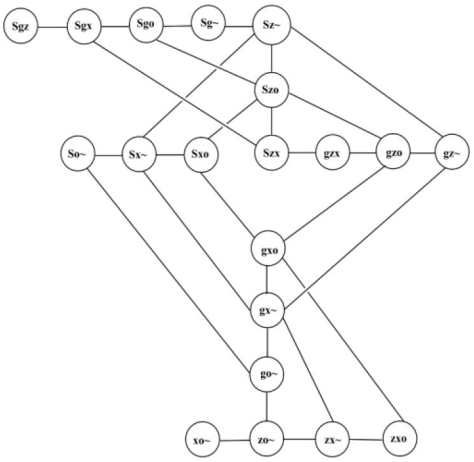

Figure 7

The TVPG(P_6) of the ciphertext *Sgzxo~* .

The second user (receiver) receives the TVPG(P_6) that is shown in Figure 7, he/ she wants to decrypt the ciphertext and recover the original plaintext. He/ She first determines the label vertices Sgz, Sgx, Sgo, Sg~, Szx, Szo, Sz~, Sxo, Sx~, So~, gzx, gzo, gz~, gxo, gzx, go~, zxo, zx~, zo~, and xo~. Later on, he/she takes only the letters from vertices without repeating to form a list. There are many cases to determine the correct choice of this list. The correct one is *Sgzxo~*. Using ASCII Table values, these letters are converted into numbers $S \rightarrow 83$, $g \rightarrow 103$, $z \rightarrow 122$, $x \rightarrow$

120, $o \rightarrow 111$, $\sim \rightarrow 126$. Since the shared secret key is equal 6, so the original message is Matrix.

5. The Security Considerations on the Proposed Symmetric Encryption Schemes

The security considerations of new proposed encryption schemes depended on secret generating of a path graph P_C that the attackers want to know it if they determine the ciphertext is computed as TVP graph. So, Eve needs to guess the vertices of graph P_C and also the shared secret key. Therefore, in case I, there are 26 possible probabilities to form the correct path graph. Thus, the total probability can be determined by:

$$C_k^n = \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Based on the result of Case (4.1), with n = 26 and K =5, then C_5^{26} = 65780 paths have existed, and one of them is the correct one. Whereas the probability of all possible path graphs, in study case (4.2), is computed by C_5^{27} = 254231775 paths, one is the correct that gives the correct original plaintext. So, if the adversaries know a ciphertext of a plaintext m is computed by P_C and represented and sent as the TVP graph, they need to guess more and more probability cases to generate the graphs P_C. Thus, it is more secure to recover the original message among all possible probabilities cases.

6. Conclusions

This work proposes two new graphs, which are called TV and TVP graphs. The TVP graph is used to give new contributions through propositional and symmetric encryption schemes. The proposed TVPG-SE schemes depend on using the EAVs and ASCII values. The study cases on the TVPG for proposed encryption schemes have been presented. The security considerations of TVPG-SE schemes are determined. The TVPG-SE schemes are more secure in comparison with previous ones.

References

[1] M. Polak, et. al. "On the applications of extremal graph theory to coding theory and cryptography," *Electronic Notes in Discrete Mathematics*, Vol. 43, pp. 329-342 (2013).

[2] J. Shruthy, and V. Maheswari, "Double Encryption, Decryption Process Using Graph Labeling Through Enhanced Vigenere Cipher," *Journal of Physics: Conference Series*, IOP Publishing, Vol. 1362, No. 1 (2019).

[3] W. Zhang, "An Image Encryption Algorithm Based on Random Hamiltonian Path," *Entropy*, Vol. 22, No. 1, pp. 73 (2020).

[4] R. Ajeena, "The soft graphic integer sub-decomposition method for elliptic scalar multiplication," *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 24, No 6 pp. 1751-1765 (2021).

[5] K. Aljamaly, and R. Ajeena, "The elliptic scalar multiplication graph and its application in elliptic curve cryptography," *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 24, No 6 pp. 1793-1807 (2021).

[6] H. Ibrahim, Raja'I. Aldiabat, and Sharmila Karim "Butterfly Triple System Algorithm Based on Graph Theory," *Journal of Information & Communication Technology*, Vol. 21, No. 1, (2022).

[7] Hoffstein, Jeffrey, et. al. An introduction to mathematical cryptography. Vol. 1. New York: springer (2008).

Received February, 2022
Revised March, 2022