Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 4, pp. 1183–1188
DOI : 10.47974/JDMSC-1565

Triple vertex of cycle graph for polyalphabetic encryption scheme

Manal Hatif Kadhim *
Ruma Kareem K. Ajeena †
Department of Mathematics
Education College for Pure Sciences
University of Babylon
Babil
Iraq

Abstract

A new version of the polyalphabetic encryption scheme (PES) has been proposed based on the triple vertex cycle graph (TVCG). In the current study, a new definition for TVCG is given. The PES has been modified based on the TVCG. The security in comparison with the previous symmetric encryption schemes is increased. The ciphertext of the plaintext, in the proposed PES, is sent to the receiver entity as the TVCG. Based on cycle graph Cn, the TVCG is created depending on the encrypted letters of the plaintext bits and the rules of a secret key. In the current study, a study case of the proposed TVCG-PES is presented as a new experimental result. Then, the security issues of the TVCG-PES are determined. The TVCG-PES is considered as a new insight for more secure communications.

Subject Classification: *11T71, 14G50, 05Cxx.*

Keywords: *Cryptography, PES, Graph theory, TV graph, TVCG, Security.*

1. Introduction

Some concepts of graph theory are considered to be the fundamental tools in wide areas of mathematics, especially in cryptography. In 2020, Wei Zhang et. al. [1] used a random Hamiltonian path for image encryption algorithm. A SG-ISD method for elliptic scalar multiplication is proposed by Ruma Ajeena [2] in 2021. Also, in 2021, Aljamaly and Ajeena

* *E-mail:* **manal.hatef.pure267@student.uobabylon.edu.iq**
(Corresponding Author)
† *E-mail:* **pure.ruma.k@uobabylon.edu.iq**

[3] defined elliptic scalar multiplication graph as a new graph to design a new asymmetric encryption scheme. In 2022, **Ghani** et. al. [4] proposed a system depending on two principles encryption and steganography using the graph theory properties. In the current study, a new graph is created based on a cycle graph, this graph is called TVCG. The outline of this work consists of six sections: Section 1 in an introduction to the current work. Section 2 introduces new graph that is TVCG with examples to explain it. Section 3 discusses a polyalphabetic encryption scheme using the TVCG. Section 4 introduces a study case of the PES. Furthermore, in Section 5, the security considerations of the PES are determined. Finally, Section 6 draws the conclusions.

2. The Proposed Triple Vertex Cycle Graph

The TVCG is defined as a main point for this work. But before presenting this definition, the triple vertex graph (TVG) should be defined:

Definition 2.1: (TVG). The $TVG_3(H)$ which is a triple vertex graph whose vertex set H(V) such that two vertices {a,b,c} and {d,e,f} are adjacent if and only if $|\{a,b,c\} \cap \{d,e,f\}| = 2$ and if a= d and b= e then c and f are adjacent in H, where H is a simple graph of order n, $n \geq 3$.

Based on Definition (2.1), one can propose a new definition, when a graph H is a cycle graph C_n. This definition is given by:

Definition 2.2: (TVCG). Let C_n be a cycle graph has n vertices and n edges. The $TVG_3(C_n)$ is a triple vertex graph of cycle C_n.

Example 2.1: A cycle graph C_6 that is shown in Figure 1 can be represented as $TVG_3(C_6)$ based on all intersected vertices that have distances 2. The $TVG_3(C_6)$ is given in Figure 2.

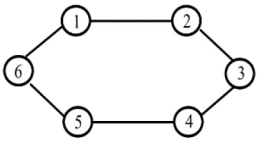

Figure 1

A cycle graph C_6.

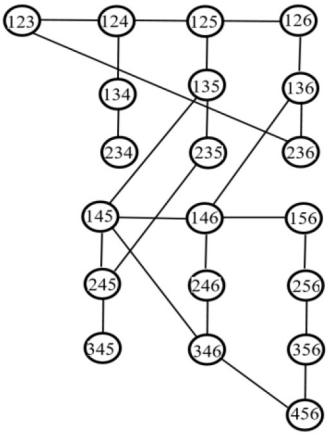

Figure 2

The TVG3 (C_6) of a cycle graph C_6.

3. The TVCG for Polyalphabetic Encryption Scheme

In this section, a new proposed polyalphabetic encryption scheme [5] using the TVCG is discussed. Let *M* be a plaintext. The letters of plaintext can be represented as the English alphabet values that are: A = 0, B = 2,…, Z = 25, (Also, it is possible to use ASCII values). A secret key takes several rules for shifting the letters of *M* into right or left positions of numbers. A ciphertext *C* of M is computed and represented as a cycle graph C_n. Using C_n the $TVG_3(C_n)$ is formed and sent as a ciphertext to receiver.

The ciphertext reaches to the receiver as $TVG_3(C_n)$. The decryption process is done to recover *M*. The label vertices of the $TVG_3(C_5)$ are determined. The vertices (that are letters) are selected as list without repeating. Many cases are determined but one of them is correct. On a secret key, the inverse rules are determined. The encrypted letters are decrypted using the English alphabetic values. An original plaintext has been recovered.

4. A Study Case for the Polyalphabetic Encryption Scheme Based on TVC

This section discusses a study case of the polyalphabetic encryption scheme based on TVCG. Suppose a plaintext M is a plaintext with a word is *apple*. Using polyalphabetic cipher based on the English alphabet values of the letters and the rules of the key:

i. Shift first letter two positions into the right.
ii. Shift second letter five positions into the right.
iii. Shift third letter four positions into the right.

results

app le → cut ni.

So the encrypted letters are cutni. Now, the ciphertext cutni is represented by cycle graph as displayed in Figure 3.

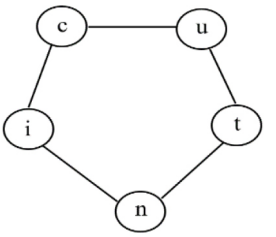

Figure 3

The cycle C_5 of the cutni.

The $TVG_3(C_5)$ of C_5 is computed by:

$\{c,u,t\} \cap \{c,u,n\} = \{c,u\} \rightarrow |\{c,u,t\} \cap \{c,u,n\}| = 2$ $\{c,u,n\} \cap \{c,u,i\} = \{c,u\} \rightarrow |\{c,u,n\} \cap \{c,u,i\}| = 2$

In similar way, one can compute all other intersections. The ciphertext is represented by $TVG_3(C_5)$, as given n Figure 4 which sending to receiver.

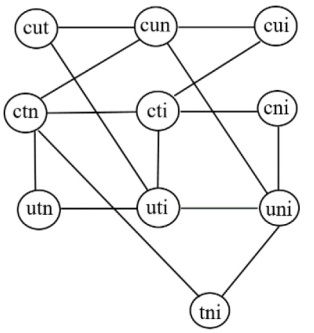

Figure 4

The $TVG_3(C_5)$ of the cutni.

The $TVG_3(C_5)$ has been received by second entity. Firstly the label vertices are determined by cut, cun, cui, ctn, cti, cni, utn, uti, uni, and tni of the $TVG_3(C_5)$. Many cases are determined, the correct one is cutni.

The inverse rules of secret key are

i. Shift first letter two positions into the left.

ii. Shift second letter five positions into the left.

iii. Shift third letter four positions into the left.

The ciphertext cut ni converted into *app le*. Thus, the original plaintext is *apple*.

5. The Security Considerations on the Proposed Symmetric Encryption Schemes

On a new proposed PES, a secret generating of C_n considers as a key secure point of the security considerations that the attackers need to know. If the computation of ciphertext is determined as TVCG then Eve needs to guess the vertices of C_n. Another points that is needed to determine is the rules of a secret key. Thus, there are 26 possible case to create the correct C_n. Hence, the total number of the probability is computed by

$$C_5^{26} = \frac{26!}{5!(26-5)!} = 65780.$$

where $p = 26$ and the vertices of C_n is 5. So, there are 65780 cases which are corresponded to the plaintext, one of them is correct. So, a more secure communication with PES is using the TVCG. If one applies the proposed version with ASCII values, then there are 254231775 cases, one of them is correct to recover the original plaintext because

$$C_5^{127} = \frac{127!}{5!(127-5)!} = 254231775.$$

6. Conclusions

This work employs a cycle graph to create a new graph that is called TVCG. The TVCG is used to design a new version of PES based on English alphabet (it is possible to use the ASCII values). The English letters of a plaintext is converted into numbers of the English alphabet values (or ASCII values), which is encrypted using the rules of a secret key that are determined secretly. The TVCG is formed based on a cycle graph that is correspondent to the ciphertext. The TVCG is sent to the receiver as a ciphertext. The security considerations are determined by the proposed

PES based on TVCG. The proposed PES is more secure for communication in comparison with other symmetric encryption schemes.

References

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

[2] R. Ajeena, "The soft graphic integer sub-decomposition method for elliptic scalar multiplication," *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 24, Bo 6 pp. 1751-1765 (2021).

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

[4] S. Abdul-Ghani, R. Abdul-Wahhab, & E. Abood. "Securing Text Messages Using Graph Theory and Steganography," *Baghdad Science Journal* 19.1, 0189-018 (2022).

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

[6] Shubham Sharma & Ahmed J. Obaid, Mathematical modelling, analysis and design of fuzzy logic controller for the control of ventilation systems using MATLAB fuzzy logic toolbox, *Journal of Interdisciplinary Mathematics*, 23:4, 843-849 (2020), DOI: 10.1080/09720502.2020.1727611.

Received February, 2022

Revised March, 2022