Scientific Hub of Applied Research in Engineering & Information Technology

Received: 26.05.2022 Revised: 09.06.2022 Accepted: 15.06.2022

*Research Article*

# Data Encryption using Graph Domination

K. Karthika*[1]

[1] *Department of Mathematics, School of Advanced Sciences, VIT Vellore, Tamilnadu, India.*

In this modern world, every industry and organization has tough competition to sustain. So, everyone needs to develop their own ideas to keep their organization exists in good condition. The new technology, innovation and updates are very confidential until it will be declared officially. It is mandatory to maintain the data and communicate the information safe from hackers and other external sources. Encryption and decryption help us to prevent and send the details in safe mode. Using graph theory in cryptography is developing as a promising field. Domination theory in the encryption process is rarely used. A new data encryption method using graph function and control number is discussed in this paper. A sample output using MATLAB program also provided using the same procedure.

*Keywords:* Encryption, Decryption, Domination number, Graph theory.

## 1. Introduction

Encryption is the method of interpreting plaintext into something that seems to be meaningless, which may be called ciphertext. "The method of converting ciphertext into plaintext is called decryption. Symmetric encryption can be used to encrypt a large amount of data. Using symmetric keys plays an important role in both the process of encryption and decryption. To decrypt a specific portion of ciphertext, the symmetric key that was used to encrypt the message must be used. The main aim of every encryption algorithm is to generate a new method and it will make complicated to decrypt the ciphertext as much as possible without using the encryption key" [3]. Graphic theory plays a major role in encryption, using graph theory in cryptography has gained a lot of attention these days.

Correspondence should be addressed to
K. Karthika; karthika.k@vit.ac.in



An encryption algorithm using graph theory properties has provided by Etaiwi. Define encryption algorithm and secure message encryption using graphical theory features [8]. In 2013, M. Yamuna et al. provide encryption and decryption of any chemical formula using stable domination separation graphs [10]. Also, they developed a new way to encrypt any tree using a new periodic binary table [9]. A method of data encryption using a circuit matrix was discussed in [5].

## 2. Preliminary note

The basic explanations and results related to the graph theory required for the proposed encryption system are described in this section.

### *2.1. Graph*

Graph G = (V, E) is a random pair of vertical V and set ed edges E, which is a subset of the vertex set V feature, i.e. the edge is a two-dimensional event and the relation is represented as a pair of random tweets with respect to the corresponding edge.

### *2.2. Weighted Graph*

Graph G is considered to be a weighted graph when a numerical value is assigned to the entire boundary of G [6]. An example of a weighted graph is given in Fig 1.

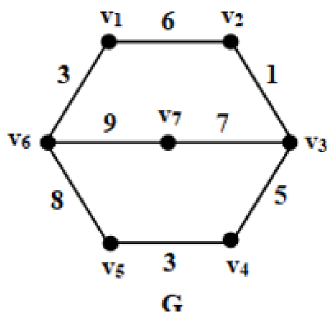



**Fig.1. G is a Weighted graph**

### *2.3. Controlling Set*

In Graphic G = (V, E), a set of texts D in G is said to dominate the set if each vertex in V - D is close to at least one vertex in D. If D has a small number of elements of any G-ruling set, then D is called the sub-rule set of G. The amount of elements in the lower G-ruling set is called the G-ruling number and is defined as $\gamma$ (G ). The governing set with a small number of G elements is called $\gamma$ - set [2].

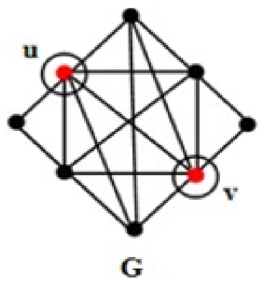



**Fig.2. { u, v } is a $\gamma$ - set for a graph G and $\gamma$ (G) = 2**

Rule D is said to be the independent rule set if there are no two situations in D nearby. Vertex v is said to be a low (critical) vertex if $\gamma$ (G – v ) < $\gamma$ ( G ).

## 3. Proposed approach

Data encryption using graph function and rule number is discussed in this section.

### *3.1. Edge Contraction*

Identifying direct pairs (u v) from G is defined as G • uv. Graph G • uv produced by G by subtracting adjacent vertices (u, v) and attaching a new vertex, say uv, where uv is adjacent to all G vertices - {u, v}, adjacent or u-u. or v in G [1].

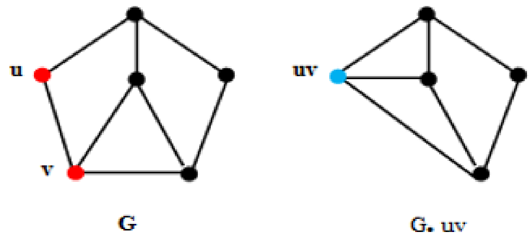



**Fig.3. Example of border compaction**

Graphic functions are widely used in various research areas. Different kinds of graph operations are available in graph theory, edge contraction is used for encrypting a given message in this paper. Consider the G graph, while the G and G control numbers •UV may or may not decrease when using edge access. If $\gamma$ ( G •uv ) = $\gamma$ (G), then the graph G is called the domination dot stable (DDS) graph [11]. We have graphs, where some edges satisfies the property and no edge satisfies the property. In this paper, the set of edges which satisfy the condition $\gamma$ ( G • uv ) = $\gamma$ ( G ) as a key for encryption.

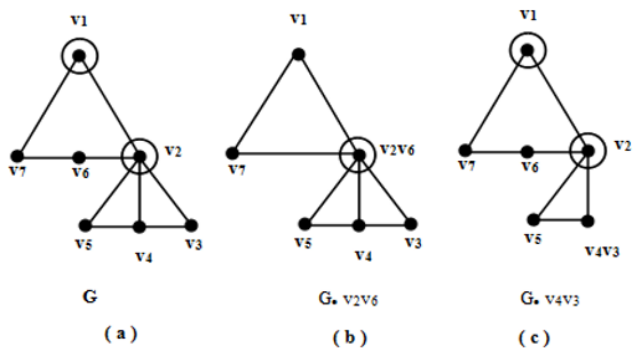



**Fig.4. (a) is a graph with $\gamma$ (G) = 2,**
**(b) is an example of $\gamma$ ( G• uv ) $\neq$ $\gamma$ (G),**
**(c) is an example of $\gamma$ ( G• uv ) = $\gamma$ (G) = 2**

We use the following results to assess the conditions

$\gamma$ ( G• uv ) < $\gamma$ (G) and $\gamma$ ( G• uv ) = $\gamma$ (G).

*Results*

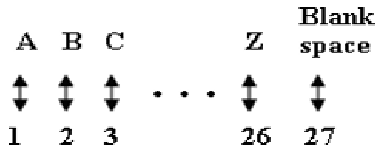
1.“Let a, b $\in$ V ( G ) for a graph G. Then $\gamma$ ( G• ab ) < $\gamma$ (G) if and only if either there exists a minimum dominating S of G such that a, b $\in$ S or at least one of a or b is critical in G [1].

2. A graph G is DDS if and only if every $\gamma$ – set of G is an independent dominating set [11]”.

### *3.2. Encryption Chart*

To encrypt a message, we can use any standard encryption chart. Sample chart is given in Table 1.

**Table 1 Encryption Chart.**




We can increase the number of characters invariably depending on the requirements of the message to encrypt.

### *3.3. Encryption Algorithm*

Consider a message that to be encrypted as M. Let us assume the length of M is equal to p.

For example, let M: GRAPHS be the given message to encrypt. Length of M = 6.

*Step 1*: In the given message M, convert the characters into numerical values using Table 1. Let $w_1$, $w_2$, $w_3$, …, $w_p$.

The required weights of the given string M are 7 18 1 16 8 19.

*Step 2:* Consider a graph G with exactly k – edges satisfying the condition $\gamma$ ( G• uv ) = $\gamma$ (G).

For our example ( $v_1$ $v_2$ ), ( $v_2$ $v_6$ ), ( $v_3$ $v_4$ ), ( $v_4$ $v_5$ ), ( $v_5$ $v_3$ ), ( $v_6$ $v_1$ ) are satisfying the above condition. A graph with exactly six edges satisfy the condition $\gamma$ ( G• uv ) = $\gamma$ ( G ) as seen in Figure 5 (a).

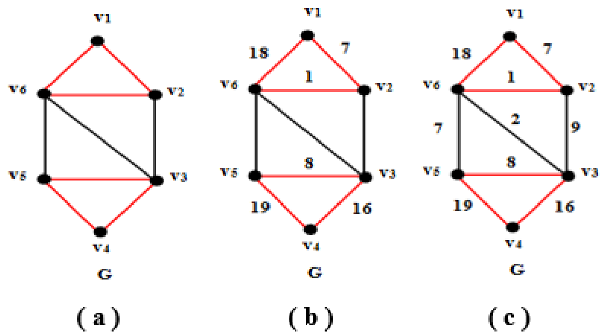



**Fig.5. Encryption Algorithm**

*Step 3:* Let X be the set of p edges that satisfy the condition $\gamma$ ( G• uv ) = $\gamma$ (G). Arrange the vertex pairs in the set X in the following order. Let vi be a vertex belongs to the set X, where i is the smallest value in the set. Collect all possible vertex pairs with vi, say ( $v_i$ $v_j$ ), where i < j and j must be in increasing order. Choose the next smallest value and repeat the same process, stop this process until p edges are selected.

Arrange the vertex pair as discussed above and assign weights { $w_1$, $w_2$, $w_3$, …, $w_k$ } edges {$e_1$, $e_2$, …, $e_k$ }.

For our example { $e_1$, $e_2$, …, $e_6$ } = { ( $v_1$ $v_2$ ), ( $v_1$ $v_6$ ), ( $v_2$ $v_6$ ), ( $v_3$ $v_4$ ), ( $v_3$ $v_5$ ), ( $v_4$ $v_5$ )} and {$w_1$, $w_2$,…, $w_6$} = { 7, 18, 1, 16, 8, 19 }.

Refer Figure 5 (b) for a graph with weights assigned to the edges selected in step 3.

*Step 4:* Assign random weights to the remaining edges of G.

*Step 5:* Send the graph G to the receiver as seen in Figure 5 (c).

### *3.4. Decryption Algorithm*

We can decrypt the graph by reversing the procedure into its corresponding data. Consider a received graph G. For example, consider the graph as shown in Fig 6.

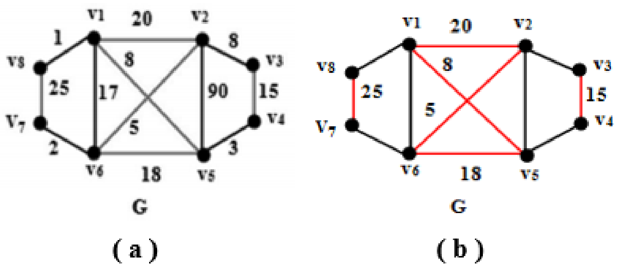



**Fig.6. (a) is a received graph. (b) is a graph G where the edges are highlighted in red color, satisfies $\gamma$ ( G• uv ) = $\gamma$ (G).**

*Step 1:* Choose the edges which satisfied the condition $\gamma$ ( G• uv ) = $\gamma$ (G).

For our example, $\gamma$ ( G ) = 3 and the edges ( $v_1$ $v_2$), ( $v_3$ $v_4$ ), ( $v_5$ $v_6$ ), ( $v_7$ $v_8$ ), ( $v_1$ $v_5$ ), ( $v_2$ $v_6$ ) which satisfies the condition $\gamma$ ( G• uv ) = $\gamma$ ( G ) = 3, as seen in Figure 6 ( b ).

*Step 2:* List the highlighted edges in increasing order.

For our example, ( $v_1$ $v_2$ ), ( $v_1$ $v_5$ ), ( $v_2$ $v_6$ ), ( $v_3$ $v_4$ ), ( $v_5$ $v_6$ ), ( $v_7$ $v_8$ ).

Step 3: Convert the weights { 20, 8, 5, 15, 18, 25 } into its corresponding character using Table 1.

The required decrypted message is THEORY.

## 4. MATLAB simulation

The sample output of encryption and decryption using MATLAB program is discussed in Figure 7 and 8.

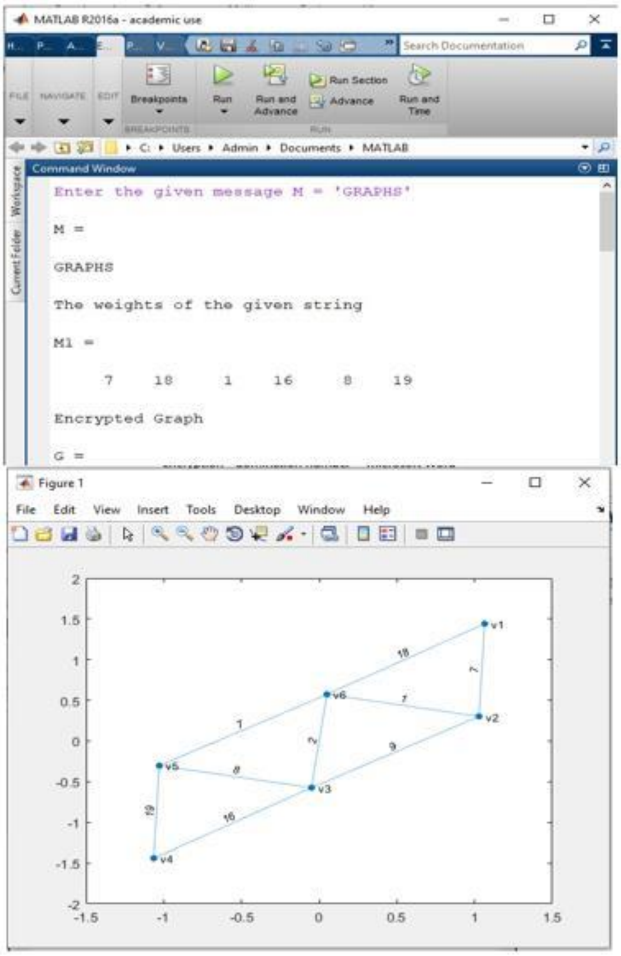



**Fig.7. The message and encrypted graph**

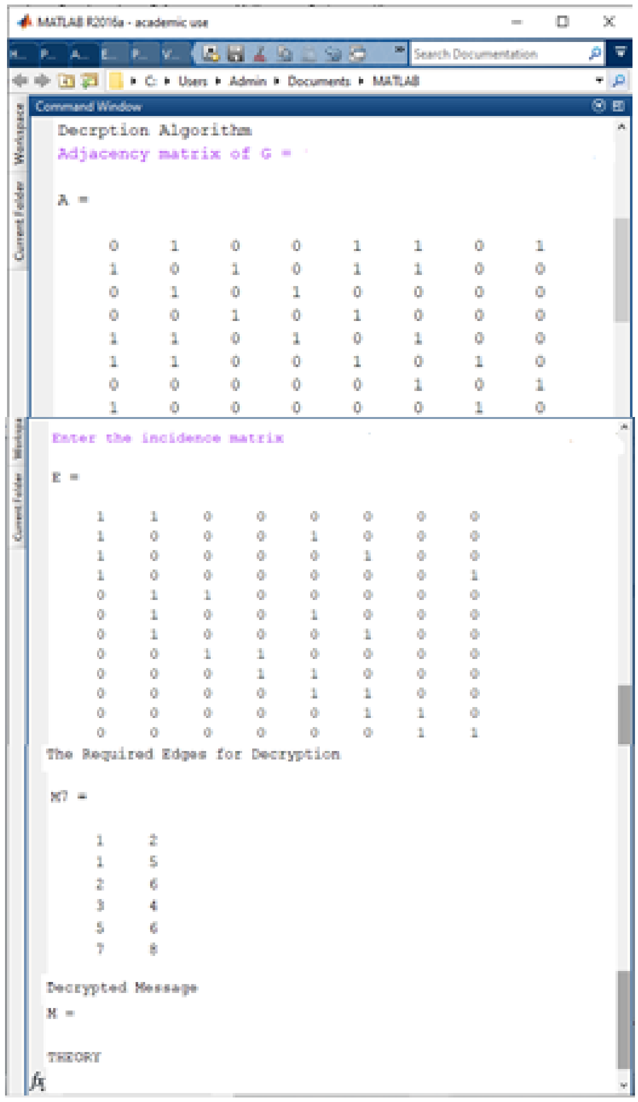



**Fig.8. The decrypted message**

## 5. Conclusion

Graphs play an important mathematical tool in many real – world problems. Graph theory properties will strengthen the safe transmission. In addition, we have used graph operation and domination property for encryption. The text may be of any length. We can create a graph with any number of vertices and edges to satisfy the structure discussed. Nowadays communicating the details to others is unavoidable. Message transmission using this method is more secure since all the edges and vertices are not used as a key for encryption. Without knowing the domination property, it is very tough to decrypt the given message. A MATLAB code also provided for the same. We conclude that the proposed method will meet the expectations on the safe transmission of any data.

## REFERENCE

[1] T. Burton and D. Sumner, "Domination Dot Critical Graphs", Discrete Math. Vol. 306, (2006), pp. 11-18.

[2] T. W. Haynes, S. T. Hedetniemi and P. J. Slater, "Fundamental of Domination in Graphs", Marcel Dekker, New York ( 1998 ).

[3] https://docs.microsoft.com/en-in/windows/win32/seccrypto/data-encryption-and-decryption?redirected from=MSDN. [online](Accessed by 24th March 2021).

[4] K. Karthika and M. Yamuna, "Domination Parameter Characterization using Matrix Representation", Indian Journal of Science and Technology, Vol. 8, No. 15, (2015), pp. 1 – 9.

[5] K. Karthika "Data Encryption using Circuit Matrix", International Journal of Scientific & Technology Research, Vol. 8, No. 12, (2019), pp. 3519 – 3522.

[6] Narsing Deo, "Graph Theory with Applications to Engineering and Computer Science", Prentice Hall India (2010).

[7] R. R. Rubalcaba, A. Schneider and P. J. Slater, "A Survey on Graphs which have Equal Domination and Closed Neighborhood Packing Numbers", AKCE J Graphs Combin., Vol. 3, No. 2, (2006), pp. 93 – 114.

[8] Wael Mahmoud Al Etaiwi, "Encryption Algorithm using Graph Theory", Journal of Scientific Research &Reports, Vol. 3, No. 19, (2014), pp. 2519 – 2527.

[9] M. Yamuna and K. Karthika, "Periodic Table as a Binary Table for Drug Encryption", Int. J. Drug Dev. & Res., Vol. 6, No. 2, (2014), pp. 52 – 56.

[10] M. Yamuna and K. Karthika. "Chemical Formula: Encryption using Graph Domination and Molecular Biology", International Journal of ChemTech Research, Vol. 5, No. 6, (2013), pp. 2747 – 2756.

[11] M. Yamuna and K. Karthika, "Excellent – Domination Dot Stable Graphs", International Journal of Engineering Science, Advanced Computing and Bio – Technology, Vol. 2, No. 4, (2011), pp. 209-216.

[12] S. Uppugalla, P. Srinivasan, J. Solid State Electrochem. 2019, 23, 295. [53]

[13] Jeevanandham, S., Dhachinamoorthi, D., Sekhar, K. B. C., Muthukumaran, M., Sriram, N., & Joysaruby, J. (2014). Formulation and evaluation of naproxen sodium orodispersible tablets " A sublimation technique. *Asian Journal of Pharmaceutics (AJP)*, *4*(1). https://doi.org/10.22377/ajp.v4i1.124

[14] Katakam P, Sriram N. Formulation and evaluation of mucoadhesive microspheres of pioglitazone hydrochloride prepared by solvent evaporation technique. Int J Biol Pharm Res 2012;3:1005-15.

[15] Sriram N. Antidiabetic and antihyperlipidemic activity of bark of Casuarina equisetifolia on streptozocin induced diabetic rats. International Journal of Pharmacy Review and Research 2011; 1(1): 4-8.

[16] Male U, Uppugalla S, Srinivasan P. Effect of reduced graphene oxide-silica composite in polyaniline: electrode material for high-performance supercapacitor. J Solid State Electrochem 2015;19(11):3381e8. [48]