Republic of Iraq
Ministry of Higher Education
and Scientific Research
University of Babylon
College of Education for Pure Sciences
Department of Mathematics

The Double Vertex Graph for Cryptography

A Research
Submitted to the Council of the College of Education for Pure Sciences in the University of Babylon In Partial Fulfillment of the Requirements for the Degree of Higher Diploma Education /Mathematics

By
Jaafar Khaled kareem mohsen

Supervised by
Asst. Prof. Dr. Ruma Kareem K. Ajeena

2021 A. D. 1443 A. H.

بسم الله الرحمن الرحيم

(يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ)

[المجادلة :١١]

Supervisor Certification

I certify that the thesis entitled the **“The Double vertex Graph for Cryptography "** by **" jaafar khaled kareem mohsen”** has been prepared under my supervision in Babylon University/ College of Education for Pure Sciences as a partial requirement for the degree of Higher Diploma in Education / Mathematics.

Signature:

Name: **Dr. Ruma Kareem K. Ajeena**

Title: **Assistant Professor**

Date: / / 2021

In view of the available recommendation, I forward this thesis for debate by the examining committee.

Signature:

Name: Dr. Azal jaafar Musa

Head of Mathematics Department

Title: Assistant Professor

Date: / / 2021

Examining Committee Certification

We certify that we have read the thesis entitled the **"The Double vertex Graph for cryptography "** by **" jaafar khaled kareem mohsen"** and as a committee examined the student in its contents and, according to our opinion, it is accepted as a thesis for the degree of Higher Diploma Education / Mathematics.

Signature:
Name: Dr . Zahir Abdul Haddi Hassan
Title: professor
Date: / / 2021

Chairman

Signature:
Name: Ali Younis Shakir
Title: Assistant Professor
Date: / / 2021

Member

Signature:

Name: Dr. Sukaina AbdAllah Lilou

Title: Lecturer

Date: / / 2021

Member /

Signature:

Name: Dr. Ruma Kareem K. Ajeena

Title: Assistant Professor

Date: / / 2021

Member / Advisor

I hereby certify the decision of the examining committee. Signature :

Name: Dr. Bahaa Hussein Salih Rabee

Title: Professor

Address: Dean of the College of Education for Pure Sciences

Date: / / 2021

Linguistic Supervisor's Certification

This is to certify that I have read this thesis entitled **" The Double vertex Graph for cryptography "** and I found that this thesis is qualified for debate.

Signature:
Name: Hassnaa Hassan Shaheed
Title: Assistant Professor

Address: Department of English, College of Education for human Sciences, University of Babylon

Date: / / 2021

Scientific Supervisor's Certification

This is to certify that I have read this thesis entitled **" The Double vertex Graph for cryptography "** and I found that this thesis is qualified for debate.

Signature:

Name: Dr.Janaan Hamza Farhood

Title: Assistant Professor

Address:

Date: / / 2021

Dedication

I dedicate this humble work
to me :

* My master and master Imam Hussein, peace be upon him .

* To the honorable parents, may God protect them and my brothers.

*To the one who supported me as I paved the path to success and filled my life with challenges and overcoming difficulties, to my beloved wife.

* And to all my friends, and those who were with me and accompanying me during my studies at the university

* And to everyone who contributed to teaching me, even with a letter, in my academic life .

*And to the martyrs of the popular crowd, the army and the police .

Aknowledge

The Almighty said: (And whoever is thankful, he is only thankful for himself). (Luqman: 12)

I thank God Almighty a great, good, and blessed thank you, full of the heavens and the earth, for the kindness with which he has given me the completion of this study, which I hope you will be pleased with.
Then I would like to express my sincere thanks and gratitude to:

Assistant Professor Dr. Ruma Kareem K. Ajeena

May God preserve her and prolong her life for her honorable kindness in supervising this research and honoring her with my advice and guidance until the completion of this research .

Researcher
Jaafar khaled kareem mohsen

Abstract

New versions of the symmetric encryption schemes are proposed in this work. These versions are used new definition of the double vertex graph (D.V.G). These new proposed schemes depended on the English alphabet values, ASCII values and the poly alphabetic cipher respectively. The message is chosen as an English word or an English sentence. The ciphertext of the original message is considered as the double vertex Graph which is sent to the receiver by sender several experimental results of the proposed encryption schemes are discussed. The security considerations of the proposed double vertex Graph encryption schemes is determined.

CONTENTS

Chapter One
General Introduction

1.1 Introduction

Cryptography is the science of secret writing with the goal of hiding the meaning of a message. Cryptography has long been the art of spies and soldiers. Nowadays, it is used everyday by billions of people for secur- ing electronic mail and payment transactions. The science of cryptography touches on many other disciplines, both within mathematics and computer science and in engineering. In mathematics, cryptology uses, and touches on, algebra, number theory, graph and lattice theory, algebraic geometry and probability and statistics. Analysis of cryptographic security leads to using theoretical computer science especially complexity theory. The actual implementation of cryptosystems, and the hardwork of carrying out security analysis for specific cryptosystems falls into engineering and practical com- puter science and computing. In this paper we have discussed and proposed an encryption-decryption algorithm using double vertex graph .

1.2 Terminology [1]

1.2.1 Cryptography: is the scientific and practical activity associated with developing of cryptographic security facilities of information and also with argumentation of their cryptographic resistance.

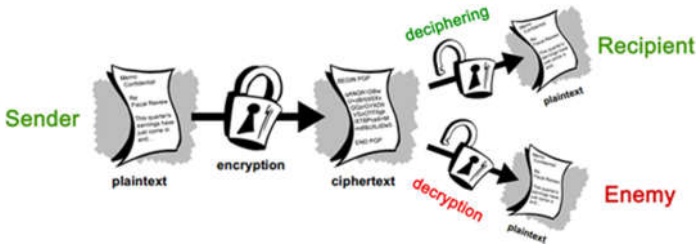
1.2.2 Plaintext : is a secret message. Often it is a sequence of binary bits.

1.2.3 Ciphertext : is an encrypted message.

1.2.4 Encryption : is the process of disguising a message in such a way as to hide its substance (the process of transformation plaintext into ciphertext by virtue of cipher).

1.2.5 Cipher : is a family of invertible mappings from the set of plaintext sequences to the set of ciphertext sequences. Each mapping depends on special parameter — a key. Key is removable part of the cipher.

1.2.6 Deciphering : is the process of turning a ciphertext back into the plaintext that realized with known key. Decryption is the process of receiving the plaintext from ciphertext without knowing the key .



1.2.7 Cryptanalysis : is the scientific and practical activity of analysis of cryptographic algorithms with the goal to obtain estimations of their cryptographic resistance.

1.2.8 Cryptology : is the concept combining both cryptography and cryptanalysis.

1.3 Cryptographic Goals [1]

1- **Confidentiality** is a service used to keep the content of information from all but those authorized to have it .

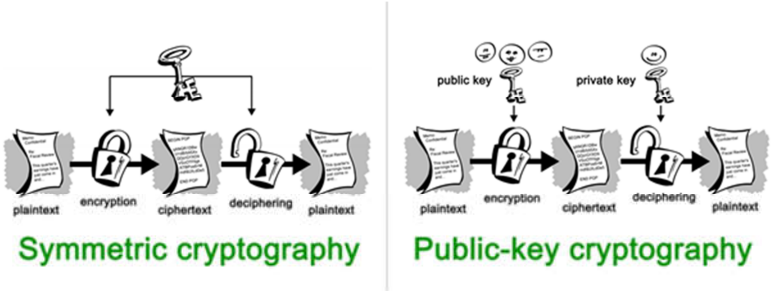
2- **Data integrity** is a service which addresses the unauthorized alteration of data .

3- **Authentication** is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other .

4- **Non-repudiation** is a service which prevents an entity from denying previous commitments or actions .

1.4 Types of Cryptographic Algorithms [1]

Symmetric algorithms (conventional algorithms) are algorithms where the encryption key can be calculated from the decryption key and vice versa.Public-key algorithms (asymmetric algorithms) are designed so that the key used for encryption (public key) is different from the key used for decryption (private key).



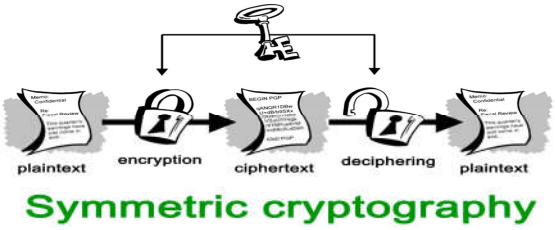
Main Principles [1]

Symmetric algorithms are algorithms in which the encryption key can be calculated from the decryption key and vice versa

⊳ Usually the encryption key = the decryption key

⊳ The sender and receiver should agree on a key before secure communication .

⊳ Security of a symmetric algorithm is guaranteed by the key; divulging the key means that anyone could encrypt and decrypt messages. As long as the communication needs to remain secret, the key should remain secret .



1.3 The problem statement of this Research

This work proposes new symmetric encryption schemes. This proposition employed using the double vertex path graph (DVPG) to increase the security level of these schemes. The security hence is determined based on encrypting the message using double vertex graph (DVPG) and sending it to the receiver.

1.4. The Structure of This Research

This research consists of five chapter :
Chapter one includes the general introduction.
Chapter two includes the mathematical background to the graph theory .
Chapter three includes The double dertex path graph for Symmetric encryption scheme .
Chapter four includes The double vertex path graph for polyalphabetic encryption scheme .
Chapter five includes conclusions and future works .

Chapter Two

Mathematical Background to Graph Theory

2.1 Graphs

A graph [2] $G = (V(G), E(G))$ or $G = (V, E)$ consists of two finite sets. $V(G)$ or V ; the vertex set of the graph, which is a non-empty set of elements called vertices and $E(G)$ or E; the edge set of the graph, which is a possibly empty set of elements called edges, such that each edge e in E is assigned as an unordered pair of vertices (u, v); called the end vertices of e.

Order and size [2]: *Order of a graph is the number of vertices in the graph. Size of a graph is the number of edges in the graph* .

parallel edges [2] : If two vertices are connected with more than one edge than such edges are called parallel edges that is many roots but one destination.

A self-loop or loop [2]: is an edge between a vertex and itself. An undirected graph without loops or multiple edges is known as a simple graph.

Simple graph [2]: A graph, that has neither self-loops nor parallel edges, is called a simple graph. An example of a simple graph is given in **fig 2.1**

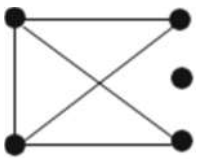


Fig 2.1 simple graph

2.2 Incidence and Degree [2]

When a vertex vi is an end vertex of some edge $ej, vi,$ and ej are said to be incident with (to or on) each other .

Adjacent : Two nonparallel edges are said to be adjacent if they are incident on a common vertex. For example, e_2 and e_3 are adjacent. Similarly, two vertices are said to be adjacent if they are the end vertices of the same edge. **In Fig. 2.2**, v_4 and v_5 are adjacent, but v_1 and v_4 are not

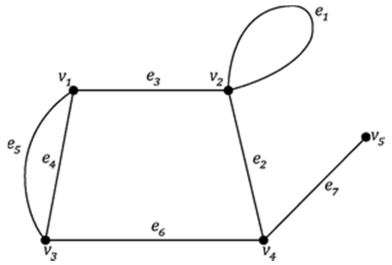


Fig 2.2 Incidence (graph)

Degree: Let v be a vertex of the graph G. The degree $d(v)$ of v is the number of edges of G incident with v, counting each self-loop twice. The minimum degree and the maximum degree of a graph G are denoted by $\delta(G)$ and Δ(G) , respectively

For example, in **Fig.1.2** : $d(v_1) = 3 = d(v_3) = d(v_4)$, $d(v_2) = 4$ and $d(v_5) = 1$

$$d(v_1) + d(v_2) + \cdots d(v_5) = 14 \; twie \; the \; number \; of \; edges \; .$$

Odd and even vertices [2] *: A vertex of a graph is called odd or even depending on whether its degree is odd or even*

In the graph of **Fig. 1.2**, there is an even number of odd vertices .

2.3 Walk , Trails and Paths [2]

Walk: A walk in a graph G is a finite sequence

$$\mathrm{W} \equiv v_0 e_1 v_1 e_2 \ldots\ldots\ldots v_{k-1} e_k v_k$$

whose terms are alternately vertices and edges such that for $1 \leq i \leq k$; the edge e_i

has ends v_i— 1 and v_i .

Thus, each edge e_i is immediately preceded and succeeded by the two vertices with which it is incident . we say that w is a walk or a walk from Origin and terminus :

The vertex v_0 is the origin of the walk W, while v_k is called the terminus of W. v_0 and v_k need not be distinct .

The vertices $v_1; v_2; \ldots; v_{k-1}$ in the above walk W are called its internal vertices. The integer , the number of edges in the walk, is called the length of W, denoted by $|W|$

In a walk W, there may be repetition of vertices and edges Trivial walk: A trivial walk is one containing no edge. Thus for any vertex v of G, $W \equiv v$ gives a trivial walk. It has length 0 .

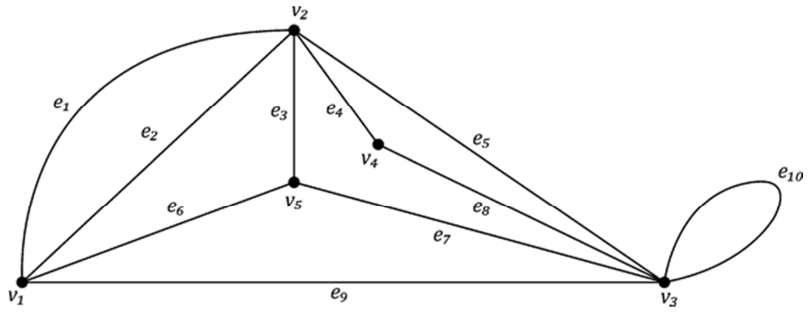


Fig. 2.3 A graph with five vertices and ten edges

In fig .1.3 , $W_1 = v_1e_1v_2e_5v_3e_{10}v_3e_5v_2e_3v_5$ and $W_2 = v_1e_1v_2e_1v_1e_1v_2$ are both walk of length 5 and 3, respectively from v_1 to v_5 and from v_1 to v_2 , respectively given two vertices u and v of a graph G , a $u - v$ walk is called closed or open , depending on whether $u = v$ or $u \neq v$.

Two walks W_1 and W_2 above are both open, while $W \equiv v_1v_5v_2v_4v_3v_1$ is closed

A path with n vertices will sometimes be denoted by P_n. Note that P_n has length $n - 1$.

In other words, a path is a walk in which no vertex is repeated. Thus, in a path no edge can be repeated either, so a every path is a trail. Not every trail is a path, though. For example, W_3 is not a path since v_1 is repeated. However, $W_4 \equiv v_2v_4v_3v_5v_1$ is a path in the graph G as shown in **Fig. 1.3** .

2.4 Connected Graphs , Disconnected Graphs [2]

Connected vertices: A vertex u is said to be connected to a vertex v in a graph G if there is a path in G from u to v**.**

Connected graph: A graph G is called connected if every two of its vertices are connected **.**

Disconnected graph: A graph that is not connected is called disconnected

2.5 The Double Vertex Graph

There are many graph functions with which one can construct a new graph from a given graph or set of graphs, such as Cartesian product and the line graph. One such graph function is called the double vertex graph. This was introduced by Alavi et al. in [3] and studied in [4, 6] inter alia. For a survey, see [5]. Let G = (V, E) be a graph of order $n \geq 2$. The double vertex graph $U_2(G)$is the graph whose vertex set consists of all $n(n-1)/2$ unordered pairs from V such that two vertices {x, y} and {u, v} are adjacent if and only if $|\{x,y\} \cap \{u,v\}| = 1$ and if $x = u$ then y and v are adjacent in G .the order and size of $U_2(G)$ are $n(n-1)/2$ and $m(n-2)$ respectively ,

where n is the order and m is the size of G .see figure 2.4 for an example of a graph and its double vertex graph .

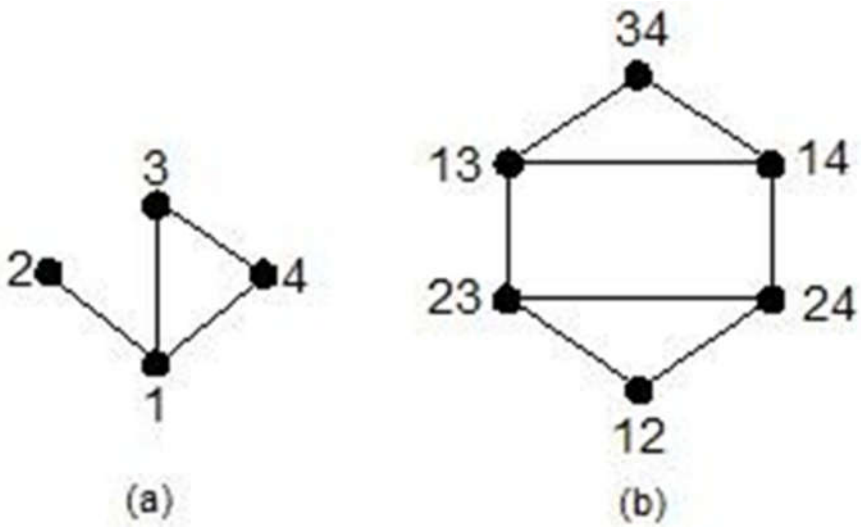


Figure 2.4 : (a) Graph G (b) Double vertex graph of G

Chapter Three

The Double Vertex Path Graph for Symmetric Encryption Scheme

3.1 Introduction

In this chapter, the Double Vertex Path Graph (DVPG) is used to give alternative modified encryption schemes. Two types of symmetric encryption schemes have been proposed. First one based of the English alphabet values, whereas, second one used the ASCII values to represent the letters of the plaintexts. Some examples on these types of the proposed symmetric encryption schemes are discussed. The security considerations of the proposed schemes are determined as same as of the DVPG schemes that are proposed in this Chapter .

3.2 The Double Vertex Path Graph [7]

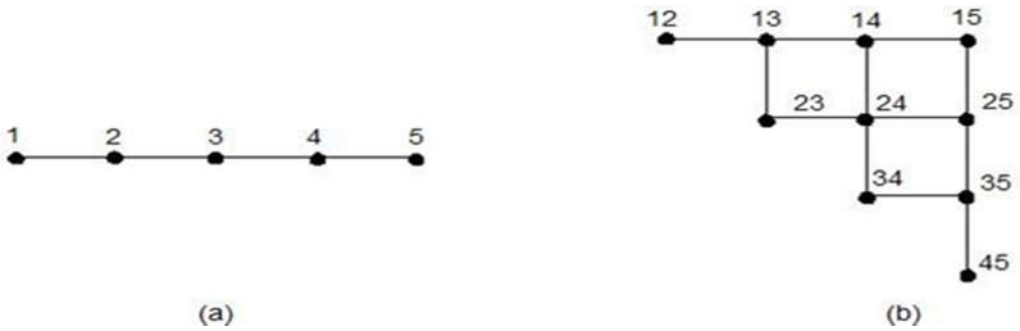


Figure 3.1: (a) Path P_5 (b) Double vertex graph of path $U_2(P_5)$

In mathematical field of graph theory, a path graph or a linear graph is a graph whose vertices can be listed in the order $1, 2, 3, \ldots, n$.

such that the edges are $(i, i + 1)$ where $i = 1, 2, 3, \ldots n - 1$. Path with n vertices is denoted as P_n. The double vertex graph of a path is denoted

as $U_2(P_n)$. In **Figure 3.1** , path P_5 and its double vertex Graph $U_2(P_5)$ is shown.

The number of vertices in $U_2(P_n)$ is $(n(n-1))/2$, the size of $U_2(P_n)$ is $n^2 - 3n + 2$, since P_n is a tree .

3.3. The Double Vertex Path Graph for Encryption Schemes

In this section, some encryption schemes have been proposed based on the double vertex path (DVP) graph which are discussed as follows.

3.3.1. The Double Vertex Path Graph for Encryption Scheme Based on the English Alphabet Values

The idea to use the DVPG for proposing new version of encryption scheme can be explained in the follow examples.

Table (3.1) plaintext alphabet [8]

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**		
14	15	16	17	18	19	20	21	22	23	24	25		

Example 3.3.1.1. (The DVP Graph for Encryption Scheme Based on the English Alphabet Values)

Suppose M is the plaintext that is given by the word "MATH". Based on the English alphabet Table (3.1) of the letters, one can convert the letters in the plaintext M into numbers. So,

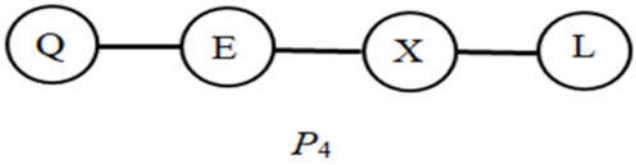
$$M \rightarrow 12, A \rightarrow 0, T \rightarrow 19, H \rightarrow 7.$$

With a shared secret key K= 4. The ciphertext C is computed by

$$C = M + K$$

$$C_1 = 12 + 4 = 16 \rightarrow Q, C_2 = 0 + 4 = 4 \rightarrow E, C_3 = 19 + 4 = 23 \rightarrow X, C_4 = 7 + 4 = 11 \rightarrow L.$$

So, the ciphertext C of M forms a path graph Q-E-X-L that is shown in Figure (3.1).



P_4

Figure 3.2. The path P4 of the ciphertext QEXL .

This path is represented as the double vertex graph (DVG) that is given **in Figure (3.3)** and sent to receiver by sender **.**

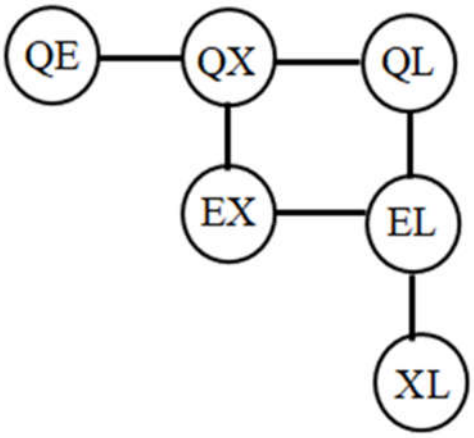


Figure 3.3. The DVG of the path P4 of the ciphertext QEXL .

After the second user (receiver) receives the double vertex graph, he/ she wants to decrypt the ciphertext and recover the original plaintext .

He/She first determines the label vertices QE, QX, QL, EX, EL and XL based DVG. Later on, he/she takes only the letters from vertices without repeating to form a list 1. There are many cases to determine the correct choice of this list. The correct one is

List 1: Q E X L .

Now, based on Table (3.1), these letters converted into numbers

$$Q \to 16 \quad E \to 4 \quad X \to 23 \quad L \to 11$$

Since the number of elements in the list 1 is equal to 4, so

$$16 - 4 = 12 \to M, 4 - 4 = 0 \to A, 23 - 4 = 19 \to T, 11 - 4 = 7 \to H$$

Thus, the original message is Math .

Example 3.3.1.2. (The DVP Graph for Encryption Scheme Based on the English Alphabet Values)

Suppose M is the plaintext that is given by the word "beautiful". Based on the English alphabet Table (3.1) of the letters, one can convert the letters in the plaintext M into numbers. So ,

$$b \to 1\,, e \to 4, a \to 0, u \to 20, t \to 19, i \to 8, f \to 5, u \to 20, l \to 11$$

With a shared secret key K= 9. The ciphertext C is computed by

$C=M+K$

$$C_1 = 1 + 9 = 10 = k\,, C_2 = 4 + 9 = 13 = n\,, C_3 = 0 + 9 = 9 = j\,, C_4 = 20 + 9 = 29 = 3 = d\,, C_5 = 19 + 9 = 28 = 2 = c, C_6 = 8 + 9 = 17 = r\,, C_7 = 5 + 9 = 14 = 0\,, C_8 = 20 + 9 = 3 = d\,, C_9 = 11 + 9 = 20 = u$$

So, the ciphertext C of M forms a path graph K-N-J-D-C-R-O-D-U that is shown in **Figure (3.3).**

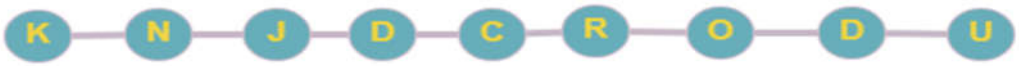


Figure 3.4. The DVG of the path P9 of the ciphertext KNJDCRODU.
This path is represented as the double vertex graph (DVG) that is given in **Figure (3.5)** and sent to receiver by sender

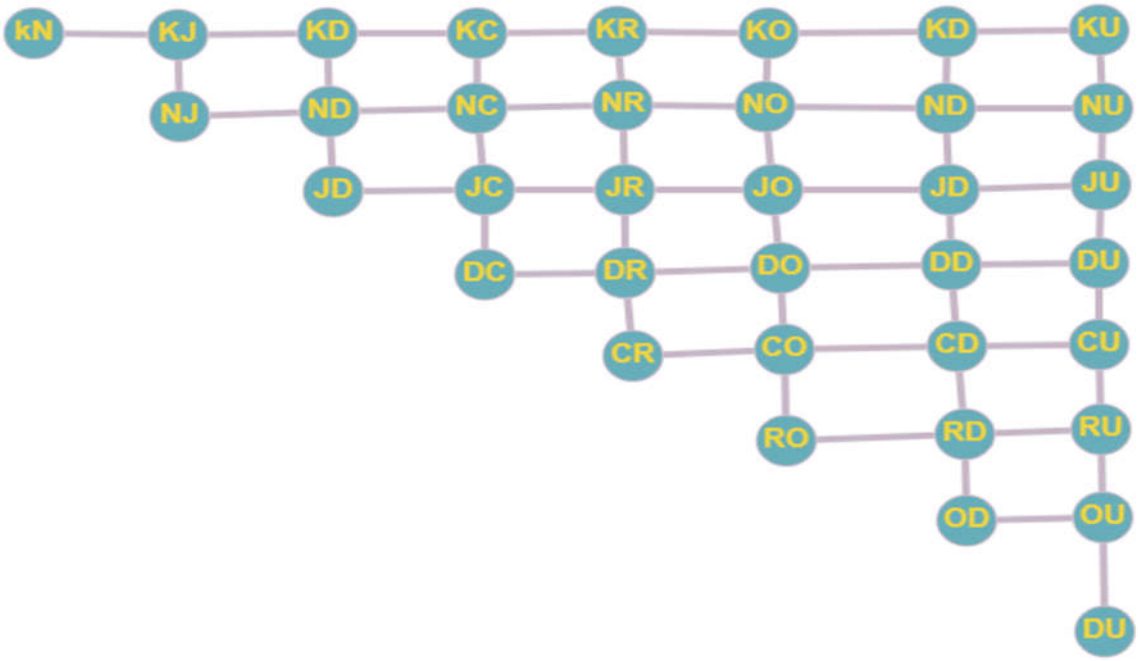


Figure (3.5) The DVPG of path graph P9

After the second user (receiver) receives the double vertex graph, he/ she wants to decrypt the ciphertext and recover the original plaintext .
He/She first determines the label vertices KN, KJ, KD, KC, KR,KO,KD,KU and NJ,ND,NC,NR,NO,ND,NU and JD,JC,JR,JO,JD,JU AND DC,DR ,DO,DD,DU and CR ,CO,CD,CU and RO, RD, RU and OD ,,OU and DU based DVG. Later on, he/she takes only the letters from vertices without repeating to form a list 1. There are many cases to determine the correct choice of this list. The correct one is
List 1: K N J D C R O D U
Now, based on Table (3.1), these letters converted into numbers
$K \to 10\ , N \to 13, J \to 9, D \to 3, C \to 2, R \to 17, O \to 14, D \to 3, U \to 20$
Since the number of elements in the list 1 is equal to 9, so
10-9=1=B , 13-9=4=E , 9-9=0=A , 3-9=-6=U ,2-9=-7=19=T ,17-9=8=I ,14-9=5=F
3-9=-6=U ,20-9=11=L
Thus, the original message is “beautiful”.

3.3.2. The Double Vertex Path Graph for Encryption Scheme Based on the ASCII Values , table (3.2) [9]

Table 3.2. ASCII Table.

Dec.	Char.	Dec.	Char.	Dec.	Char.	Dec.	Char.
0	Null	32	Space	64	@	96	`
1	Start of heading	33	!	65	A	97	a
2	start of text	34	"	66	B	98	b
3	end of text	35	#	67	C	99	c
4	end of transmission	36	$	68	D	100	d
5	Enquiry	37	%	69	E	101	e
6	Acknowledge	38	&	70	F	102	f
7	Bell	39	'	71	G	103	g
8	Backspace	40	(	72	H	104	h
9	horizontal tab	41	)	73	I	105	i
10	NL line feed, new line	42	*	74	J	106	j
11	vertical tab	43	+	75	K	107	k
12	NP form feed, new page	44	,	76	L	108	l
13	carriage return	45	-	77	M	109	m
14	shift out	46	.	78	N	110	n
15	shift in	47	/	79	O	111	o
16	data link escape	48	0	80	P	112	p
17	device control 1	49	1	81	Q	113	q
18	device control 2	50	2	82	R	114	r
19	device control 3	51	3	83	S	115	s
20	device control 4	52	4	84	T	116	t
21	negative acknowledge	53	5	85	U	117	u
22	synchronous idle	54	6	86	V	118	v
23	end of trans. Block	55	7	87	W	119	w
24	Cancel	56	8	88	X	120	x
25	end of medium	57	9	89	Y	121	y
26	Substitute	58	:	90	Z	122	z
27	Escape	59	;	91	[	123	{
28	file separator	60	<	92	\	124	|
29	group separator	61	=	93	]	125	}
30	record separator	62	>	94	^	126	~
31	unit separator	63	?	95	_	127	Del

The idea to use the DVPG for proposing new version of encryption scheme with ASCII values can be explained in the follow examples.

Example 3.3.2.1. (The DVP Graph for Encryption Scheme Based on the ASCII Values)

Suppose *m* is the plaintext that is given by the word **Central**. Based on the ASCII Table (3.2) of the letters, one can convert the letters in the plaintext *m* into numbers. So,

$C \rightarrow 067$, $e \rightarrow 101$, $n \rightarrow 110$, $t \rightarrow 116$, $r \rightarrow 114$, $a \rightarrow 097$, $l \rightarrow 108$.

The length *K* of *m* is equal to 7. Adding *K* to all of these numbers one by one respectively give

067+7=074, 101+7=108, 110+7=117, 116+7=123,114+7=121, 097+7=104,

108+7=115.

These numbers can be written as a list:

List: 74, 108, 117, 123, 121, 104, 115.

Using this list, a path graph can be created as shown in Figure (3.6).

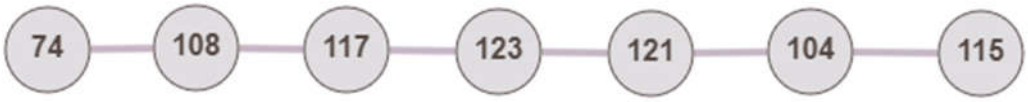


Figure 3.6.the path graph p7

The ciphertext of a message *m* is considered as the DVP graph as shown in **Figure (3.6)** which is sent to receiver by sender.

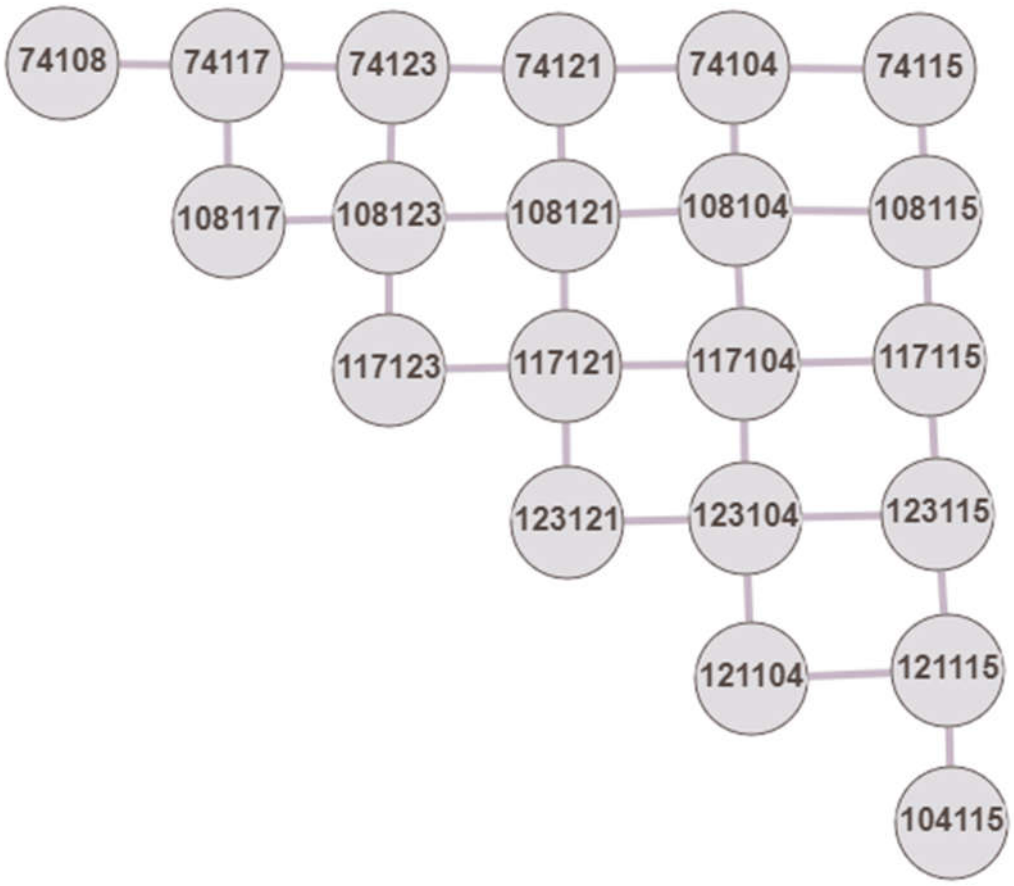


Figure 3.7. The DVPG of path graph P7

The second user (receiver) receivers the DVP graph. He/ She wants to decrypt the ciphertext and recover the original plaintext. Since the length of m is $K = 7$ and based on the ASCII Table (3.2), the user performs the following computations:

$074 - 7 = 067 \rightarrow C$,$108 - 7 = 101 \rightarrow e$,$117 - 7 = 110 \rightarrow n$, $123 - 7 = 116 \rightarrow t$, $121 - 7 = 114 \rightarrow r$, $104 - 7 = 097 \rightarrow a$,$115 - 7 = 108 \rightarrow l$.

Thus, the plaintext m is the word "**Central"**.

Example 3.3.2.2. (The DVP Graph for Encryption Scheme Based on the ASCII Values)

Suppose m is the plaintext that is given by the word " Precious". Based on the ASCII **Table (3.2)** of the letters, one can convert the letters in the plaintext m into numbers. So,

P → 080, r→114, e→101, c→099, i→105, o→111, u→117 , s→115.

The length K of m is equal to 8. Adding K to all of these numbers one by one respectively give

080+8=088 , 114+8=122 , 101+8=109 , 099+8=107 ,105+8=113 ,

111+8=119 , 117+8=125 , 115+8=123 ,

These numbers can be written as a list:

List: 088, 122, 109, 107, 113, 119, 125,123

Using this list, a path graph can be created as shown in **Figure (3.8)**.

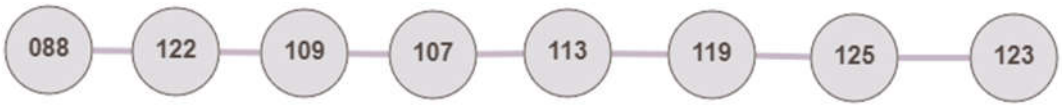


Figure 3.8 the path graph P8

The ciphertext of a message m is considered as the DVP graph as shown in Figure **(3.8)** which is sent to receiver by sender.

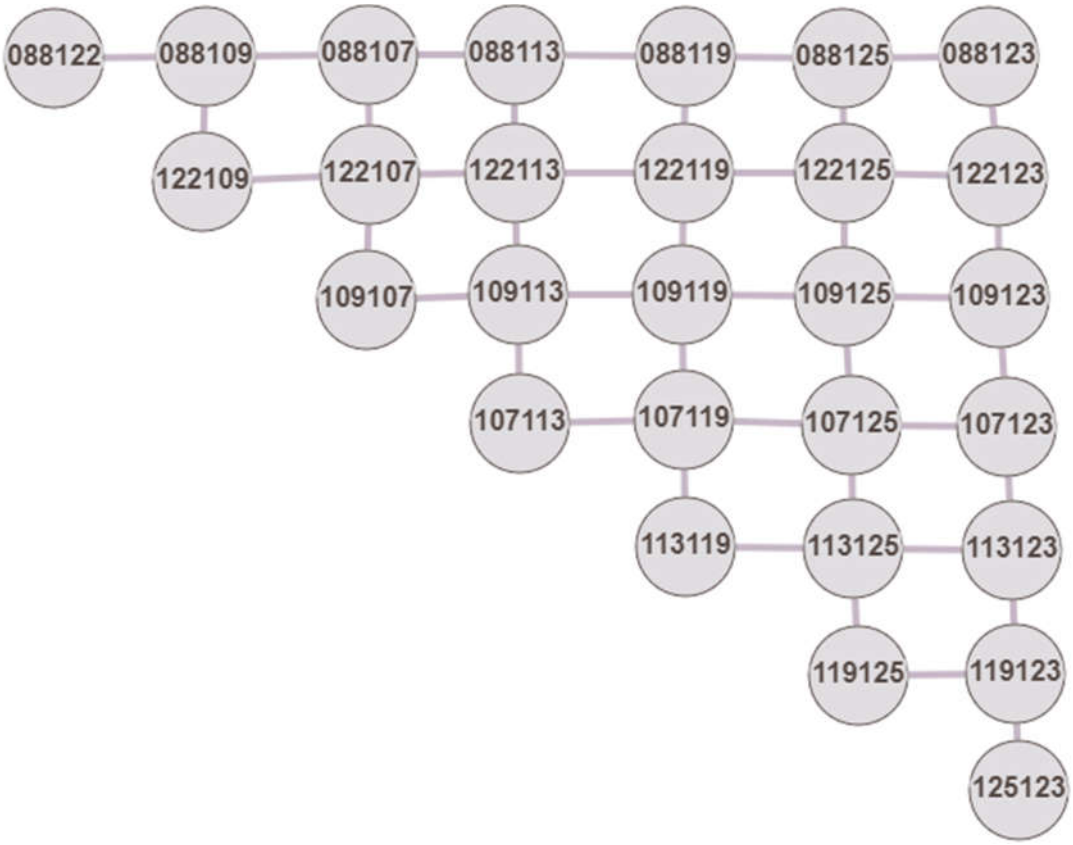


Figure 3.9 The DVPG of path graph P8

The second user (receiver) receivers the DVP graph. He/ She wants to decrypt the ciphertext and recover the original plaintext. Since the length of m is K = 8 and based on the ASCII **Table (3.2),** the user performs the following computations :

088 –8= 080 → P ,122 – 8 = 114 →r, 109 – 8 = 101 →e , 107-8=099→c

113-8=105→i , 119-8=111→o , 125-8=117→u , 123-8=115→s

Thus, the plaintext m is the word “Precious”.

Chapter Four

The Double Vertex Path Graph for Polyalphabetic Encryption Scheme

4.1 Introduction

In this chapter, the Double Vertex Path Graph (DVPG) is used to give alternative modified polyalphabetic encryption schemes. Two types of symmetric polyalphabetic encryption schemes have been proposed. First one based of the English alphabet values, whereas, second one used the ASCII values to represent the letters of the plaintexts. Some examples on these types of the proposed symmetric encryption schemes are discussed. The security considerations of the proposed schemes are determined as same as of the DVPG schemes that are proposed in Chapter three .

4.2 The DVPG for Polyalphabetic Encryption Scheme Based on English Alphabet Values

Before starting with the proposed encryption schemes, it is important to explain the polyalphabetic cipher. This cipher based on the substitution using the multiple substitution English alphabets. It is considered as a symmetric encryption scheme, since it depended on the shared secret key. On this key, some rules are determined to make it more secure and difficult to recover.

Let *m* be a plaintext can be given as an English word or an English sentence. This word or sentence has some English letters. Based on the

English alphabet Table (3.1) of these letters, one can convert the letters in the plaintext m into numbers.

It can work with alphabet Table (3.1) and some rules are putting on the key K. So, applying this rules (r_1, r_2 or r_k) to all of these numbers one by one has been done. For instance, if the letters of plaintext m is m_1, m_2, …, m_K then $\#m_1$ it move according to the r_1 (mod 26) ≡ a_1, $\#m_2$ it move according to the r_2(mod 26) ≡ a_2, … , $\#m_K$ it move according to the m_i (mod 26) ≡ a_K, where $\#m_i$ are numbers in Table (3.1).

In other words, it is possible to write these numbers in the list

$$\text{List: } \{a_1, a_2, \ldots, a_l, a_{l+1}, a_{l+2}, \ldots, a_K\}.$$

This list can be represented by path graph P. The graph P is used to form the DVPG which considered as the ciphertext that is sent to receiver by sender.

The second user (receiver) receivers the DVPG. He/ She wants to decrypt the ciphertext and recover the original plaintext. He/ She first writes down the labeled vertices in list without repeating the letters or the numbers that are correspond to these letters. This list is

$$\text{List: } \{a_1, a_2, \ldots, a_l, a_{l+1}, a_{l+2}, \ldots, a_K\}.$$

Since K is a shared secret key with its some, so first user computes the following computations:

a_1 it moves in the opposite direction according to the r_1 (mod 26) ≡ $\#m_1$, a_2 it moves in the opposite direction according to the r_2 (mod 26) ≡ $\#m_2$, ..., a_K it moves in the opposite direction according to the r_i (mod 26) ≡ $\#m_K$.

Based on the English alphabet Table (3.1), the previous numbers converted into

$\#m_1 \rightarrow m_1$, $\#m_2 \rightarrow m_2$, …, $\#m_l \rightarrow m_l$ and $\#m_{l+1} \rightarrow m_{l+1}$, …, $\#m_K \rightarrow m_K$.

Thus, the original plaintext is recovered by $m = m_1 m_2 \ldots m_K$.

Example 4.2.1. The DVPG for Polyalphabetic Encryption Scheme Based on English Alphabet Values

Suppose *m* is the plaintext that is given by the word **"MATH"**. Based on the English alphabet Table (3.1) of the letters, one can convert the letters in the plaintext *m* into numbers. So,

$$M \rightarrow 12, A \rightarrow 0, T \rightarrow 19, H \rightarrow 7.$$

Some rules on the key *K* are determined by

1- Shift first letters three positions to its right.

2- Shift the second letters four positions to its right.

In more details, the letter *M* moves into three positions to its right to become P, *A* letter moves to four positions to its right to become *C*. Repeating the key process for all letters of the word as follows.

$$MA \quad TH$$

$$PE \quad WL$$

The letters of the encoded word "*PEWL"* which can form by a list

List: {*P,E,W,L*} = {15,4,22,11}.

This list can be represented by path graph P_4 shown in Figure (4.1). The graph P_4 is used to form the DVPG which considered as the ciphertext that is sent to receiver by sender.

Figure 4.1. The path graph P_4 has four vertices.

The ciphertext C of a message *m* is considered as the DVPG as show in Figure (4.2) which is sent to receiver by sender.

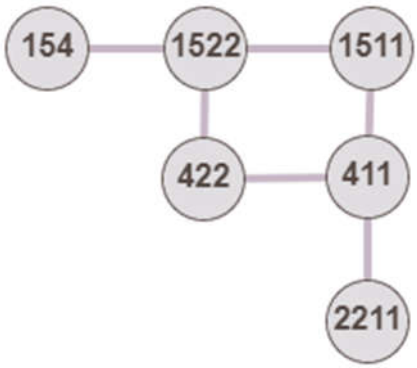


Figure 4.2. The DVPG of path graph P_4.

The second user (receiver) receivers the DVPG. He/ She wants to decrypt the ciphertext and recover the original plaintext. He/ She first writes down the labeled vertices in list without repeating the letters or the numbers that are correspond to these letters. This list is

List: = {15, 4, 22, 11}.

For decryption process, second user using the inverse rules of the key to recover the original plaintext. The rules are

1. Shift first letters three positions to its left.
2. Shift the second letters four positions to its left.

With more details, the letter *P* moves to three positions to its left to become M, the letter *E* moves to four positions to its left *A*, Repeating the key process for all letters of the word and based on the English alphabet Table (3.1), the encoded word

PE WL

becomes

MA TH

Thus, the plaintext *m* is **MATH.**

Example 4.2.2. The DVPG for Polyalphabetic Encryption Scheme Based on English Alphabet Values .

Suppose m is the plaintext that is given by the word “SQUARE”. Based on the English alphabet Table (3.1) of the letters, one can convert the letters in the plaintext m into numbers. So,

$$S\rightarrow 18 \text{ , } Q\rightarrow 16 \text{ , } U\rightarrow 20 \text{ , } A\rightarrow 0, R\rightarrow 17 \text{ , } E\rightarrow 4$$

Some rules on the key K are determined by

1- Shift first letters five positions to its right.

2- Shift the second letters three positions to its right.

3- Shift the third letters two positions to its right.

In more details, the letter M moves into three positions to its right to become P, A letter moves to four positions to its right to become C. Repeating the key process for all letters of the word as follows.

SQU : XTW

ARE : FUG

The letters of the encoded word “XTWFUG” which can form by a list

$$\text{List: } \{ X,T,W,F,U,G \} = \{23,19,22,5,20,6\}.$$

This list can be represented by path graph P4 shown in **Figure (4.3)**. The graph P4 is used to form the DVPG which considered as the ciphertext that is sent to receiver by sender.

Figure 4.3. The path graph P6 has four vertices.

The ciphertext C of a message m is considered as the DVPG as show in **Figure (4.4)** which is sent to receiver by sender.

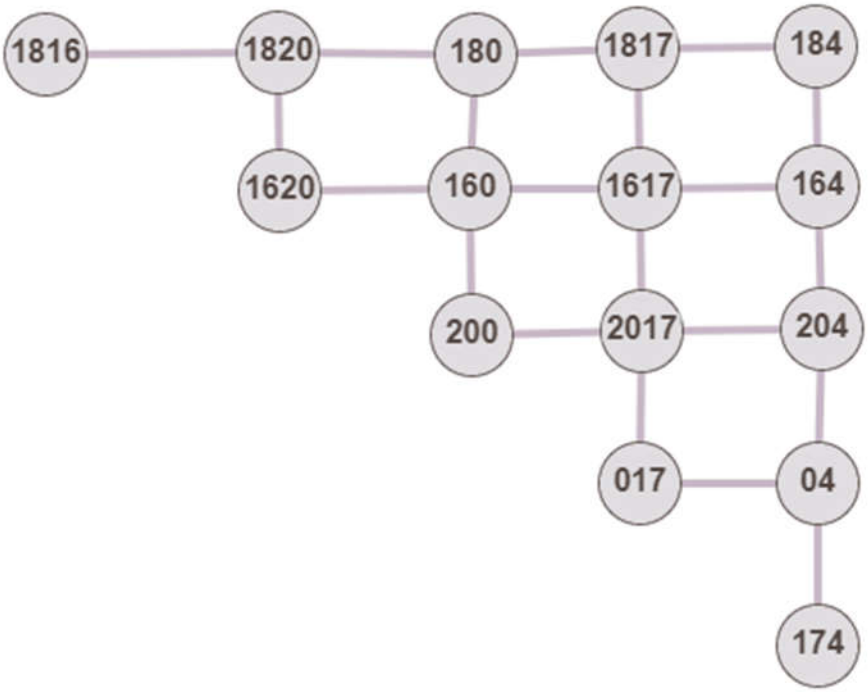


Figure 4.4. The DVPG of path graph P6.

The second user (receiver) receivers the DVPG. He/ She wants to decrypt the ciphertext and recover the original plaintext. He/ She first writes down the labeled

vertices in list without repeating the letters or the numbers that are correspond to these letters. This list is

List : = {23,19,22,5,20,6}.

For decryption process, second user using the inverse rules of the key to recover the original plaintext. The rules are

1- Shift first letters five positions to its left.

2- Shift the second letters three positions to its left.

3- Shift the third letters two positions to its left.

With more details, the letter P moves to three positions to its left to become M, the letter E moves to four positions to its left A, Repeating the key process for all letters of the word and based on the English alphabet **Table (3.1)**, the encoded word

XTW FUG

Becomes

SQU ARE

Thus, the plaintext m is SQUARE.

Chapter Five
Conclusions and Future Works

5.1 Conclusions

In this work, one can conclude that the concepts of graph theory have been used to give new sights for proposing new versions of symmetric encryption schemes. This application used the DVPG to design these versions with more secure level to create the ciphertext of the original message. These versions are DVPG encryption scheme based on English alphabet values and DVPG encryption scheme based on ASCII values. On the other hand, these graphs are applied to modify the polyalphabetic substitution cipher.

5.2 Future Works

It is possible to apply the same idea of the proposed encryption scheme with other kinds of symmetric and asymmetric encryption schemes and also it can use other types of the graphs.

References

1)Tokareva, Natalia. "Connections between graph theory and cryptography." G2C2: Graphs and Groupts, Cycles and Coverings, September (2014) **.**

2) Beezer, Robert A. "Graph Theory, by JA Bondy and USR Murty." (2008).

3) Yousef Alavi, Mehdi Behzad, Paul Erd Os and Don R. Lick, Double vertex graphs, Journal of Combinatorics, Information and System Sci., Vol.16, Issue 1, pp 37 − 50, 1991.

4) Yousef Alavi, M. Behzad, Jiuqiang Liu, Don R. Lick, and Bi- wen Zhu, Connectivity of double vertex graphs, Graph theory, combinatorics, and algorithms, Vol.1, 2 pp. 723 − 741, 1995.

5) Yousef Alavi, Don R. Lick and Jiuqiang Liu, Survey of double vertex graphs, Graphs and Combinatorics, Vol.18, Issue 4, pp 709 − 715, 2002 .

6) Yousef Alavi, Mehdi Behzad, and J. E. Simpson, Planarity of double vertex graphs, Graph Theory, Combinatorics, algo- rithms and applications, SIAM, Philadelphia, PA, pp 472 485, 1991.

7) BEAULA, C.; VENUGOPAL, O.; PADMAPRIYA, N. Graph distance of vertices in double vertex graphs. International Journal of Pure and Applied Mathematics, 2018, 118.23: 343-351.

8)codes and ciphers :Julius Caesar ,the Engma,and the internet ,by Robert churchhouse .cambridge university press,2002.

9) KINARIWALA, Bharat; DOBRY, Tep. Programming in C1. 1993.

بيان الرأس المزدوج للتشفير

الخلاصة :

تم اقتراح إصدارات جديدة من مخططات التشفير المتماثل في هذا العمل. تستخدم هذه المخططات .(D.V.G) الإصدارات تعريفًا جديدًا للرسم البياني للرأس المزدوج والتشفير الأبجدي المتعدد على ASCII المقترحة الجديدة على قيم الأبجدية الإنجليزية وقيم التوالي. يتم اختيار الرسالة ككلمة إنجليزية أو جملة إنجليزية. يعتبر النص المشفر للرسالة الأصلية بمثابة الرسم البياني للرأس المزدوج الذي يتم إرساله إلى جهاز الاستقبال عن طريق المرسل ، حيث تمت مناقشة العديد من النتائج التجريبية لخطط التشفير المقترحة. يتم تحديد اعتبارات الأمان لأنظمة تشفير الرسم البياني ذات الرأس المزدوج المقترحة .