Republic Of Iraq
Ministry of Higher Education
and Scientific Research
University of Babylon
College of Education of Pure Science
Department of Mathematics

The Corona Graph for Cryptography

A Research
Submitted to the Council of 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

Awrad Abd Hamza Hussain

Supervised by

Asst. Prof. Dr. Ruma Kareem K. Ajeena

August 2021 **Muharram 1443**

بسم الله الرحمن الرحيم

((يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَالَّذِينَ

أُوتُوا الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ

خَبِيرٌ))

صدق الله العلي العظيم

سورة المجادلة١١

Supervisor Certificate

I certify that this research entitled " **The Corona Graph for Crptography** " for the student **Awrad Abd Hamza**, was prepared under my supervision in University of Babylon, 66 College of Education for pure Science as a partial requirement for the Degree of Higher Diploma Education /Mathematic.

Signature:

Name: **Dr. Ruma Kareem K. Ajeena**
Title: **Asst. Prof.**

Date:

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

Signature:

Name: **Azal Mera**

Head of mathematics Department

Title: **Assist. Prof. Dr**

Date:

Certification of Scientific Expert

This is to certify that I have read this research, entitled "**The Corona Graph for Crptography"** And I found that this research is qualitied for debate.

Signature:

Name:

Title:

Address: Collage of education for pure sciences

Date:

Certification of Linguistic Expert

This is to certify that I have read this research, entitled **“The Corona Graph for Cryptography”** And I found that this research is qualitied for debate.

Signature:

Name:

Title:

Address: Collage of education for pure sciences

Date:

Examination Committee Certification

We certify that we have read this research entitled " **The Corona Graph for Cryptography”"** as examining committee examined the student **Awrad Abd Hamza** in its contents and that in our opinion it is adequate for the partial fulfillment of the requirement for the Degree of Higher Diploma Education/ Mathematics

Chairman
Signature:
Name:
Title:
Date:

Member
Signature:
Name:
Title:
Date:

Member
Signature:
Name:
Title:
Date:

Member / Supervisor
Signature:
Name:
Title:
Date:

Approved by the dean of collage of education for pure sciences

Signature:
Name: Dr.Bahaa Hussein Salih Rabee
Scientific grade: professor
Address: Dean of collage of education for pure sciences
Date:

Acknowledgement

All praise and glory to Almighty ALLAH for providing me with the health and strength to finish this work and do something that will benefit humanity.

My thanks and appreciations go to my supervisors **Asst. Prof. Dr. Ruma Kareem K. Ajeena** for his guidance, patience, motivation, support, and advice during the research.

Dedication

I dedicate this work to:

The reason for my existence in life; My parents

The soul of my dear brother whose separation has hurt me

Abstract

New version of the symmetric encryption schemes are proposed in this work. These versions are used new definition of the corona graph (CG). These new proposed schemes depended on the English alphabet values, ASCII values and the polyalphabetic cipher respectively. The message is chosen as an English word or an English sentence. The ciphertext of the original message is considered as the corona graph which is sent to receiver sender. Several experimental results of the proposed corona graph encryption schemes are discussed. The security consideration of the proposed corona graph encryption schemes is determined.

Publications

The Corona Graph For Symmetric Encryption Schemes, AL- Kadhum 2nd International Conference for Modern Applications of Information and Communication Technology, AIP journal, Scopas, 2021, (Submitted).

List of Contents

Chapter One

Introduction

CHAPTER 1
INTRODUCTION

1.1 Introduction

The Coronavirus Covid-19 has affected almost all the countries and millions of people got infected and more deaths have been reported everywhere. The uncertainty and fear created by the pandemic can be used by hackers to steal the data from both private and public systems. Hence, there is an urgent need to improve the security of the systems. This can be done only by building a strong cryptosystem. So many researchers started embedding different topics of mathematics like algebra, number theory, and so on in cryptography to keep the system, safe and secure. In this study, a cryptosystem using graph theory has been attempted, to strengthen the security of the system.

1.2 Previous Works

(Zehui et al., 2020), provided a study on new type of symmetric encryption by converting the classical monoalphabetic affine cipher into a polyalphabetic cipher. The proposed encryption utilizes the properties of outer-convex dominating set in the corona of graphs to generate random keys from the shared keyword to every character of the message. The new encryption eliminates the weaknesses of affine cipher, thus increasing the level of confidence for exchanging messages.

Edge domination numbers of Boolean Function Graph B(Kp , L(G), NINC) of some standard graphs and corona graphs obtained by (S. Muthammai and S. Dhanalakshmi, 2019). They suggested that:

For any graph G, let V (G) and E (G) denote the vertex set and edge set of G respectively. The Boolean function graph B ($\overline{Kp}$Kp , L(G), NINC) of G is a graph with vertex set V(G) » E(G) and two vertices in B($\overline{Kp}$, L(G), NINC) are

adjacent if and only if they correspond to two adjacent edges of G or to a vertex and an edge not incident to it in G. For brevity, this graph is denoted by B2 (G).

(B.J. Murali et al., 2017) proved the existence of labeling to the graphs (i) flower graph and (ii) corona graph. They suggested:

Let G = (V, E) be a graph with n vertices. A function

$$f : V(G) \rightarrow \begin{cases} n \\ i \end{cases} ; 0 \leq i \leq n$$

of the graph G is said to be a combination cordial labeling if the induced edge function $f^* : E \rightarrow \{0, 1\}$ defined by

$$f^*(uv) = \begin{cases} 1\ 1\ if\ f(u) = f(v) \\ 0\ if\ f(u)\ 6 \neq f(v) \end{cases}$$

Satisfies the condition $|ef^*(0) - ef^*(1)| \leq 1$. A graph G which admits the combination cordial labeling is called a combination cordial graph.

A graph labeling is the concept of assigning labels, to the edges or vertices or both edges and vertices of the graphs using integers subject to certain conditions. (S.Sangeetha and U.Usharani, 2019) have obtained the Relaxed mean labeling (RML) for certain corona graphs.

Let G = (V, E) be a graph and let D be a minimum total dominating set of G. If V – D contains a total dominating set D' of G, then D' is called an inverse total dominating set of G with respect to D. The inverse total domination number γ_t^{-1} (G) of G is the cardinality of a smallest inverse total dominating set of G. (V. R. Kulli., 2016) obtained the inverse total domination number for some classes of graphs such as union, join and generalized corona of graphs.

(C Beaula and P Venugopal, 2020) constructed a new graph from the given graph, known as a double vertex graph. The edge labeling of this double vertex graph is used in encryption and decryption. A new cryptosystem using the

amalgamation of the path, its double vertex graph and edge labeling has been proposed. From the double vertex graph of a path, we have given a method to find the original path. To hack such an encrypted key, the knowledge of graph theory is important, which makes the system stronger. The one-word encryption method will be useful in every security system that needs a password for secure communication or storage or authentication.

1.3 The Problem Statement of This Research

This work proposed new symmetric encryption schemes. This proposition employed using the CG to increase Security level of these schemes. The Security have is determined based on encrypting the message using CG and sending it to the receiver.

1.4 The structure of this Research

This research consists of five chapters:

Chapter 1 includes the general introduction, previous works and the problem statement of this research

Chapter 2 includes the mathematical background to the graph theory, graph Order and Size and Walks, Trails, and Paths

Chapter 3 the corona graph for symmetric encryption scheme, the Corona Graph for encryption schemes: Case II and The Security Considerations of CG Encryption Schemes

Chapter 4 the corona graph for polyalphabetic encryption scheme, The CG for Polyalphabetic Encryption Scheme Based on English Alphabet Values

Chapter 5 conclusion and references**.**

Chapter Two

Theoretical Aspects And Previous Works

CHAPTER 2

THEORETICAL ASPECTS AND PREVIOUS WORKS

2.1 Introduction

In this introductory chapter we provide an intuitive background to the material that we present more formally in later chapters. Terms that appear here in bold-face type are to be thought of as descriptions rather than as definitions. Having met them here in an informal setting, you should find them more familiar when you meet them later. So read this chapter quickly, and then forget all about it!

2.2 What is a graph theory?

A graph theory is a branch of mathematics with networks of points connected by lines. The subject of graph theory had its beginning in recreational math problems, but it has grown into a significant area of mathematical research, with applications in chemistry, operations research, social sciences and computer science.

The history of graph theory may be specifically traced to 1735, when the Swiss mathematician "Leonhard Euler" solved the problem an old puzzle concerning the possibility of finding a path over every one of seven bridges that span a forked river flowing past an island but without crossing any bridge twice.

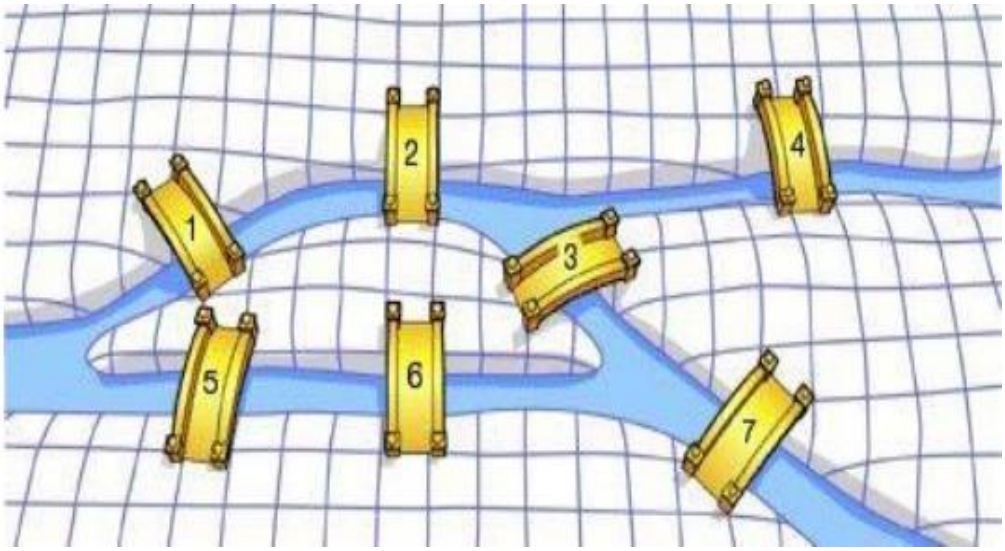


Fig. 2-1 Graph of seven bridge

Graph

A graph G consists of a set Vof vertices and a set of edges such that edge e is associated with as un eroded pair of vertices. In simple a graf is set of point (called vertices) connected by line (called edges). Graphs are denoted by uppercase letter such as G .Then the set of vertices of Graph G is denoted by V(G) and the set of edges of graph G is denoted by E(G).

Order and Size

We defined |V| = n to be the order of G and |E| = m to be the size of G.

We are dealing with Fig. 2-1, which depicts part of the roadmap and part of some type of electrical network.

Either of these situations can be represented diagrammatically by means of points and lines.

1. The points are called vertices;
2. The lines are called edges;
3. The whole diagram is called graph.

The degree of a vertex is the number of edges with that vertex as an end-point; it corresponds in Fig. 2-2 to the number of roads at an intersection.

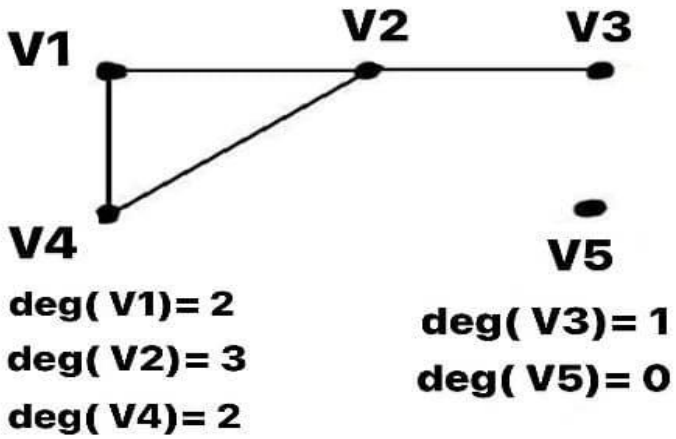


Fig. 2-2 degree of avertex

In the following graph , there exists at most one edge joining each pair of varices. The edges joining this points denoted by multiple edges.

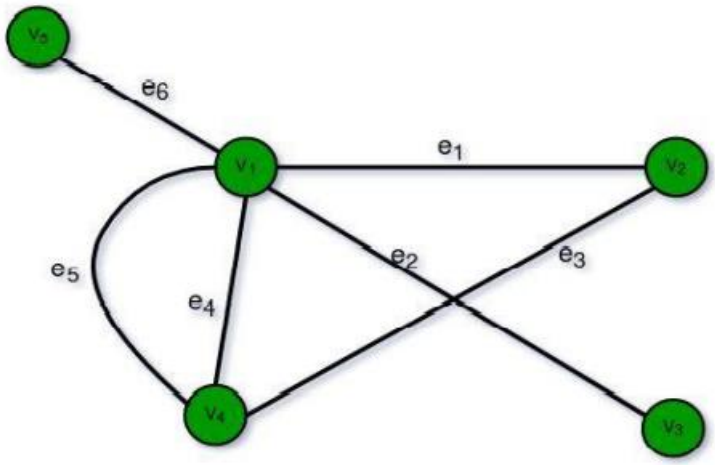


Fig. 2-3 Multiple edges

Drawing an edge from a point to itself, is denoted by a loop, such as the Fig.2-4.

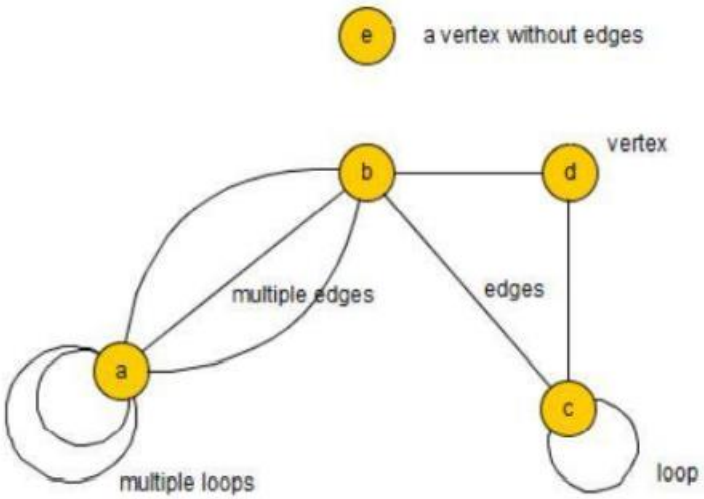


Fig. 2-4 aloop

Graphs with no loops or no multiple edges, such as the graph in Fig. 2-5.

Simple graph Multigraph

Fig. 2-5 Simple graph and Multigraph

2.3 Walks, Trails, and Paths

1-Walk

A walk is a sequence of vertices and edges of a graph i.e. if we traverse a graph then we get a walk.

Vertex can be repeated

Edges can be repeated

W =V0e1V1e2V2 -----Vn-1enVu

Vi-1Vi=ei 1≦ i ≦1

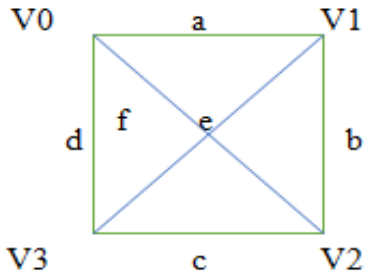


Fig. 2-6 : Walk

Walk can be open or closed

2- Trail

Trail is an open walk in which no edge is repeated

Vertex can be repeated

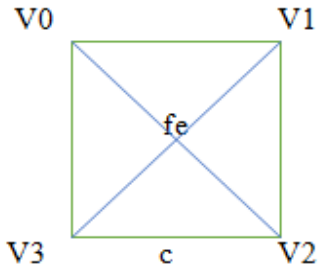


Fig. 2-7 : Trail

3- Path

It is a trail in which neither vertices nor edges are repeated if we traverse a graph such that we don't repeat a vertex and nor we repeat an edge .A path is also a trail thus it is an open walk .

Vertex not repeated

Edges not repeated

P: [v1, v2, vo, v3]

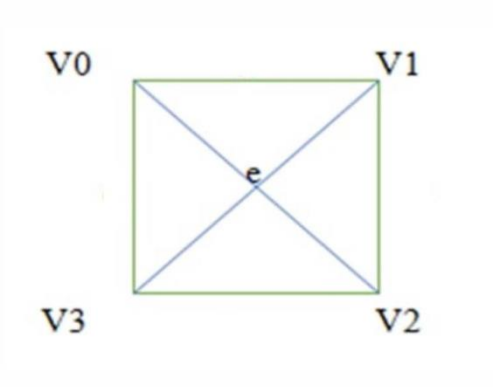


Fig. 2-8 : Path

Chapter Three

The Corona Graph for Symmetric Encryption Scheme

CHAPTER 3
The Corona Graph for Symmetric Encryption Scheme

3.1 Introduction

In this chapter, the definition of the corona graph (CG) has been proposed. The CG is used for encryption schemes. Two types of symmetric encryption schemes have been proposed. First one based of the English alphabet values and 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.

3.2 The Corona Graph

The concept of the corona graph (CG) is defined as follows.

Definition 3.2.1.

A corona graph G is a graph has original vertices n and edges m. each original vertex has some other vertices to form the corona vertices.

For instance, a corona graph G has 3 original vertices. Each vertex has 4 vertices.

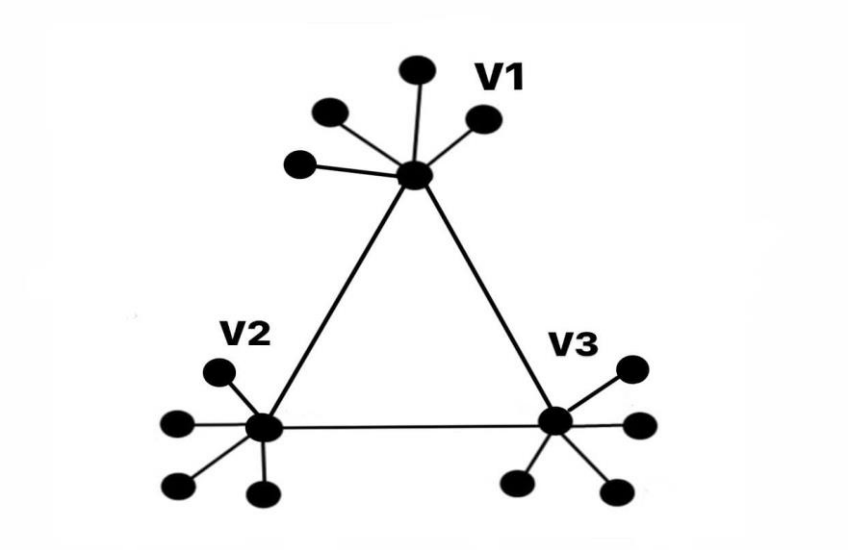


Figure 3.1. The corona graph CG.

3.3 The Corona Graph For Encryption Schemes

In this section, some encryption schemes have been proposed based on the Corona graphs which are discussed as follows.

3.3.1 The Corona Graph for Encryption Schemes: Case I.

Suppose a plaintext *m* is chosen as an English word or English sentence. This word or sentence consists of some English letters. These letters can be converted into numbers using the English alphabet Table (3.1).

Table 3.1. English alphabet Table.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**G**	**K**	**L**	**M**	**N**
1	2	3	4	5	6	7	8	9	10	11	12	13	14
O	P	Q	R	S	T	U	V	W	X	Y	Z		
15	16	17	18	19	20	21	22	23	24	25	26		

In other words, the plaintext m divides into the blocks m_i such that

$$m = (m_1, m_2, \ldots, m_n),$$

where $m_i = (m_{i1}, m_{i2}, \ldots, m_{il})$. The length of each block is l. Using the alphabet Table (3.1), one can transfer the letters in each block m_i of the plaintext m into numbers $\# m_i$. Since the number of the blocks is equal to n, so the numbers in the blocks are shifted by adding to them using the shift cipher, namely

$$\#m_1 + n \pmod{26} = (a_{11}, a_{12}, \ldots, a_{1l})$$
$$\#m_2 + n \pmod{26} = (a_{21}, a_{22}, \ldots, a_{2l})$$
$$\ldots$$
$$\#m_n + n \pmod{26} = (a_{n1}, a_{n2}, \ldots, a_{nl}).$$

Now, the first user takes his shared secret key which is a prime number p, where $p > 26$. The ciphertext C of the elements in shifted blocks is computed based on the inverse elements modulo p. So,

$$C = (c_1, c_2, \ldots, c_n)$$

where

$$c_1 = (c_{11}, c_{12}, \ldots, c_{1l}), c_2 = (c_{21}, c_{22}, \ldots, c_{2l}), \ldots, c_n = (c_{n1}, c_{n2}, \ldots, c_{nl}).$$

In more details, the computations are done by

$$c_{11} \equiv a_{11} \pmod{p}, c_{12} \equiv a_{12} \pmod{p}, \ldots, c_{nl} \equiv a_{nl} \pmod{p}.$$

The ciphertext C has been sent to second user as a corona graph.

After the second user receives the corona graph, he/ she will do the following computations:

He/ She takes the blocks (c_1, c_2, ..., c_n) and he/she uses his/her shared secret key to compute the inverses elements of c_{ij}, for $i = 1,2,\ldots, n$ and $j = 1,2,\ldots, l$.

In other words,

$$(c_{ij})^{-1} \pmod{p} \equiv a_{ij}, \text{ for } i = 1,2,\ldots, n \text{ and } j = 1,2,\ldots, l.$$

Since a plaintext message has n blocks, therefore, he/she computes

$$a_{ij} - n \pmod{26} \equiv \#m_i, \text{ for } i = 1,2,\ldots, n.$$

Based on Table (3.1), one can recover the alphabet letters m_i that correspond to these numbers $\#m_i$.

Example 3.3.1.1. Study Case I: Corona graph Encryption Scheme

Suppose m is a message that is given by the following sentence

"The brown fox jumps over a cat".

Here $m = (m_1, m_2, m_3, m_4, m_5, m_6)$ such that

m_1 = Theb, m_2 = rown, m_3 = foxj, m_4 = umps, m_5 = over, m_6 = acat.

Based on the alphabet Table (3.1), the blocks of message m_i, for $i = 1,2,3,\ldots,6$, can be converted into numbers as follows:

$$m_1 = \text{Theb} \rightarrow (20, 8, 5, 2)$$

$$m_2 = \text{rown} \rightarrow (18, 15, 23, 14)$$

$$m_3 = \text{foxj} \rightarrow (6, 15, 24, 10)$$

$$m_4 = \text{umps} \rightarrow (21, 13, 16, 19)$$

$$m_5 = \text{over} \rightarrow (15, 22, 5, 18)$$

$$m_6 = \text{acat} \rightarrow (1, 3, 1, 20).$$

Since the number of the blocks is equal to 6, so the numbers in blocks are shifted by adding 6 to them using the shift cipher, namely

$$(20, 8, 5, 2) + 6 \pmod{26} \equiv (26, 14, 11, 8)$$

$$(18, 15, 23, 14) + 6 \pmod{26} \equiv (24, 21, 3, 20)$$

$$(6, 15, 24, 10) + 6 \pmod{26} \equiv (12, 21, 4, 16)$$

$$(21, 13, 16, 19) + 6 \pmod{26} \equiv (1, 19, 22, 25)$$

$$(15, 22, 5, 18) + 6 \pmod{26} \equiv (21, 2, 11, 24)$$

$$(1, 3, 1, 20) + 6 \pmod{26} \equiv (7, 9, 7, 26).$$

Now, the first user takes his shared secret key which is a prime number p =29, where p =29 > 26. The ciphertext $C = (c_1, c_2, c_3, c_4, c_5, c_6)$, where $c_1 = (c_{11}, c_{12}, c_{13}, c_{14})$, $c_2 = (c_{21}, c_{22}, c_{23}, c_{24})$ and so on, is computed for elements in the shifted blocks though the computations of the inverses elements modulo p as follows.

$$c_{11} \equiv 26^{-1} \pmod{29} \equiv 19$$

$$c_{12} \equiv 14^{-1} \pmod{29} \equiv 1$$

$$c_{13} \equiv 11^{-1} \pmod{29} \equiv 8$$

$$c_{14} \equiv 8^{-1} \pmod{29} \equiv 11$$

$$c_{21} \equiv 24^{-1} \pmod{29} \equiv 23$$

$$c_{22} \equiv 21^{-1} \pmod{29} \equiv 18$$

$$c_{23} \equiv 3^{-1} \pmod{29} \equiv 10$$

$$c_{24} \equiv 20^{-1} \pmod{29} \equiv 16$$

$$c_{31} \equiv 12^{-1} \pmod{29} \equiv 17$$

$$c_{32} \equiv 21^{-1} \pmod{29} \equiv 18$$

$$c_{33} \equiv 4^{-1} \pmod{29} \equiv 22$$

$$c_{34} \equiv 16^{-1} \pmod{29} \equiv 20$$

$$c_{41} \equiv 1^{-1} \pmod{29} \equiv 1$$

$$c_{42} \equiv 19^{-1} \pmod{29} \equiv 26$$

$$c_{43} \equiv 22^{-1} \pmod{29} \equiv 4$$

$$c_{44} \equiv 25^{-1} \pmod{29} \equiv 7$$

$$c_{51} \equiv 21^{-1} \pmod{29} \equiv 18$$

$$c_{52} \equiv 2^{-1} \pmod{29} \equiv 15$$

$$c_{53} \equiv 11^{-1} \pmod{29} \equiv 8$$

$$c_{54} \equiv 24^{-1} \pmod{29} \equiv 23$$

and

$$c_{61} \equiv 7^{-1} \pmod{29} \equiv 25$$

$$c_{62} \equiv 9^{-1} \pmod{29} \equiv 13$$

$$c_{63} \equiv 7^{-1} \pmod{29} \equiv 25$$

$$c_{64} \equiv 26^{-1} \pmod{29} \equiv 19.$$

The ciphertext has been sent to second user as a corona graph as shown in Figure (3.2).

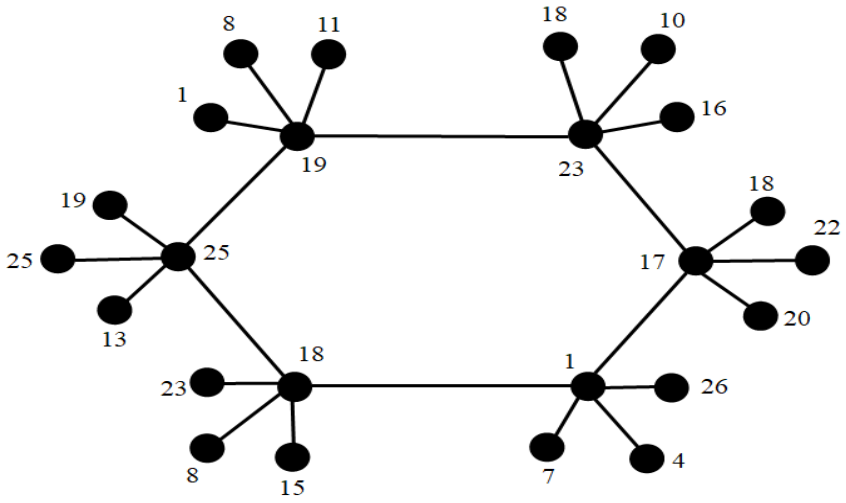


Figure 3.2. A corona graph with 6 original vertices.

After the second user receives the corona graph, he/ she will do the following computations:

He/ She takes the first block (c_{11}, c_{12}, c_{13}, c_{14}) = (19, 1, 8, 11) and he/she uses his/her shared secret key p =29 to compute the inverses elements of c_{11}, c_{12}, c_{13} and c_{14} as follows.

$$19^{-1} \pmod{29} \equiv 26$$
$$27^{1} \pmod{29} \equiv 14$$
$$8^{-1} \pmod{29} \equiv 11$$
$$11^{-1} \pmod{29} \equiv 8$$

So, a second user gets (26, 14, 11, 8) and since a plaintext message has 6 blocks, therefore, he/she computes

$$(26, 14, 11, 8) - 6 \pmod{26} \equiv (20, 8, 5, 2) = m_1.$$

In the same way, he/she computes all other blocks to m_2, m_3, m_4, m_5 and m_6. In the other words,

$$(24, 21, 3, 20) - 6 \pmod{26} \equiv (18, 15, 23, 14) = m_2$$
$$(12, 21, 4, 16) - 6 \pmod{26} \equiv (6, 15, 24, 10) = m_3$$
$$(1, 19, 22, 25) - 6 \pmod{26} \equiv (21, 13, 16, 19) = m_4$$
$$(21, 2, 11, 24) - 6 \pmod{26} \equiv (15, 22, 5, 18) = m_5$$
$$(7, 9, 7, 26) - 6 \pmod{26} \equiv (1, 3, 1, 20) = m_6.$$

Based on Table (3.1), one can recover the alphabet letters that correspond to these numbers by

$$(20, 8, 5, 2) \rightarrow (\mathrm{T}, \mathrm{h}, \mathrm{e}, \mathrm{b})$$

$$(18, 15, 23, 14) \rightarrow (r, o, w, n)$$

$$(6, 15, 24, 10) \rightarrow (f, o, x, j)$$

$$(21, 13, 16, 19) \rightarrow (u, m, p, s)$$

$$(15, 22, 5, 18) \rightarrow (o, v, e, r)$$

$$(1, 3, 1, 20) \rightarrow (a, c, a, t).$$

Thus, the blocks of the original message is recovered by

Theb – rown – foxj – umps – over – acat.

Hence the message with correct meaning is

The brown fox jumps over a cat.

Example 3.3.1.2.

Suppose m is a message that is given by the following sentence

Smile as much as ache

Here $m = (m_1, m_2, m_3, m_4, m_5)$ such that

m_1 = smil, m_2 = easm, m_3 = ucha, m_4 = syou, m_5 = ache

Based on the alphabet Table (3.1), the blocks of message m_i, for i = 1,2,3,…,5, can be converted into numbers as follows:

$$m_1 = \text{smil} \rightarrow (19, 13, 9, 12)$$

$$m_2 = \text{easm} \rightarrow (5, 1, 19, 13)$$

$$m_3 = \text{ucha} \rightarrow (21, 3, 8, 1)$$

$$m_4 = \text{syou} \rightarrow (19, 25, 15, 21)$$

$$m_5 = \text{ache} \rightarrow (1, 3, 8, 5).$$

Since the number of the blocks is equal to 6, so the numbers in blocks are shifted by adding 5 to them using the shift cipher, namely

$$(19, 13, 9, 12) + 5 \pmod{26} \equiv (24, 18, 14, 17)$$

$$(5, 1, 19, 13) + 5 \pmod{26} \equiv (10, 6, 24, 18)$$

$$(21, 3, 8, 1) + 5 \pmod{26} \equiv (1, 8, 13, 6)$$

$$(19, 25, 15, 21) + 5 \pmod{26} \equiv (24, 4, 20, 1)$$

$$(1, 3, 8, 5) + 5 \pmod{26} \equiv (6, 8, 13, 10).$$

Now, the first user takes his shared secret key which is a prime number p =29, where p =29 > 26. The ciphertext $C = (c_1, c_2, c_3, c_4, c_5, c_6)$, where $c_1 = (c_{11}, c_{12}, c_{13}, c_{14})$, $c_2 = (c_{21}, c_{22}, c_{23}, c_{24})$ and so on, is computed for elements in the shifted blocks though the computations of the inverses elements modulo p as follows.

$$c_{11} \equiv 24^{-1} \pmod{29} \equiv 23$$

$$c_{12} \equiv 18^{-1} \pmod{29} \equiv 21$$

$$c_{13} \equiv 14^{-1} \pmod{29} \equiv 27$$

$$c_{14} \equiv 17^{-1} \pmod{29} \equiv 12$$

$$c_{21} \equiv 10^{-1} \pmod{29} \equiv 3$$

$$c_{22} \equiv 6^{-1} \pmod{29} \equiv 5$$

$$c_{23} \equiv 24^{-1} \pmod{29} \equiv 23$$

$$c_{24} \equiv 18^{-1} \pmod{29} \equiv 21$$

$$c_{31} \equiv 1^{-1} \pmod{29} \equiv 1$$

$$c_{32} \equiv 8^{-1} \pmod{29} \equiv 11$$

$$c_{33} \equiv 13^{-1} \pmod{29} \equiv 14$$

$$c_{34} \equiv 6^{-1} \pmod{29} \equiv 5$$

$$c_{41} \equiv 24^{-1} \pmod{29} \equiv 23$$

$$c_{42} \equiv 5^{-1} \pmod{29} \equiv 6$$

$$c_{43} \equiv 20^{-1} \pmod{29} \equiv 24$$

$$c_{44} \equiv 1^{-1} \pmod{29} \equiv 1$$

$$c_{51} \equiv 6^{-1} \pmod{29} \equiv 5$$

$$c_{52} \equiv 8^{-1} \pmod{29} \equiv 11$$

$$c_{53} \equiv 13^{-1} \pmod{29} \equiv 9$$

$$c_{54} \equiv 10^{-1} \pmod{29} \equiv 3$$

The ciphertext has been sent to second user as a corona graph as shown in Figure (3.3).

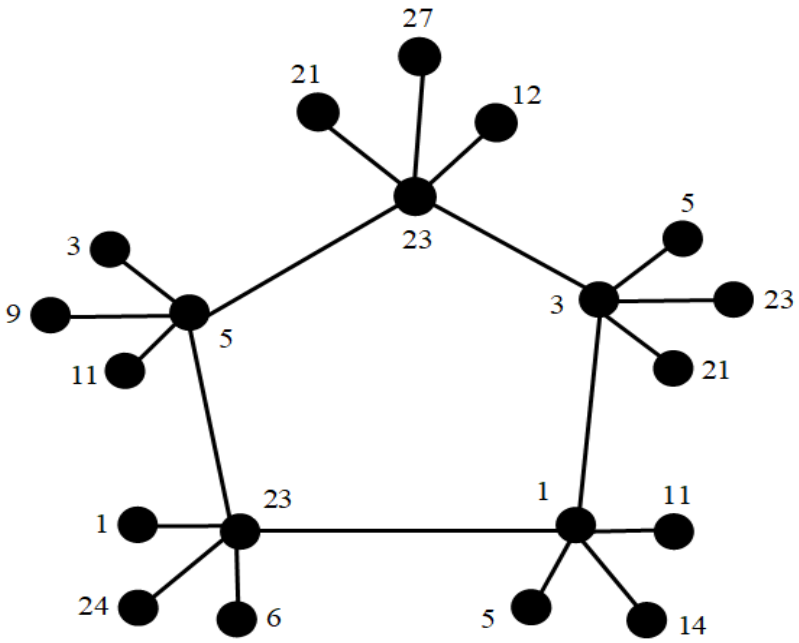


Figure 3.3. A corona graph with 5 original vertices.

After the second user receives the corona graph, he/ she will do the following computations:

He/ She takes the first block (c_{11}, c_{12}, c_{13}, c_{14}) = (23, 21, 27, 12) and he/she uses his/her shared secret key p =29 to compute the inverses elements of c_{11}, c_{12}, c_{13} and c_{14} as follows.

$$23^{-1} \pmod{29} \equiv 24$$

$$21^{1} \pmod{29} \equiv 18$$

$$27^{-1} \pmod{29} \equiv 14$$

$$12^{-1} \pmod{29} \equiv 17$$

So, a second user gets (24, 18, 14, 17) and since a plaintext message has 5 blocks, therefore, he/she computes

$$(24, 18, 14, 17) - 5 \pmod{26} \equiv (19, 13, 9, 12) = m_1.$$

In the same way, he/she computes all other blocks to m_2, m_3, m_4 and m_5. In the other words,

$$(10, 6, 24, 18) - 5 \pmod{26} \equiv (5, 1, 19, 13) = m_2$$

$$(1, 8, 13, 6) - 5 \pmod{26} \equiv (21, 3, 8, 1) = m_3$$

$$(24, 4, 20, 1) - 5 \pmod{26} \equiv (19, 25, 15, 21) = m_4$$

$$(6, 8, 13, 10) - 5 \pmod{26} \equiv (1, 3, 8, 5) = m_5.$$

Based on Table (3.1), one can recover the alphabet letters that correspond to these numbers by

$$(19, 13, 9, 12) \rightarrow (s, m, i, l)$$

$$(5, 1, 19, 13) \rightarrow (e, a, s, m)$$

$$(21, 3, 8, 1) \rightarrow (u, c, h, a)$$

$$(19, 25, 15, 21) \rightarrow (s, y, o, u)$$

$$(1, 3, 8, 5) \rightarrow (a, c, h, e).$$

Thus, the blocks of the original message is recovered by

smil – easm – ucha – syou – ache

Hence the message with correct meaning is

Smile as much as you ache.

3.3.2 Corona Graph for Encryption Schemes: Case II.

The same idea of case (I) can be applied to encrypt the plaintext *m* has the English letters that are represented by numbers of ASCII Table (3.2). The possibility here to choose a plaintext as an English word or an English sentence

consists of some words is more than 26 letters. The number of the allowed letters that can be chosen is 127. So, the letters of the plaintext here have been converted into ASCII Table numbers.

Suppose

$$m = \{m_1, m_2, \ldots, m_k\}.$$

The numbers $\#m_i$ that are corresponded to m_i, for $i = 1, 2, \ldots, k$. The length of the message is k. The first user chooses p, where p is the nearest prime number greater than 127 (127 is the number of the English alphabet letters in ASCII Table) and p is a shared secret key that is computed by the Diffie – Hellman key exchange. The ciphertext C of a message m is computed in similar way as computed in Case (I) as a corona graph. Upon second user receives the corona

graph form the blocks, subtracting the number of all blocks from the elements blocks gives the original message.

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

Example 3.4.1.1. (Study Case II: Encryption Scheme Based on the CG)

Suppose the message is given by the following sentence:

Smile as much as you ache

m (m_1, m_2, m_3, m_4, m_5)

m_1= smile m_2=easm m_3= ucha m_4= syou m_5= ache

Based on encoding alphabet table that is given Table (3.2) the block of message m_i for i = 1,2,3,4,5 can be transformed into number as follows

$$m_1 = \text{smil} \rightarrow (83, 77, 73, 76)$$

$$m_2 = \text{easm} \rightarrow (69, 65, 83, 77)$$

$$m_3 = \text{ucha} \rightarrow (85, 67, 72, 65)$$

$$m_4 = \text{syou} \rightarrow (83, 89, 79, 85)$$

$$m_5 = \text{ache} \rightarrow (65, 67, 72, 69)$$

Since the number of the block is equal to 5, so numbers in blocks are shifted adding 5 to them. The shift cipher namely

$$(83, 77, 73, 76) + 5 \pmod{127} = (88, 82, 78, 81)$$

$$(69, 65, 83, 77) + 5 \pmod{127} = (74, 70, 88, 82)$$

$$(85, 67, 72, 65) + 5 \pmod{127} = (90, 72, 77, 70)$$

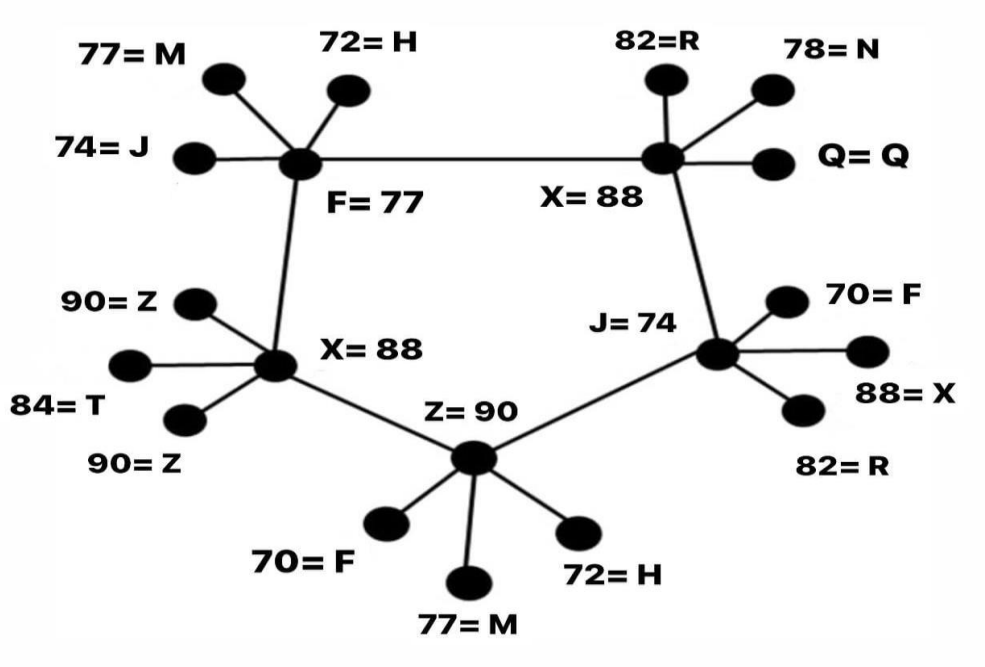
$$(83, 89, 79, 85) + 5 \pmod{127} = (88, 94, 74, 90)$$

$$(65, 67, 72, 69) + 5 \pmod{127} = (70, 72, 77, 74)$$

Now, the first user takes his shared security key which is a prime number P= 131 where 131 > 127

The cipher text of the element modulo as follows:

The ciphertext has been sent to second user as a corona graph as shown in Figure ().



After receiving the coronagraph she/he will do the following computation.

He/she takes the first block (C_{11}, C_{12}, C_{13}, C_{14}) and he/she will use his/her. A shared secret key p=131 to compute inverse elements of C_{11}, C_{12}, C_{13}, C_{14}.

So, second user gets computes

$$(88, 82, 78, 81) - 5 \pmod{131} \equiv (83, 77, 73, 76)$$

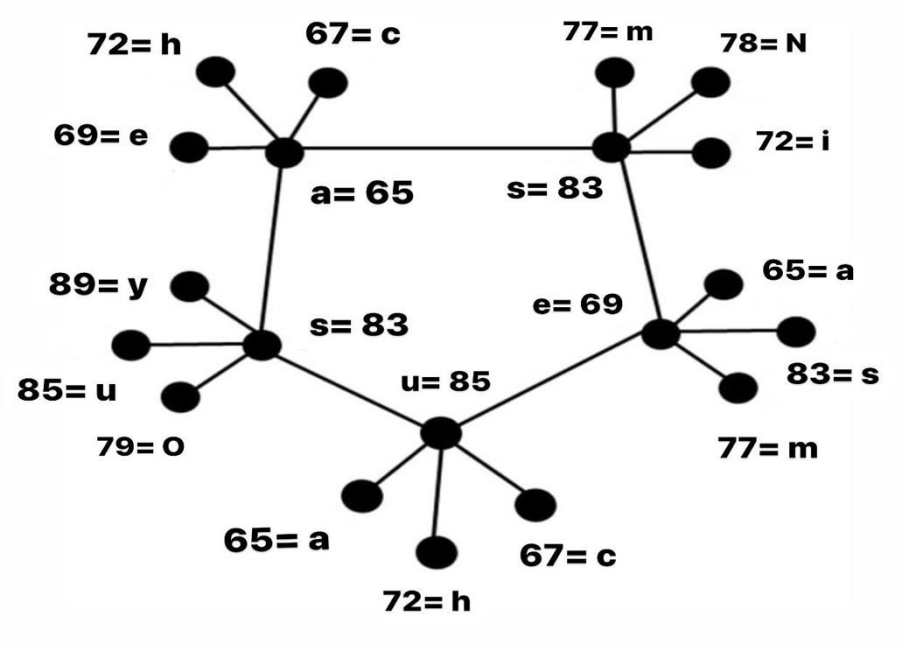
$$(74, 70, 88, 83) - 5 \pmod{131} \equiv (69, 65, 83, 84)$$

$$(90, 72, 77, 72) - 5 \pmod{131} \equiv (85, 67, 72, 67)$$

$$(88, 94, 74, 90) - 5 \pmod{131} \equiv (83, 89, 63, 83)$$

$$(70, 72, 77, 74) - 5 \pmod{131} \equiv (65, 67, 72, 69)$$

Based on Table (3.2) can recover the alphabet letter that are corresponding to these number



so,

$$(83, 77, 73, 76) \rightarrow \text{smil} = m_1$$

$$(69, 65, 83, 77) \rightarrow \text{easm} = m_2$$

$$(85, 67, 72, 65) \rightarrow \text{ucha} = m_3$$

$$(83, 89, 79, 85) \rightarrow \text{syou} = m_4$$

$$(65, 67, 72, 69) \rightarrow \text{ache} = m_5$$

Example 3.4.1.2. (Study Case II: Encryption Scheme Based on the CG)

Suppose the message is given by the following sentence:

The patience is the head of the faith

So, m = (m_1, m_2, m_3, m_4, m_5), thus

m_1= Thepat m_2=iencei m_3= sthehe m_4= adofth m_5=efaith

m_1= Thepat → (84, 72, 69, 80, 65, 84)

m_2= iencei → (73, 69, 78, 67, 69, 73)

m_3= sthehe → (83, 84, 72, 69, 72, 69)

m_4= adofth → (65, 68, 79, 70, 84, 72)

m_5= efaith → (69, 70, 65, 73, 84, 72)

Since the number of the block is equal to 5, so numbers in blocks are shifted adding 5 to them. The shift cipher namely

(84, 72, 69, 80, 65, 84) + 5 (mod 127) = 897774857089

(73, 69, 78, 67, 69, 73)+ 5 (mod 127) = 787483737478

(83, 84, 72, 69, 72, 69)+ 5 (mod 127) = 888977747774

(65, 68, 79, 70, 84, 72)+ 5 (mod 127) = 707384758977

(69, 70, 65, 73, 84, 72)+ 5 (mod 127) = 747569788977

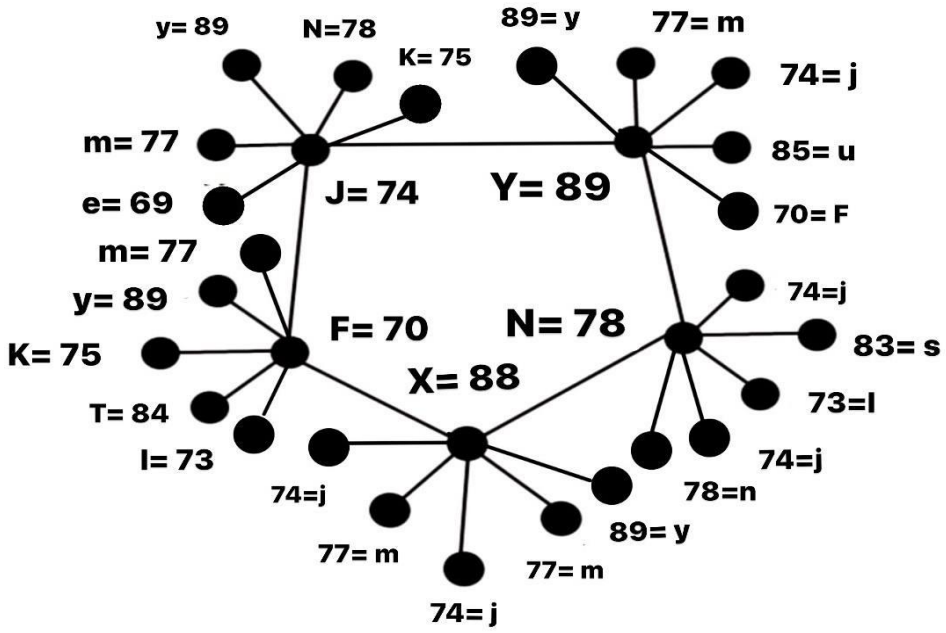
Now, the first user takes his shared security key which is a prime number P= 137 where 137 > 127

The cipher text of the element modulo as follows:

C = (C_1, C_2, C_3, C_4, C_5)

C_1 = (C_{11}, C_{12}, C_{13}, C_{14}), C_2 = (C_{21}, C_{22}, C_{23}, C_{24}) and so on.

The cipher text has been sent to second user as corona graph as shown in Figure (3.4)



After receiving the coronagraph she/he will do the following computation. He/she takes the first block (C_{11}, C_{12}, C_{13}, C_{14}) and he/she will use his/her. Shared key p=137 to compute invers element of C_{11}, C_{12}, C_{13}, C_{14} as follows $(aij)^{-1} \pmod{137} \equiv \#mi$

$$897774857089^{-5} \pmod{137} \equiv 847269806584$$

$$787483737478^{-5} \pmod{137} \equiv 736978686973$$

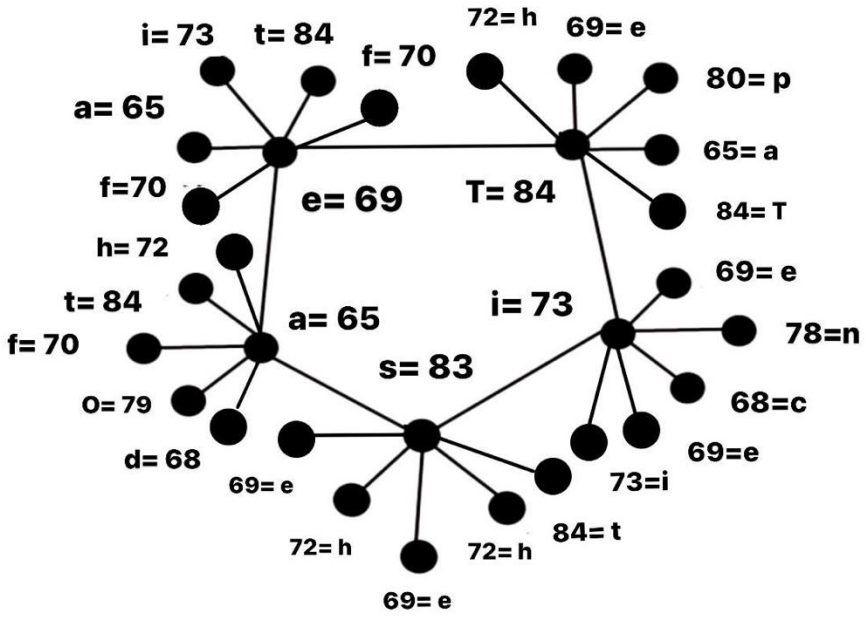
$$888977747774^{-5} \pmod{137} \equiv 838472697269$$

$$707384758977^{-5} \pmod{137} \equiv 656879708472$$

$$747569788977^{-5} \pmod{137} \equiv 697065738472$$

Based on Table (1) can recover the alphabet letter that are corresponding to these number

$84 \rightarrow$ T $72 \rightarrow$ h $69 \rightarrow$ e $65 \rightarrow$ a $84 \rightarrow$ t



$(84, 72, 69, 80, 65, 84) \rightarrow \text{Thepat} = m_1$

$(73, 69, 78, 67, 69, 73) \rightarrow \text{iencei} = m_2$

$(83, 84, 72, 69, 72, 69) \rightarrow \text{sthehe} = m_3$

$(65, 68, 79, 70, 84, 72) \rightarrow \text{adofth} = m_4$

$(69, 70, 65, 73, 84, 72) \rightarrow \text{efaith} = m_5$

3.5 The Security Considerations of CG Encryption Schemes

The proposed symmetric encryption schemes based on the CG graph is a more secure in compare with other symmetric encryption schemes. With CG, the ciphertext has been computed as the CG. The security considerations of new proposed CG encryption schemes depended on random generating the graph *CG* that the attackers want to know them if they determine the ciphertext is computed as CG graph. So, Eve needs to guess the vertices of graph *CG*. Therefore, in case I, each vertices needs 26 possible probabilities to form the correct CG.

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

Based on the result of Case (I), with n = 26 and V =4, then

$$C_4^{26} = \frac{26!}{4!\,(26-4)!} = 14950.$$

Therefore, there are 14950 cases for first original vertex. The total possible probabilities to determine correct graph needs 89700 cases, one of them is correct.

Chapter Four

The Corona Graph for Polyalphabetic Encryption Scheme

CHAPTER 4
The Corona Graph for Polyalphabetic Encryption Scheme

4.1 Introduction

In this chapter, corona graph (CG) 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 CG schemes that are proposed in Chapter (3).

4.2 The CG 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 these rules R_1, R_2 and R_3 to all of these numbers one by one has been done. For instance, if the letters of plaintext m is $m_1, m_2, \ldots, m_K$ then $\#m_1$ it can be moved according to the $R_1 \pmod{26} \equiv a_1$, $\#m_2$ it moves according to the

$R_2(\text{mod } 26) \equiv a_2, \ldots, \#m_K$ it will be moved into the $R_i \ (\text{mod } 26) \equiv a_K$, 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 $r_1 \ (\text{mod } 26) \equiv \#m_1$, a_2 it moves in the opposite direction according to the $r_2 \ (\text{mod } 26) \equiv \#m_2$, ..., a_K it moves in the opposite direction according to the $r_i \ (\text{mod } 26) \equiv \#m_K$.

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

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

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

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

Suppose m is a message that is given by the following sentence

"The brown fox jumps over a cat".

Here $m = (m_1, m_2, m_3, m_4, m_5, m_6)$ such that

m_1 = Theb, m_2 = rown, m_3 = foxj, m_4 = umps, m_5 = over, m_6 = acat.

Based on the alphabet Table (3.1), the blocks of message m_i, for $i = 1,2,3,\ldots,6$, can be converted into numbers as follows:

$$m_1 = \text{Theb} \rightarrow (20, 8, 5, 2)$$

$$m_2 = \text{rown} \rightarrow (18, 15, 23, 14)$$

$$m_3 = \text{foxj} \rightarrow (6, 15, 24, 10)$$

$$m_4 = \text{umps} \rightarrow (21, 13, 16, 19)$$

$$m_5 = \text{over} \rightarrow (15, 22, 5, 18)$$

$$m_6 = \text{acat} \rightarrow (1, 3, 1, 20).$$

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.
3- Shift the third letters five positions to its right.
4- Shift the fourth letters six positions to its right.
5- Shift the fifth letters seven positions to its right.
6- Shift the sixth letters nine positions to its right.

$$(20, 8, 5, 2) \rightarrow (23, 11, 8, 5) \rightarrow \text{Wkhe}$$

$$(18, 15, 24, 10) \rightarrow (21, 19, 2, 14) \rightarrow \text{YSBN}$$

$$(6, 15, 24, 10) \rightarrow (11, 21, 3, 14) \rightarrow \text{KOXJ}$$

$$(21, 13, 16, 19) \rightarrow (1, 19, 22, 25) \rightarrow \text{ASVY}$$

$$(15, 22, 5, 18) \rightarrow (22, 3, 12, 25) \rightarrow \text{VCLY}$$

$$(1, 3, 1, 20) \rightarrow (10, 12, 10, 3) \rightarrow \text{JLJC}$$

In more details, the letter *T* moves into three positions to its right to become *w*, *h* letter moves to four positions to its right to become *k*. Repeating the key process for all letters of the word as follows.

Theb rown foxj umps over acat

Wkhe YSBN KOXJ ASVY VCLY JLJC

The letters of the encoded word "Wkhe YSBN KOXJ ASVY VCLY JLJC" which can form by a list

List: {*w, k, h, e*} = {23,11,8,5, …….}.

This list can be represented by corona graph CG as shown in Figure (4.1). which considered as the ciphertext that is sent to receiver by sender.

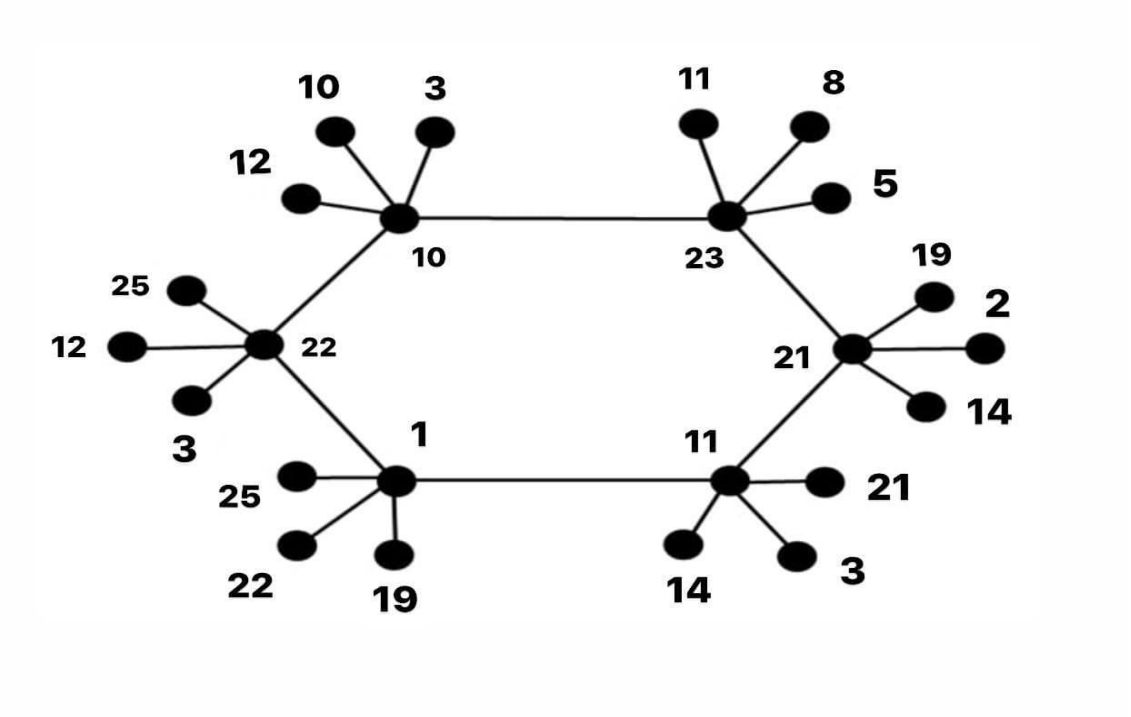


Figure 4.1. The Corona graph with 6 vertices.

The second user (receiver) receivers the Corona graph. He/ She wants to decrypt the ciphertext and recover the original plaintext. He/ She first writes down the labeled vertices in list This list is

List: = {23,11,8,5, ……}.

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 into left.
2. Shift the second letters four positions to into left.
3. Shift the third letters five positions to into left.
4. Shift the fourth letters six positions to into left.
5. Shift the fifth letters seven positions to into left.
6. Shift the sixth letters nine positions to into left.

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

Wkhe YSBN KOXJ ASVY VCLY JLJC

becomes

Theb rown foxj umps over acat

Thus, the plaintext *m* is **"The brown fox jumps over a cat".**

Example 4.2.2.

Suppose *m* is a message that is given by the following sentence :

"The brown fox jumps over a cat".

Here $m = (m_1, m_2, m_3, m_4, m_5, m_6)$ such that

m_1 = Theb, m_2 = rown, m_3 = foxj, m_4 = umps, m_5 = over, m_6 = acat.

Based on the alphabet Table (3.1), the blocks of message m_i, for $i = 1,2,3,\ldots,6$, can be converted into numbers as follows:

m_1 = Theb → (20, 8, 5, 2)

m_2 = rown → (18, 15, 23, 14)

m_3 = foxj → (6, 15, 24, 10)

m_4 = umps → (21, 13, 16, 19)

$$m_5 = \text{over} \rightarrow (15, 22, 5, 18)$$

$$m_6 = \text{acat} \rightarrow (1, 3, 1, 20).$$

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.

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

4- Shift the fourth letters six positions to its right.

5- Shift the fifth letters seven positions to its right.

6- Shift the sixth letters nine positions to its right.

$$(20, 8, 5, 2) + 3 \text{ (mod1 27)} \equiv 231185$$

$$(18, 15, 23, 14) + 4 \text{ (mod 127)} \equiv 22192718$$

$$(6, 15, 24, 10) + 5 \text{ (mod 127)} \equiv 11202915$$

$$(21, 13, 16, 19) + 6 \text{ (mod 127)} \equiv 27192225$$

$$(15, 22, 5, 18) + 7 \text{ (mod127)} \equiv 22291225$$

$$(1, 3, 1, 20) + 9 \text{ (mod 127)} \equiv 10121029$$

Now, the first user takes his shared security key which is a prime number P= 131 where 137 > 127

The cipher text of the element modulo as follows:

$$C = (C_1, C_2, C_3, C_4, C_5, C_6)$$

$$C_{11} \equiv 23^{-1} \text{ (mod 131)} \equiv \quad \text{(mod 131)}$$

$$C_{12} \equiv 11^{-1} \text{ (mod 131)} \equiv \quad \text{(mod 131)}$$

$$C_{13} \equiv 8^{-1} \text{ (mod 131)} \equiv \quad \text{(mod 131)}$$

$$C_{14} \equiv 5^{-1} \pmod{131} \equiv \quad \pmod{131}$$

$$C_{21} \equiv 22^{-1} \pmod{131} \equiv \quad \pmod{131}$$
$$C_{22} \equiv 19^{-1} \pmod{131} \equiv \quad \pmod{131}$$
$$C_{23} \equiv 27^{-1} \pmod{131} \equiv \quad \pmod{131}$$
$$C_{24} \equiv 18^{-1} \pmod{131} \equiv \quad \pmod{131}$$

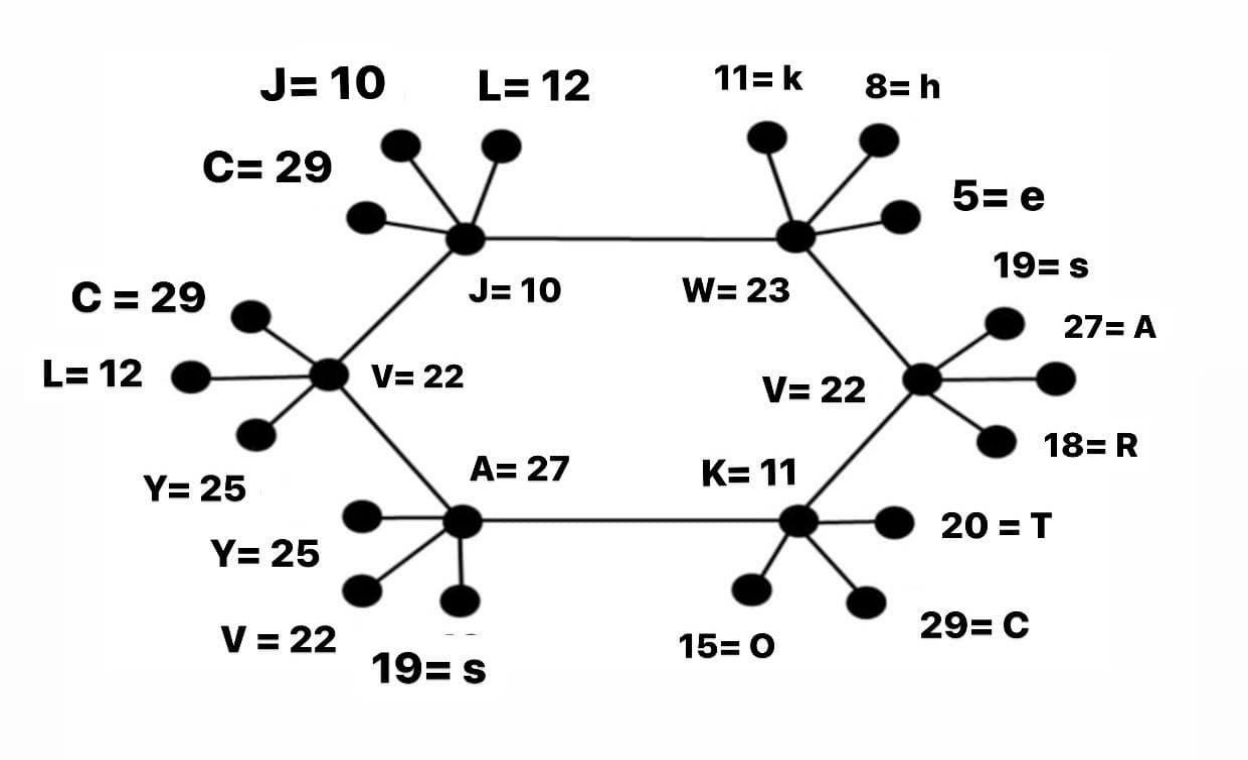
$$C_{31} \equiv 11^{-1} \pmod{131} \equiv \quad \pmod{131}$$
$$C_{32} \equiv 20^{-1} \pmod{131} \equiv \quad \pmod{131}$$
$$C_{33} \equiv 29^{-1} \pmod{131} \equiv \quad \pmod{131}$$
$$C_{34} \equiv 15^{-1} \pmod{131} \equiv \quad \pmod{131}$$

$$C_{41} \equiv 27^{-1} \pmod{131} \equiv \quad \pmod{131}$$
$$C_{42} \equiv 19^{-1} \pmod{131} \equiv \quad \pmod{131}$$
$$C_{43} \equiv 22^{-1} \pmod{131} \equiv \quad \pmod{131}$$
$$C_{44} \equiv 25^{-1} \pmod{131} \equiv \quad \pmod{131}$$

$$C_{51} \equiv 22^{-1} \pmod{131} \equiv \quad \pmod{131}$$
$$C_{52} \equiv 29^{-1} \pmod{131} \equiv \quad \pmod{131}$$
$$C_{53} \equiv 12^{-1} \pmod{131} \equiv \quad \pmod{131}$$
$$C_{54} \equiv 25^{-1} \pmod{131} \equiv \quad \pmod{131}$$

$$C_{61} \equiv 10^{-1} \pmod{131} \equiv \quad \pmod{131}$$
$$C_{62} \equiv 12^{-1} \pmod{131} \equiv \quad \pmod{131}$$
$$C_{63} \equiv 10^{-1} \pmod{131} \equiv \quad \pmod{131}$$
$$C_{63} \equiv 29^{-1} \pmod{131} \equiv \quad \pmod{131}$$

The cipher text has been sent to second user as a corona graph as shown in Figure ( ).



After receiving the coronagraph she/he will do the following computation.

He/she takes the first block (C_{11}, C_{12}, C_{13}, C_{14}) and he/she will use his/her. shared key p=131($)^{-1}$ (mod 13) =

$$231185 - 3 \pmod{131} \equiv 20852$$

$$22192718 - 4 \pmod{131} \equiv 18152314$$

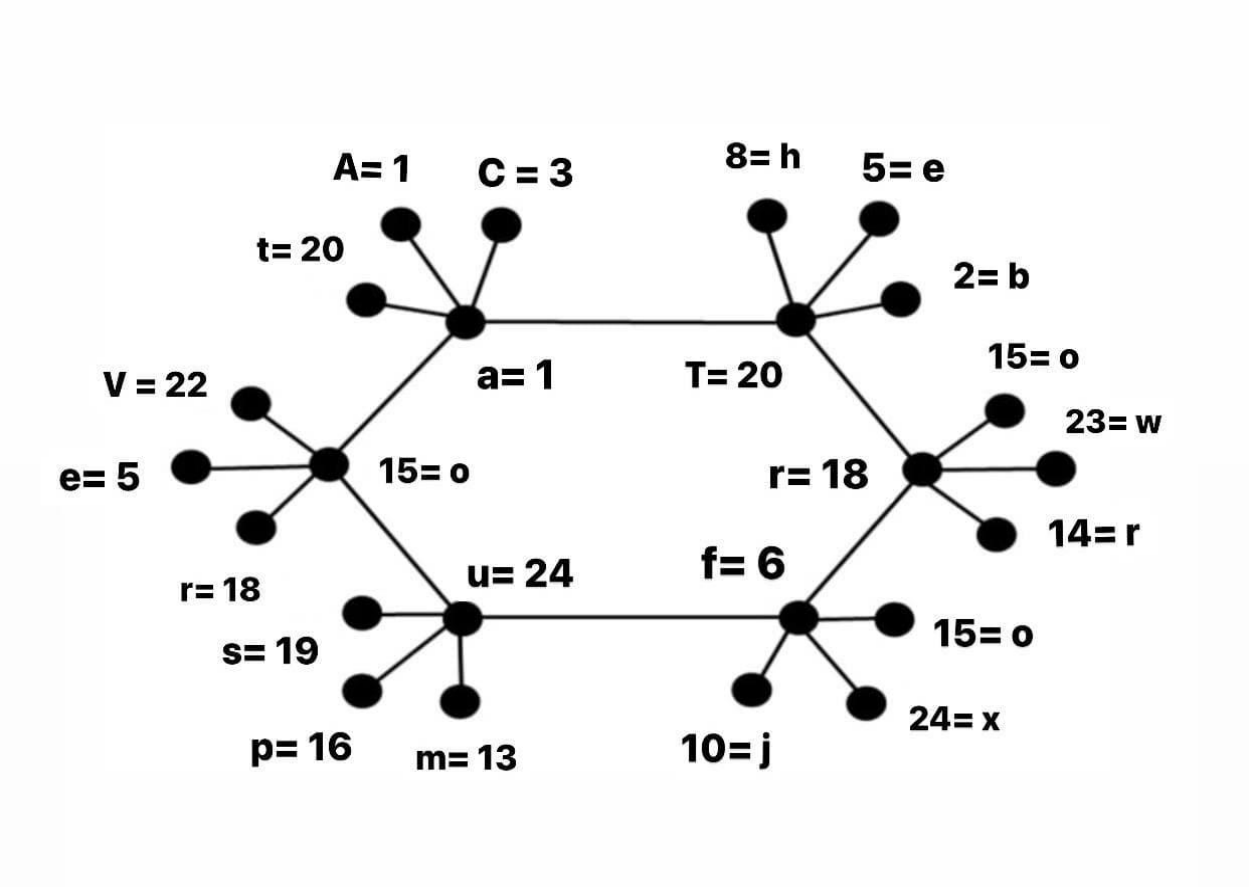
$$11202915 - 5 \pmod{131} \equiv 6152410$$

$$27192225 - 6 \pmod{131} \equiv 21131619$$

$$22291225 - 7 \pmod{131} \equiv 1522518$$

$$10121029 - 9 \pmod{131} \equiv 13120$$

Based on Table (1) can recover the alphabet letter that are corresponding to these number



(20, 8, 5, 2) → Theb = m_1

(18, 15, 23, 14) → rown = m_2

(6, 15, 24, 10) → foxj = m_3

(21, 13, 16, 19) → umps = m_4

(15, 22, 5, 18) → over = m_5

(1, 3, 1, 20) → acat = m_6

Chapter Five

Conclusion And References

CHAPTER 5

CONCLUSION AND REFERENCES

5.1 Conclusions

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

5.2 Future work

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. Shao, Z., Kosari, S., Anoos, R., Sheikholeslami, S. M., & Dayap, J. A. (2020). Outer-convex dominating set in the corona of graphs as encryption key generator. Complexity, 2020.
2. Muthammai, S., & Dhanalakshmi, S. (2019). Edge domination in Boolean function graph B (L (G), NINC) of a graph. *Journal of Discrete Mathematical Sciences and Cryptography*, *22*(5), 847-855.
3. Murali, B. J., Thirusangu, K., & Balamurugan, B. J. (2017). Combination Cordial Labeling of Flower Graphs and Corona Graph. *International Journal of Pure and Applied Mathematics*, *117*(11), 45-51.
4. Sangeetha, S., & Usharani, U. (2019, June). Relaxed mean labeling of some corona graphs. In *AIP Conference Proceedings* (Vol. 2112, No. 1, p. 020067). AIP Publishing LLC.
5. Kulli, V. R. (2016). Inverse total domination in corona and join of graphs. *Journal of Computer and Mathematical Sciences*, *7*(2), 61-64.
6. Beaula, C., & Venugopal, P. (2020). Cryptosystem using double vertex graph. *Indian Journal of Science and Technology*, *13*(44), 4483-4489.

الملخص

تم اقتراح نسخة جديدة من مخططات التشفير المتماثل في هذا العمل .تستخدم هذه الإصدارات تعريفًا جديدًا للرسم البياني لكورونا .اعتمدت هذه المخططات المقترحة الجديدة على قيم الأبجدية الإنجليزية ، وقيم ASCII والتشفير متعدد الأبجدية على التوالي .يتم اختيار الرسالة ككلمة إنجليزية أو جملة إنجليزية . يعتبر النص المشفر للرسالة الأصلية بمثابة مخطط كورونا الذي يتم إرساله إلى مرسل المستلم .تمت مناقشة العديد من النتائج التجريبية لخطط تشفير مخطط كورونا المقترحة .يتم تحديد الاعتبارات الأمنية لأنظمة التشفير المقترحة.

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابل -كلية التربية للعلوم الصرفة
قسم الرياضيات

مخطط كورونا للتشفير

بحث مقدم الى
قسم الرياضيات -كلية التربية للعلوم الصرفة -جامعة بابل
و هو جزء من نيل شهادة الدبلوم العالي تربية / رياضيات

من قبل
اوراد عبد حمزة حسين

بأشراف
ا.م.د. رومى كريم عجينة

محرم ١٤٤٣ ايلول 2021