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

Color Star Graph for Encryption Schemes

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

Atheer Jawad Kadhim Omran

Supervised by

Asst. Prof. Dr. Ruma Kareem K. Ajeena

A.D 2022 **1444**

بسم الله الرحمن الرحيم

﴿ قَالُواْ سُبْحَانَكَ لا عِلْمَ
لَنَآ إِلَّا مَا عَلَّمْتَنَآ إِنَّكَ
أَنتَ ألعَلِيم ألْحَكِيمُ ﴾

صدق الله العظيم

سورة البقرة

آية (32)

Supervisor Certificate

I certify that this research entitled " **Colored Graphs for Encryption Schemes** " for the student **Atheer Jawad Kadhim Omran** , 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 “**Color Star Graph for Encryption Schemes ”** And I found that this research is qualitied for debate.

Signature:

Name: Dr.Hawraa Abbas Almurieb

Title: Functional Approximation Theory

Address: Collage of education for pure sciences

Date:

Certification of Linguistic Expert

This is to certify that I have read this research, entitled **“Color Star Graph for Encryption Schemes”** And I found that this research is qualitied for debate.

Signature:
Name: Amera Al-funjan
Title:Lecturer
Address: Collage of education for pure sciences
Date:

Examination Committee Certification

We certify that we have read this research entitled " **Color Star Graph for Encryption Schemes ”** 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: **Ali Younis Shakir**
Title: Algebra
Date:

Member / Supervisor
Signature:
Name: **Dr. Ruma Kareem K.Ajeena**
Title: Cryptography and number theory
Date:

Member
Signature:
Name: **Dr. Hayder Kadhim Zghair**
Title: **infonmation Technolveg**
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.

Chapter One

Introduction

Chapter Two

Two Graph theory and Cryptography

Chapter Three

Coloring Star Graph for Encryption Scheme

Dedication

To who gave me the endurance to complete my road my father

To the kindest woman with most pure endless love in the universe, my mother

To my lovely sister and brothers

To my close friends

To my beloved country, Iraq

The martyrs of Iraq with all the love and appreciation

Abstract.

In this work, alternative symmetric encryption (DE) scheme are proposed based on new formula of shared secret key. This key is generated using the coloring star graph (CSG). This cipher text of the plaintext, that is an english word or english sentence, is computed and sent in the channel as the CSG. The attackers here with the proposed SE scheme facing the difficulty to recover the secret key. So, the security of the proposed CSG-SE scheme depending on how to generate the secret key. Thus, the CSG-SE scheme considers as more secure SE scheme in compare with previous ones for communication.

List of Contents

CHAPTER 1

1.1 Introduction

Cryptography is science to design and analysis the mathematical techniques that enable secure communications in the presence of malicious adversaries[4]. It is a technique that enables secure communication in the face of attacks by hackers or other attackers. Graph theory is widely used as a tool for encryption due to its various properties and its easy representation on computers as a matrix. It is considered as an essential tool in many cryptographic applications. Most of them focused on applying various concepts of graph theory to design the symmetric encryption algorithms [1,2]. Some researchers proposed cryptographic algorithms using paths in any graph [3] and others proposed encryption algorithms using directed graphs [4].

1.2 Previous Works

In 2001, Ustimenko patented a new study using graphs as tools for symmetric encryption. The general idea of this study is to treat the vertices of a graph as messages and walks of a certain length as encryption tools. He studied the quality of such an encryption in the case of graphs of high girth by comparing the probability of guessing the message (vertex) at random with the chance of breaking the key [2].

In 2004, Samid [3], presented an encryption method that considered a graph as a key. Charting a path on that graph is used to encrypt the data. A sequence of vertices on the path of the key graph forms the plaintext. Whereas, a sequence of edges between those vertices forms the ciphertext. In 2007, Mittenthal [4], proposed an algorithm for finding the complete Latin squares based on the directed graphs and their applications to encryption schemes.

In 2012, Selvakumar and Gupta, [5], proposed their study using the fundamental circuits and cut-sets in cryptography. They presented an innovative algorithm for encryption and decryption using the connected graphs.

In 2015, Femina and Antony [6], introduced a study of data encryption standard using graph theory. Her study used the rules of Hamilton's path and the process of anti-magic graph labeling on a cube to arrive into the ultimate secure condition.

In 2017, Ahmed and Babujee [7], introduced an encryption scheme through the labeled graphs using the strong face bimagic labeling.

In 2019, Ajeena [8], proposed two studies, first one is her chapter to use subgraph H of the graph G or the other graphs to represent a scalar v in elliptic scalar multiplication vP directly. Speeding up of elliptic scalar multiplication computations have been obtained through reducing the computational complexities of the proposed algorithms and previous ones.

1.3 The Problem Statement of This Research

This work proposed new symmetric encryption scheme using the coloring star graph (CSG). The shared secret key is generated as a sequence based on the CSG and encrypted the plaintext and sending to receiver as the CSG to increase the level of security for these schemes.

1.4 The structure of this Research

This research consists of three chapters:

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

Chapter 2. Mathematical Background on Graph theory and Cryptography

Chapter 3. Coloring Star Graph for Encryption Scheme

Chapter Two

Two Graph theory and Cryptography

This chapter includes two parts, first one presents some graph theory concepts. Whereas, in second part the introduction to cryptography has been discussed.

2.1 Introduction to Graph Theory

This section presents some important concepts of the graph theory, especially, coloring graph

Definition 2.2.1. (Graph)[9]. The graph G=(V(G),E(G) or simply G=(V,E) is collection of non-empty finite vertex set $V(G)$ and edge set $E(G)$ can be an empty set. Each element of V(G) is called a vertex of G and each element (u,v) $\in$ E(G) is an unordered pair called an edge of G where (u,v) $\in$ V(G).

Example 2.2.1 A graph with five vertices and five edges.

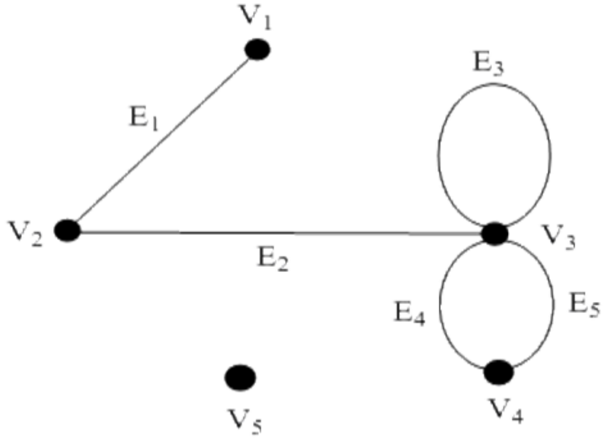

Figure 2.1. A graph with five vertices and five edges.

Definition 2.2.2. (Adjacent) [9]. If $E_1=V_1V_2$ is an edge of G then V_1 and V_2 are adjacent to each other as shown in Figure (2.1).

Definition 2.2.3. (Order and Size of *G*) [10]. A graph G is said to be of order n if $|V(G)|=n$ and, of size m if $|E(G)|=m$.

For example, in a graph G in Figure (2.1), $|V(G)|=5$ and $|E(G)|=5$.

Definition 2.2.4. (Edge) [9]. Two vertices u and v are adjacent if they are connected by an edge, in the word (u,v) is an edge.

Definition2.2.5. (Parallel) [9]. In a graph if edges have the same end vertices, then these edges are called parallel whereas, a loop can be formed by edge that has the same begin vertex and end vertex. See Example (2.2.1), the parallel edges are E_4 and E_5, while E_3 forms a loop has a vertex V_3.

Definition 2.2.6. (Simple Graph) [10]. A graph is simple if it has no parallel edges or loops.

Definition 2.2.7. (Multi Graph) [9]. A graph that has more than one edge between a pair of vertices is called Multi Graph.

Example 2.2.2. A multi graph as shown in Figure (2.2).

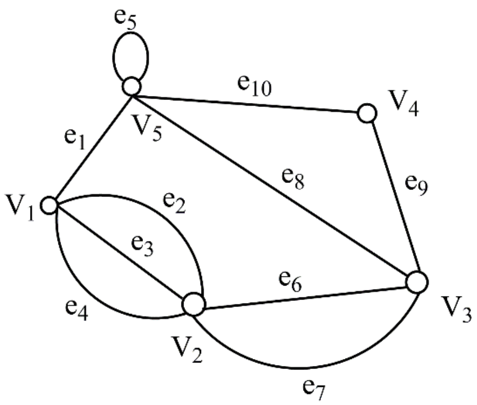

Figure 2.2. A multi graph.

Definition 2.2.8. (Null graph) [9]. A graph with an empty edge set is called a null graph. A null graph with n vertices is denoted by N_n.

Example 2.2.4. A null graph N_6 with six vertices as shown in Figure (2.3).

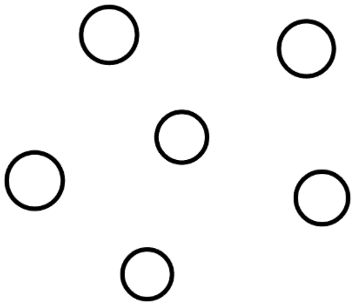

Figure 2.3. A null graph.

Definition 2.2.9. (Complete Graph) [10]. A graph in which each pair of distinct vertices are adjacent is called a complete graph. A complete graph with *n* vertices is denoted by K_n.

Example 2.2.5. A complete graph K_5 as shown in Figure (2.4).

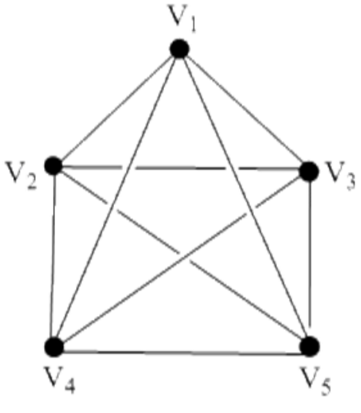

Figure 2.4. A complete graph K_5.

Definition 2.2.10. (**Bipartite Graph)** [9]. A graph G is called a bipartite graph if the vertex set V of G can be partitioned into two disjoint nonempty sets V_1 and V_2, both of which are independent.

Example 2.2.5. A bipartite graph as shown in Figure (2.5)

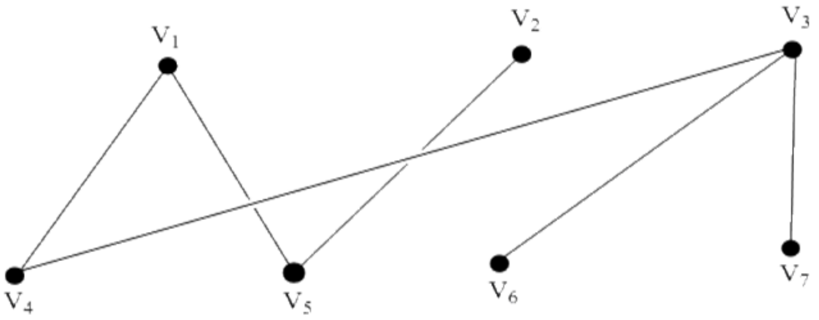

Figure 2.5. A bipartite graph.

$V=\{ V_1,V_2 ,V_3,V_4,V_5,V_6 ,V_7\}$

$U=\{ V_1,V_2 ,V_3\}$

$T=\{V_4,V_5,V_6 ,V_7\}$

No edge between any vertex U and T. And $V= U \cup T$.

Definition 2.2.11. (Complete Bipartite Graph) [9]. A complete bipartite graph where the two partite sets contains 3 and 4 vertices, respectively. This graph is denoted by $K_{3,4}$. In general, a complete bipartite graph is denoted by $K_{m,n}$ if its two partite sets contain m and n vertices, respectively. One can easily see that $K_{m,n}$ contains $m \times n$ edges.

Example 2.2.6. A complete bipartite graph as shown in Figure (2.6).

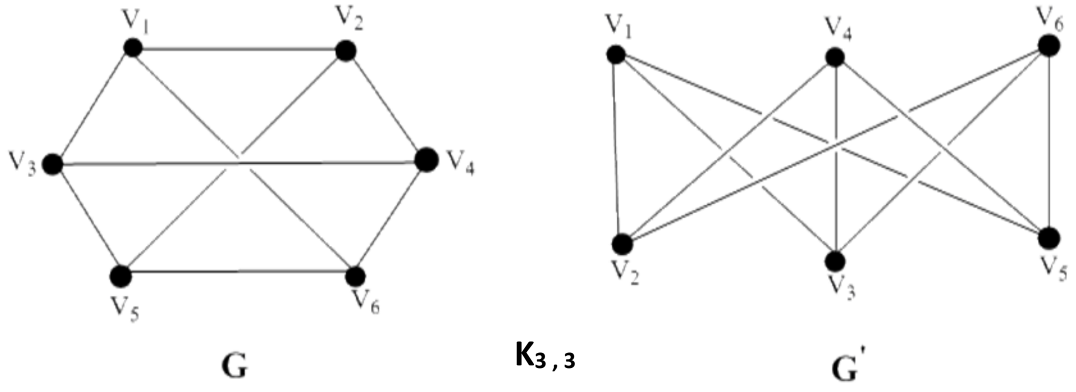

Figure 2.6. A complete bipartite graph.

Definition 2.2.12. (Regular Graph) [9]. If all the vertices of a graph *G* have equal degrees, then we call *G* a regular graph. We call it a *k-regular graph* if the common degree is *k*.

Example 2.2.7. A regular graph as shown in Figure (2.7).

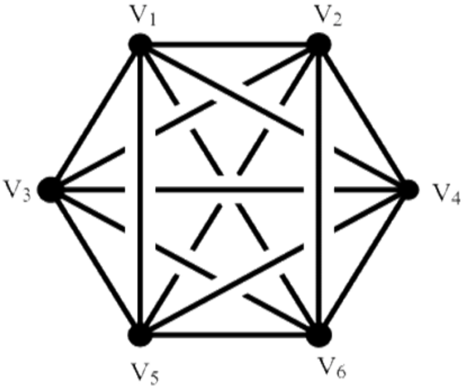

Figure 2.7. A regular graph.

Definition 2.2.13. (Path Graph) [9]**.** A path graph is a graph *G* that contains a list of vertices $V_1,V_2,\ldots,V_p$ of *G* such that for $1 \leq i \leq p\text{-}1$, there is an edge $(V_i\ ,$ $V_{i+1})$ in *G* and these are the only edges in *G* the two vertices V_1 and V_2 are called the end-vertices of *G*, path with *n* vertices P_n

Definition 2.2.14. (Open Path) [10]**.** An open path in which the first and last vertices are distinct.

Example 2.2.8. A path graph has 9 vertices and 8 edges.

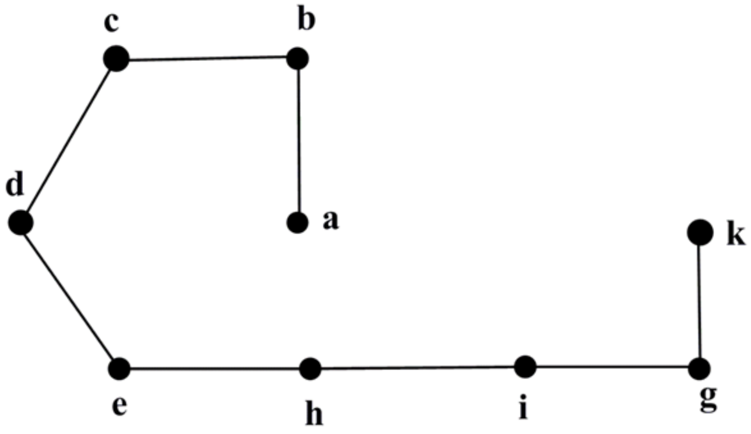

Figure 2.8. A path graph.(open path)

Definition 2.2.15. (Walk Graph) [9]**.** Let *G* be a graph, a walk in *G* is a nonempty list $W=V_0,E_1, V_1,E_2,\ldots,V_{f-1},E_f$. whose element are alternately vertices and edge of G where for $1 \leq i \leq f$, the edge E_i has end vertices V_{i-1} and V_i . The vertices V_0 and V_f are called the end vertices of *W*. If the end vertices of a walk *W* of a graph *G* are *u* and *v* respectively, *W* is also called an *u*, *v*-walk in *G*.

Definition 2.2.16. (Trial Graph) [10]. A graph *G* is a walk in *G* with no repeated edges. That is, in a trail an edge cannot appear more than once.

Remark 2.2.1. A path is with no repeated except and vertices [11].

Remark 2.2.2. A path is a trial but the converse is not true [11].

Example 2.2.9. A walk and trial graph

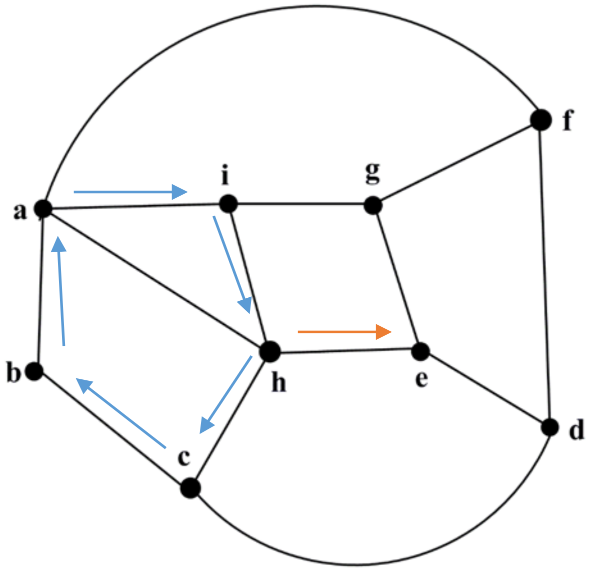

Figure 2.9. A walk graph.

W_1=$a,(a,i),i,(i,h),h,(h,c),c,(c,b),b$

W_2= $a,(a,i),i,(i,h),h,(h,c),c,(c,b),b,(b,a),a,(a,i),i$

W_1 is a walk and trial

W_2 is walk but not trial.

2.3 Color Graph

2.3.1. Vertex Coloring:

It is nothing but an assignment of colors to the non-adjacent vertices of the given Graph[9]. It means that the terminal vertices of the edge should not be assigned by the same color.

2.3.2. Edge Coloring:

It is the way of assigning colors to the non-adjacent edges of the given graph[14].

2.3.3. Region Coloring:

It is an assignment of colors to the different region of the planar graph [12]. These regions are converted into graph. The regions are partitioned into different connected graph. The edges of the regions are collected. Different edges enclosed the region are assigned by same color

2.3.4. Chromatic Number

The minimum number of colors required to color the non-adjacent vertices of the graph is called as chromatic number. It is denoted by CN (G)[13].

2.3.4.1. Calculating Chromatic Number to Various Types of Graphs

In this section, calculating the chromatic number for Various Graph is determined [13]. Such as Null Graph, Trivial Graph, Complete Graph, Regular Graph, Star Graph, Cycle Graph. Chromatic Number depends on their structures of the corresponding graphs.

2.3.5.Null Graph

It has single vertex or more than one vertex without edge. This graph chromatic number is equivalent to number of vertices of the given graph. Each vertex is not adjacent itself. Each vertex has colored by different colors. Therefore CN (G) = Number of Vertices V (G) [13].

2.3.6.Trivial Graph

This graph has single vertex only. It has colored by single color only ie.

CN (G) =1.

2.3.5. Complete Graph:

Each vertex of Complete Graph is adjacent with other vertices of the given graph. A graph with n vertices has n-1 degree. It is denoted by K_n. Each vertex is colored by different colors [13]. A complete Graph has n Chromatic Number i.e. CN (G) =n.

2.3.6. Wheel Graph

This graph looks like a wheel. All Vertices are adjacent with the center vertex throughthe edges. It gets from the cycle graph [13]. All the vertices of the cycle graph are incident withthe center vertex. It is denoted by W_n.

This graph has n vertices and 2n-1 edges. In the First

2.3.7. Star Graph

This is the very interested type of Graph [13]. Here single vertex is connected with all the other vertices in the given graph. n vertex star graph is denoted S_n. n-1 vertices are adjacent with nth vertex (called as center node). These n-1 vertices are not adjacent themselves. It looks like wheel graph but it has loosened its boundary edges. Center Nodeonly has degree n-1. Remaining vertices has single degree. It may be considered as terminal nodes. Coloring of this type of graph is very easiest one. It needs only two colors for coloringthis type of graphs. Here Chromatic number is two only [13].

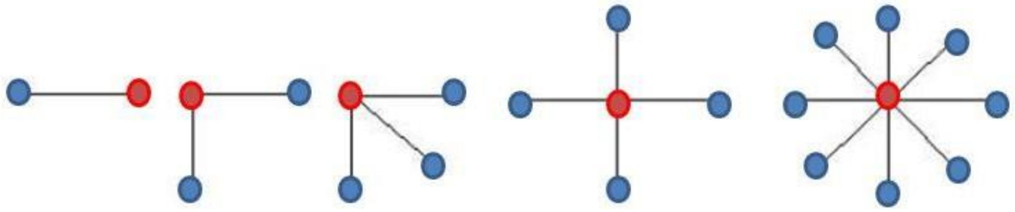

Figure 2.10. Graph Coloring of Star Graphs.

2.4 Introduction to Cryptography

Some basic concepts related to cryptography are discussed as follows.

2.4.1 Basic Concepts

In this section, some important definitions are presented as follows.

Definition 2.4.1.1. Cryptography is the design and analysis of mathematical techniques that enable secure communications in the presence of adversaries [14].

Definition 2.4.1.2. Cryptosystem. A cryptographic system is specifically a set of methods (algorithms) for computing (implementing) the encryption and decryption [14].

Definition 2.4.1.3. Cryptanalysis is the study of analyzing cryptosystem in order to study the hidden aspects of the systems [14].

Definition 2.4.1.4. [40] Plaintext. The information which we want to protect from other people (attackers) [14].

Definition 2.4.1.5. Security. It means that the difficulty to know the information which transferred over the channel easily [14].

2.4.2 Basic Communications Model

In Figure (2.11), entities **A** (Alice) and **B** (Bob) are communicating over an unsecured channel. We assume that all communications take place in the presence of an adversary **E** (Eve) whose objective is to defeat any security services being provided to **A** and **B** [14].

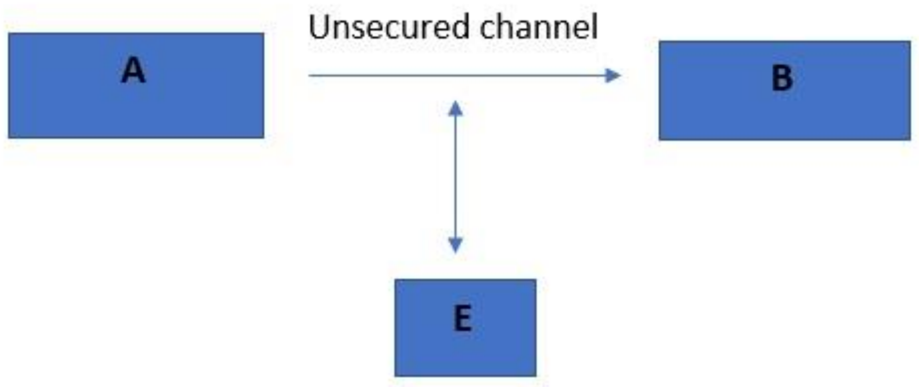

Figure 2.12 Basic communications model.

For example, A and B could be two people communicating over a cellular telephone network, and E is attempting to eavesdrop on their conversation.

2.4.3. Some Important Kinds of Cryptosystems

2.4.3.1 Symmetric-Key Cryptosystems.

The cryptosystems which use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information. Basically, symmetric encryption uses a single key for both encryption and description. And it is fast in execution. It is algorithm DES, 3DES, AES, and RC4. The purpose of the symmetric encryption is uses for bulk data transmission [14].

information. Basically, symmetric encryption uses a single key for both encryption and description.

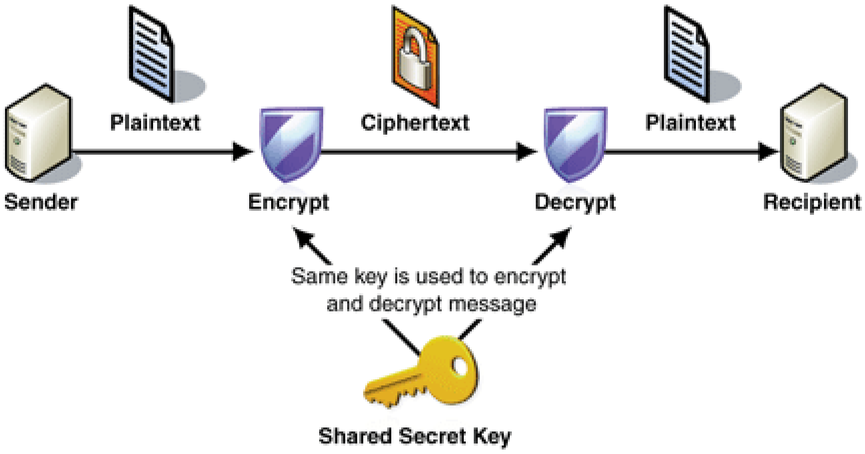

Figure 2.13. Symmetric-Key Cryptosystems.

2.4.3.2 Asymmetric-Key Cryptosystems (Public-Key Cryptosystems).

They use public and private keys to encrypt and decrypt data. The keys are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key and another one can stay as a secret, which is called a private key. Basically, asymmetric encryption uses a different key for encryption and decryption. And it is slow in execution due to the high computation burden. It is algorithm Diffie-Hellman, RSA. The purpose of the asymmetric encryption is often used for securely exchanging secret key [14].

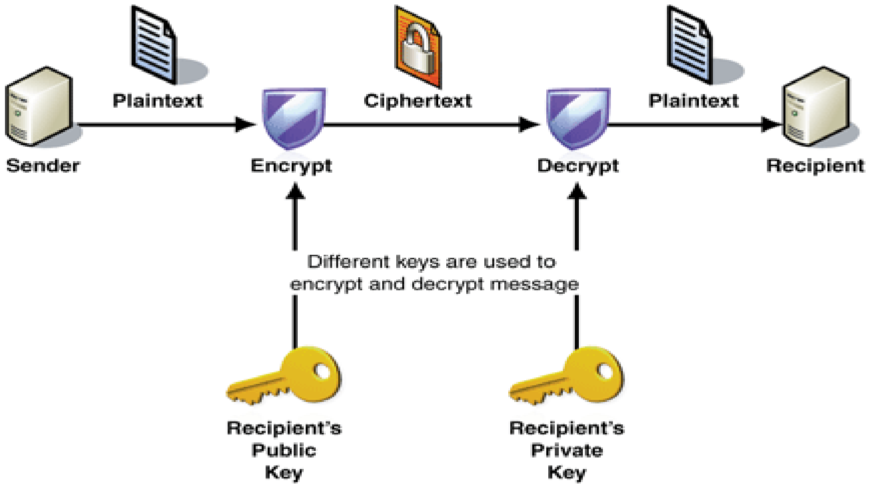

Figure 2.14 Asymmetric-Key Cryptosystems (Public-Key cryptosystems).

Chapter Three

Coloring Star Graph for Encryption Scheme

3.1 Introduction

The chapter presents new version of symmetric encryption scheme which used the coloring star graph to generate the shared secret key and to compute the cipher text of a plain text that is represented by an English word or sentence this version is discussed as follows.

3.2 The Symmetric Encryption Scheme Based on CSG

The coloring star Graph for symmetric Encryption scheme suppose M is plaintext that can be given in an english word or sentence. In other words,

$$M = \{m_1, m_2, \ldots, m_n\} = \{m_i\}_{\,i=1,2,\ldots,n}.$$

The English alphabetic values (EAVS) is given by

$$A \to 0,\ \ B \to 1,\ \ C \to 2,\ \ D \to 3, \ldots ,\ Z \to 25.$$

Using the EAVS to convert the letters of the plaintext into the numbers modulo 26. The binary representations of these numbers are computed. Let K be a coloring star graph (CSG) that shown in Figure (3.1).

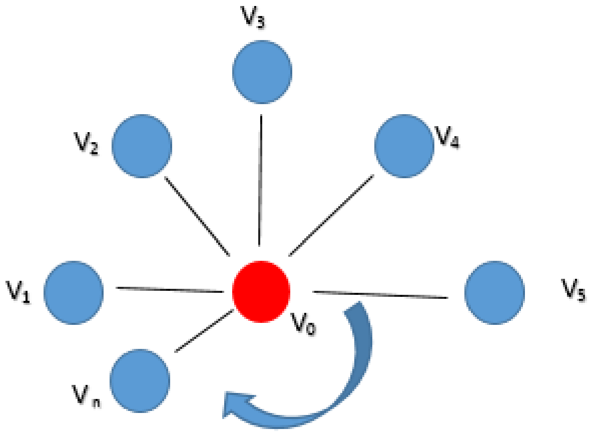

Figure 3.1.

Based on the K graph, first user can determine his / her secret key by

$$K \equiv n * \text{the color (mod26)},$$

K= {$K_i \equiv n*c_i$ (mod 26) | n = |v| , c_i is the number of letter

When n is the number of the vertices in CSG except the color of the center vertex. The decimal representations of the letters of the color are done using the EAVS. After that, these decimals are represented in binary strings. The ciphertext C of M is computed by

$$C \equiv (M + K)(\text{mod } 2).$$

C≡ {$C_i \equiv m_i$(mod 2) + k_i(mod2) | m_i ε M ,K_i ε K }

In more details,

$$c_i \equiv (m_i + k_i)\ \ (\text{mod } 2),\ \ for\ i = 1,2,3,\dots,n.$$

The string of the cipher text $C = (c_1, c_2, \dots, c_n\}$ is represented as the CSG that will be sent to second user as shown in Figure (3.2).

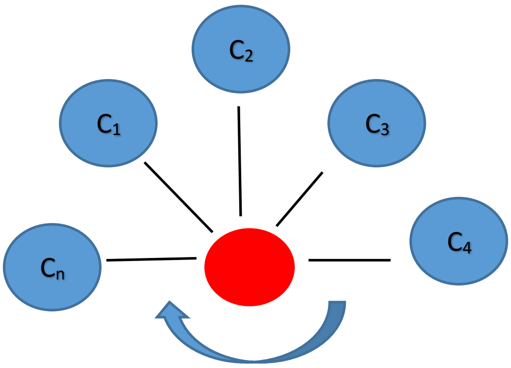

Figure 3.2.

Second (receiver) receives the cipher text as the CSG, he / she will do the following steps to recover the original plaintext. He / She depends on the CSG to determine the correct cipher text that is $\{c_1, c_2, c_3, \ldots, c_n\}$. He / She converts it into decimal representations using the EAVs. Second user computes the binary representations of these decimal numbers. Also, from the CSG, he / she determines his / her secret key, namely, since the color of vertices in CSG is (say red) and the number of the vertices is n, so the secret key is determined by

$$K \equiv n * \text{the color (say red) (mod 26).}$$

K= {k_i≡ n*c_i (mod 26) | n = |V|-1 , c_i is the number of letter }

The original plaintext is computed by

$$m_i \equiv (c_i - k_i) \pmod 2, for\ i = 1,2, \ldots, n.$$

Therefore, the original plaintext is

$$M \equiv \{m_1, m_2, m_3 \ldots\ldots, m_n\}$$

3.3 Study Case of the CSG for the SE Scheme

Let M be a plaintext, which is given by the word Ali. In other words,

$$M = \{m_1, m_2, m_3\} = \{A, l, i\}.$$

Based on the EAVS , the letters of m_1, m_2 and m_3 are converted into numbers as follows.

$$M = \{0, 11, 8\}.$$

The binary representations of the numbers 0, 11 and 8 are

$$0 \rightarrow 00000,$$

$$11 \rightarrow 01011,$$

$$8 \rightarrow 01000\,.$$

Now, suppose the K is a coloring star graph that is given by

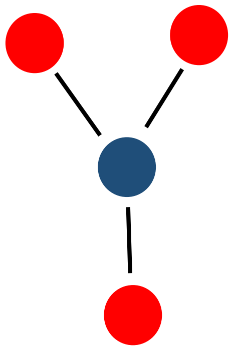

Figure 3.3.

Based on the K graph, first user can determine his / her secret key by

K= 3* red,

where 3 is the red color vertices and red is a color of the vertices except the center vertex of a coloring star graph (*CSG*).

Now, the decimal representations of the letters *r*, *e*, *d* in the red word are done based the EAVS.

Let

$$r \rightarrow 17, \qquad e \rightarrow 4 \quad \text{and } d \rightarrow 3$$

Thus

$$K \equiv 3 * \{ r , e, d \}(mod\ 26)$$

$$\equiv \{3 * 17 , 3 * 4 , \ 3 * 3 \} \ (mod\ 26)$$

$$\equiv \{25 , 12 , 9 \}.$$

The binary representations of the numbers 25 , 12 , 9 are

$$25 \rightarrow 11001 \quad = \ k_1,$$

$$12 \rightarrow 01100 \quad = \ k_2,$$

$$9 \rightarrow 01001 \quad = \ k_3.$$

The ciphertext *C* of *M* is computed by

$$C_i \equiv (M_i + K_i) \quad (mod 2), \; for\ i = 1,2,3.$$

In more details,

$$C_1 \equiv M_1 + K_1 \quad (mod\ 2)$$

$$\equiv 0000 + 11001 = 11001$$

$$C_2 \equiv M_2 + K_2 \quad (mod\ 2)$$

$$\equiv 01011 + 01100 = 00111$$

$$C_3 \equiv M_3 + K_3 \quad (mod\ 2)$$

$$\equiv 01000 + 01001 = 00001$$

So,

C = {11001, 00111, 00001}

= {25 , 7 , 1 }

Thus,

$C = ZHB.$

The *CSG* of *C* is formed by

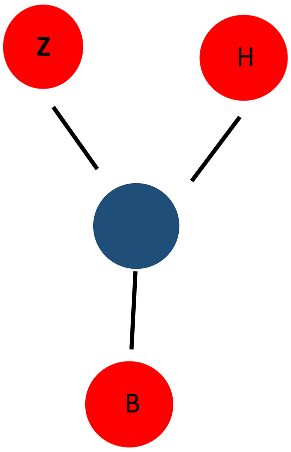

Figure 3.4.

First user sends the *CSG* to the receivers.

Second user (receiver) receives the cipher text *CSG*, he /she will do the following steps to recover the original plaintext.

He / She depends on the *CSG* to determine the covert cipher text that is *ZHB*.

He /She converts it into decimal representation based on by

$$Z \to 25, \quad H \to 7 \; and \; B \to 1.$$

He / She computes the binary representation of these numbers

$$Z \to 25 \to 11001, \quad H \to 7 \to 00011 \; and \; B \to 1 \to 00001.$$

Also, from the *CSG*, he /she determines his / her secret key. Since the color of vertices in *CSG* is red and the number of them is 3, so, the secret key is

$$Z \to 25 \to 11001, \quad H \to 7 \to 00011 \; and \; B \to 1 \to 00001$$

Since

$$r \to 17, \; e \to 4 \text{ and } d \to 3,$$

So,

$$K \;\; \equiv \; 3 * \{17, 4, 3\} \quad (mod\; 26).$$

$$\equiv \{25, 12, 9\},$$

In other words,

$$25 \to 11001, \quad 12 \to 01100 \; and \; 9 \to 01001.$$

The original plaintext is computed by

$$M \;\; \equiv (C + K) \;\; (mod\; 2).$$

$$M_1 \equiv 11001 + 11001 = 00000 \to 0 \to A,$$

$$M_2 \equiv 00111 + 01100 = 01011 \to 11 \to l,$$

$$M_3 \equiv 00001 + 01001 = 01000 \rightarrow 8 \rightarrow i$$

Therefore, the original plaintext is the word Ali.

3.4 Study Case of the CSG for the SE Scheme

Let M be a plaintext which is given be the sentence " Hi Ahmed " , namely

$$M = \{ m_1 , m_2 , m_3 , m_4 , m_5 , m_6 , m_7 \}$$

$$= \{ H , i , A , h , m , e , d \}$$

M_i , for i=1, 2 , 3 , …

Are converted into numbers as follows.

$$M= \{ 7 , 8 , 0 , 7 , 12 , 4 , 3 \}$$

The binary representations of the numbers

7 , 8 , ….. 3 are

$$7 \rightarrow 00111 = m_1$$

$$8 \rightarrow 01000 = m_2$$

$$0 \rightarrow 00000 = m_3$$

$$7 \rightarrow 00111 = m_4$$

$$12 \rightarrow 01100 = m_5$$

$$4 \rightarrow 001000 = m_6$$

$$3 \rightarrow 00011 = m_7$$

Now, suppose the K is a coloring star graph that

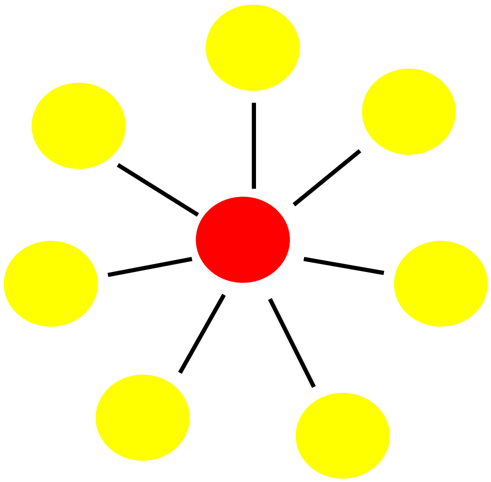

Figure 3.5.

Based on the K graph , first users can determine

His / her secret key by

K = 7 * yellow (mod 26) ,

Where 7 is the yellow color vertices and yellow

Is a color of the vertices except the center vertex of a coloring star graph (CSG)

Now, the decimal representation of the letters y , e , l , l , o , w in the yellow word are done based on the EAVs.

So,

$$Y \rightarrow 24 \quad , \quad e \rightarrow 4 \quad , \; l \rightarrow 11 \quad , \; l \rightarrow 11 \quad , \; 0 \rightarrow 14 \quad , \quad w \rightarrow 22.$$

Thus,

$$K \equiv 7 * \{ y , e , l , l \; , o \; , w \} \;\; (mod \; 26)$$

$$\equiv 7 * \{ 24 ,4 ,11 ,11 \; ,14 ,23 \} \; (mod \; 26)$$

$$\equiv \{ 12 ,2 , 25 \; , 25 , 20 , 24 \}$$

The binary representations of the numbers

12 , 2 , 25 , 25 , 20 , 24 are

$$12 \ \rightarrow 01100$$

$$2 \rightarrow 00010$$

$$25 \rightarrow 11001$$

$$25 \ \rightarrow 11001$$

$$20 \ \rightarrow 10100$$

$$24 \rightarrow 11000$$

The ciphertext C o f M is computed be

$c_i \equiv (m_l + k_l)\ (mod\ 2\ )$, for i = 1, 2 , …. 7 .

In more details

$$C \ \equiv (m_1 + k_1\ )(mod\ 2\ )$$

$$c_1 \equiv 00111 + 01100 = 01010 \rightarrow 11 \rightarrow l$$

$$c_2 \ \equiv 01000 + 00010 = 01010 \rightarrow 10 \ \rightarrow k$$

$$c_3 \equiv 00000 + 11001 = 11001 \rightarrow 25 \ \rightarrow z$$

$$c_4 \equiv 00111 + 11001 = 11110 \rightarrow 4 \ \rightarrow e$$

$$c_5 \equiv 01100 + 10100 = 11000 \rightarrow 24 \ \rightarrow y$$

$$c_6 \equiv 00100 + 11000 = 11100 \rightarrow 2 \ \rightarrow c$$

$$c_7 \equiv 00011 + 01100 = 01111 \rightarrow 15 \ \rightarrow p$$

So,

The ciphertext C is

$$C = l\ k\ zeycp$$

The CSG of C is formed by

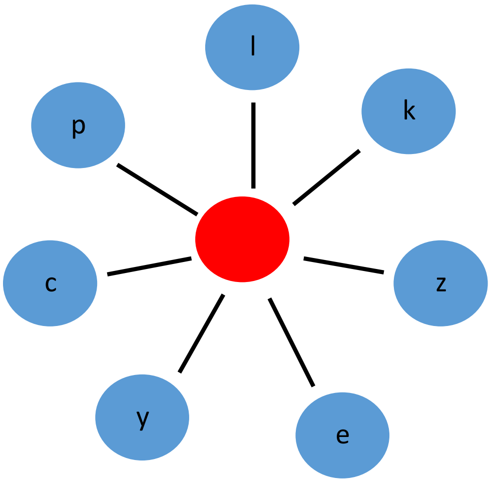

Figure 3.6

.

First user sends the CSG to the receiver .

Second user (receiver) receives the cipher tat as the CSG , he / she will do the following steps to recover the original plaintext .

He / she depend on the CSG to determine the correct cipher text that is l k Zeycp .

He / she converts it into decimal representations based on the EAVs by

$l \to 11\ .k \to 10\,.z\ \to 25\,.e\ \to 4\,.e\ \to 4\,.y\ \to 24$

$c \to 2\ .p \to 4\,.l\ \to 15$

He / she computes the binary representations of these numbers

$$l \to 11 \to 01011$$

$$k \to 10 \to 01010$$

$$z \to 25 \to 11001$$

$$e \to 4 \to 11110$$

$$y \to 24 \to 11000$$

$$c \to 2 \to 11100$$

$$p \to 15 \to 01111$$

Also, from the CSG , he / she determines his / her secret key .

Since the color of vertices in CSG is yellow and the number of them is 7.

So,

The secret key is

$$K \equiv 7 * \{ y . e . l . l . o . w \} \quad (mod\, 26)$$

$$K \equiv 7 * \{ 24 . 4 . 11 .11 . 14 . 22 \} \quad (mod\, 26)$$

$$K \equiv \{ 12 . 2 . 25 .25 . 20 . 24 \}$$

The binary representation of the numbers 12, 2, 25, 25, 20, 24 are

$$12 \to 01100$$

$$2 \to 00010$$

$$25 \to 11001$$

$$25 \to 11001$$

$$20 \to 10100$$

$$24 \to 11000$$

The original plaintext is computed by

$$M = C - K \ (\text{mod } 2)$$

$$m_1 \equiv 01011 - 01100 = 00111 \rightarrow 7 \rightarrow H$$

$$m_2 \equiv 01010 - 00010 = 01000 \rightarrow 8 \rightarrow i$$

$$m_3 \equiv 11001 - 11001 = 00000 \rightarrow 0 \rightarrow A$$

$$m_4 \equiv 11110 - 11001 = 00111 \rightarrow 7 \rightarrow H$$

$$m_5 \equiv 11000 - 10100 = 01100 \rightarrow 12 \rightarrow m$$

$$m_6 \equiv 11100 - 11000 = 00100 \rightarrow 4 \rightarrow e$$

$$m_7 \equiv 01111 - 01100 = 00011 \rightarrow 3 \rightarrow d$$

So,

The original plaintext is

M = Hi Ahmed.

Applications of Graph Coloring

► Map Coloring

► Making timetable

►Mobile Radio Frequency Assignment

► Data mining

►Image segmentation

► Networking

► Resource allocation

Conclusions and future works

The conclusions and future work of this work can be discussed as follows. The proposed CSG-SE scheme is more secure in compare with the previous SE schemes, since the shared secret key is generated using the coloring star graph to form a sequence as compare as with previous SE schemes those using the numbers modulo 26. Also, the ciphertext with proposed CSG-SE scheme is computed and sent as CSG, while in previous SE schemes, the ciphertext is computed as number modulo 26.

References

1. V. Ustimenko. Cryptim: Graphs as tools for symmetric encryption. In International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, pages 278–286. Springer, (2001).

2. G. Samid. Denial cryptography based on graph theory, Nov. 23. US Patent 6,823,068 ,(2004)

3. H. Edwards. A normal form for elliptic curves. Bulletin of the American mathematical society, 44(3):393–422,(2007).

4. L. Mittenthal. Sequencings and directed graphs with applications to cryptography. In Sequences, Subsequences, and Consequences, pages 70–81. Springer, (2008).

5. R. Selvakumar and N. Gupta. Fundamental circuits and cut-sets used in cryptography. Journal of Discrete Mathematical Sciences and Cryptography, 15(4-5):287–301,(2012).

6. H. O. Abdullah and M. Eftekhari. Cryptanalysis and improvements on some graph-based authentication schemes. Journal of Discrete Mathematical Sciences and Cryptography, 16(4-5):297–306 (2013).

7. W. M. Al Etaiwi. Encryption algorithm using graph theory. Journal of Scientific Research and Reports, pages 2519–2527, (2014).

8. P. Femina and D. A. David. A study of data encryption standard using graph theory. In 2nd International Conference on Science, Technology and Management, University of Delhi, New Delhi, India,(2015).

9. M. A. Ahmed and J. B. Babujee. Encryption through labeled graphs using strong face bimagic labeling. In International Mathematical Forum, volume 12, pages 151–158, (2017).

10. A. Krishnaa. Inner magic and inner antimagic graphs in cryptography. Journal of Discrete Mathematical Sciences and Cryptography, 22(6):1057–1066,(2019).

11. R. K. K. Ajeena. The graphs for elliptic curve cryptography. In Applied Mathematics. IntechOpen, (2019).

12. R. Kuppan, L. Shobana, and I. N. Cangul. Encrypting and decrypting algorithms using strong face graph of a tree. International Journal of Computer Mathematics: Computer Systems Theory, 5(4):225–233,(2020).

13. S.Muthammai, S., & Dhanalakshmi, S. Edge domination in Boolean function graph B (L (G), NINC) of a graph. *Journal of Discrete Mathematical Sciences and Cryptography*, *22*(5), 847-855.(2020).

14. Z .Shao, S. Kosari, R.Anoos, S. M. Sheikholeslami, & J. A. Dayap , Outer-convex dominating set in the corona of graphs as encryption key generator. Complexity, (2020).

الملخص

في هذا العمل ، تم اقتراح مخطط بديل للتشفير المتماثل (DS) بناءً على صيغة جديدة للمفتاح السري المشترك. يتم إنشاء هذا المفتاح باستخدام الرسم البياني الملون على شكل نجمة (CSG) هذا النص المشفر للنص العادي ، أي كلمة إنجليزية أو جملة إنجليزية ، يتم حسابه وإرساله في القناة باسم (CSG) يواجه المهاجمون هنا مع مخطط SE المقترح صعوبة في استعادة المفتاح السري. لذلك ، يعتمد أمان مخطط CSG-SE المقترح على كيفية إنشاء المفتاح السري. وبالتالي ، يعتبر مخطط CSG-SE مخطط SE أكثر أمانًا مقارنةً بالمخططات السابقة للاتصال.

جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة بابل -كلية التربية للعلوم الصرفة

قسم الرياضيات

تشفير النصوص باستخدام البيان النجمي الملون

بحث مقدم الى

قسم الرياضيات -كلية التربية للعلوم الصرفة - جامعة بابل

وهو جزء من متطلبات نيل شهادة الدبلوم العالي تربية / رياضيات

من قبل

اثير جواد كاظم عمران

بأشراف

ا.م.د. رومى كريم خضرعجينة

١٤٤٤ 2022