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

Tree Graphs 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

Rhan Muhi Hashim AL- Husseini

Supervised by

Asst. Prof. Dr. Ruma Kareem K. Ajeena

2022 **1444**

بسم الله الرحمن الرحيم

وَيَسْـَٔلُونَكَ عَنِ الرُّوحِ ۖ قُلِ الرُّوحُ مِنْ أَمْرِ رَبِّي وَمَا أُوتِيتُمْ مِ

نَ الْعِلْمِ إِلَّا قَلِيلً (85)

صدق الله العظيم

سورة الاسراء

Supervisor Certificate

I certify that this research entitled " **Tree Graphs for Encryption Schemes**" for the student **Rhan Muhi Hashim AL- Husseini** , 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 "**Tree Graphs for Encryption Schemes"** 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 **“Tree Graphs for Encryption Schemes”** 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 " **Tree Graphs for Encryption Schemes”"** as examining committee examined the student **Rhan Muhi Hashim AL-Husseini** 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

Title:
Date:

Chairman
Signature:
Name:
Title:
Date:

Member / Supervisor
Signature:
Name: Dr. Ruma Kareem K. Ajeena
Title: Asst. Prof.
Date:

Member
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:

Member
Signature:
Name:

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 my work to

Holy crowd

Which emerged from the Muhammadiyah message to the call of the supreme reference, Sayyid Ali al-Sistani, with the fatwa of the sufficient jihad, which saved Iraq and the world from the schemes of the black gangs of ISIS and exposed its criminal nature.

Abstract.

In this work, new versions of the symmetric encryption (SE) schemes are proposed using the binary tree graph (BTG). The shared secret key is computed. using the Diffie- Hellman key exchange. This ciphertext of the plaintext, that is an English word or English sentence, is computed and sent in the channel as the BTG. The attackers here with the proposed SE scheme facing the difficulty to recover the original plaintext. So, the security of the proposed BTG-SE scheme depending on how to generate the secret key. Thus, the BTG-SE scheme considers as more secure SE scheme in compare with previous ones for communication.

List of Contents

Chapter One

Introduction

Chapter One
INTRODUCTION

1.1 Introduction

Cryptography is science to design and analysis the mathematical techniques that enable secure communications in the presence of malicious adversaries. 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 [11, 63]. Some researchers proposed cryptographic algorithms using paths in any graph [54] and others proposed encryption algorithms using directed graphs [43].

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.

In 2004, Samid, 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, 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, [56], 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, 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, introduced an encryption scheme through the labeled graphs using the strong face bimagic labeling.

In 2019, Ajeena, 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 binary tree graph (BTG). The shared secret key is generated using the Diffie- Hellman key exchange. The plaintext is divided into two blocks, encrypted and sending to receiver as the BTG to increase the level of security for these schemes.

1.4 The Structure of this Research

This research consists of four chapters:

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

Chapter 2. Mathematical Background on Graph theory and Cryptography

Chapter 3. The Symmetric Encryption Scheme Based on BTG.

Chapter 4. Conclusions and future works.

Chapter Two

Mathematical Background on Graph theory and Cryptography

Chapter Two
Mathematical Background to Graph Theory and Cryptography

2.1 Introduction

In this chapter, some concepts of graph theory are presented and discussed through the definitions and examples in the first part. Whereas, the introduction to cryptography and some symmetric encryption schemes are explained in the second part.

2.2 Basic Concepts of Graph Theory

In this section, some important concepts of the graph theory are discussed as follows.

Definition 2.2.1. (Graph) . 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 $(u,v) \in V(G)$.

Definition 2.2.2. (Adjacent). 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*). 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). 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). 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). A graph is simple if it has no parallel edges or loops.

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

Example 2.2.3. A multi graph as shown in Figure (2.3).

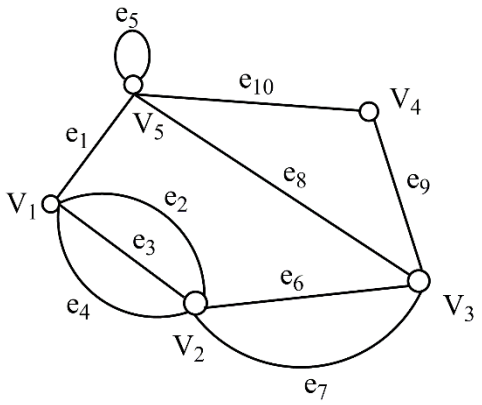


Figure 2.3. A multi graph.

Definition 2.2.8. (Null graph) [38]. 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 (2.4).

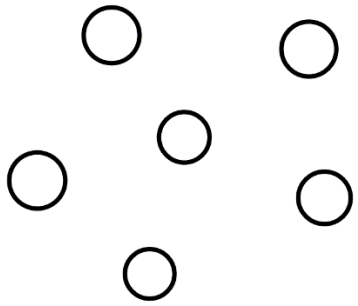


Figure 2.4. A null graph.

Definition 2.2.9. (Complete Graph). 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 (2.5).

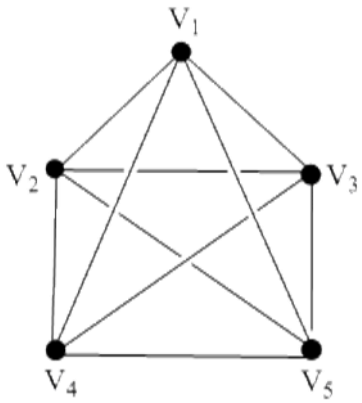


Figure 2.5. A complete graph K_5.

Definition 2.2.10. (**Bipartite Graph)**. 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 (2.6)

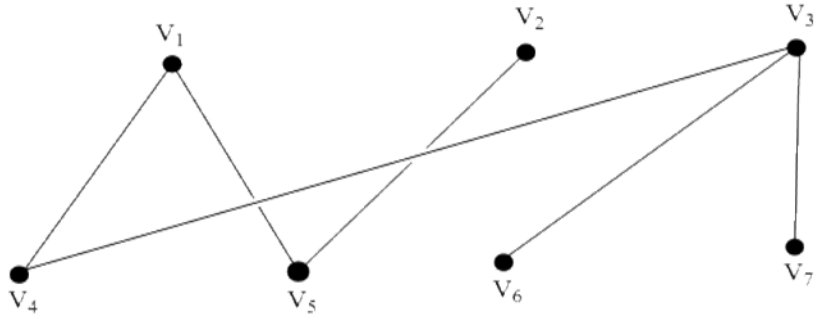


Figure 2.6. A bipartite graph.

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) [38]. 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 (2.7).

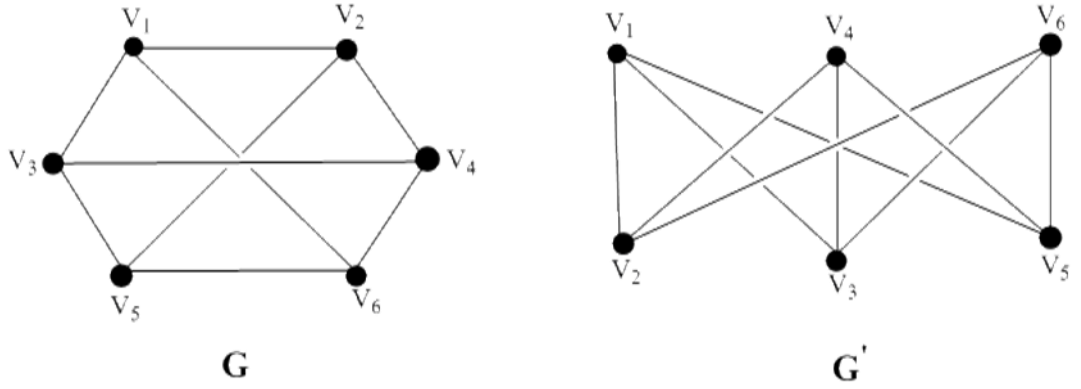


Figure 2.7. A complete bipartite graph.

Definition 2.2.12. (Regular Graph). 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 (2.8).

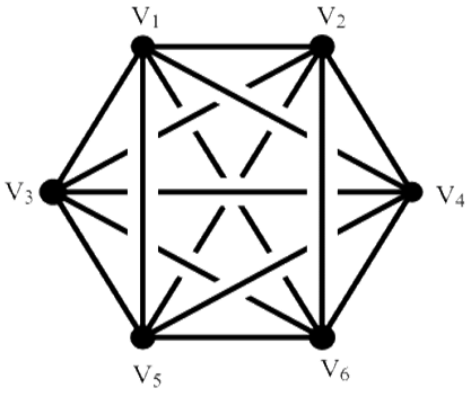


Figure 2.8. A regular graph.

Definition 2.2.13. (Path Graph). 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 $1 \leq i \leq p-1$, 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). 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.

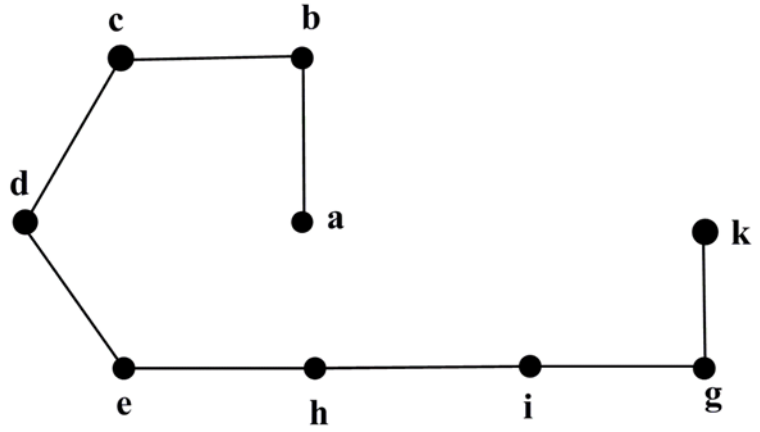


Figure 2.9. A path graph.

Definition 2.2.15. (Walk Graph). 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). 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.

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

Example 2.2.9. A walk and trial graph

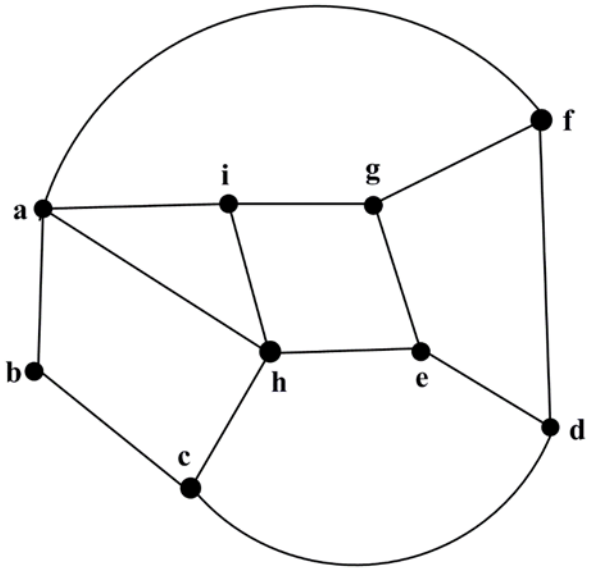


Figure 2.10. A walk graph.

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

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

W_1 is a walk and trial

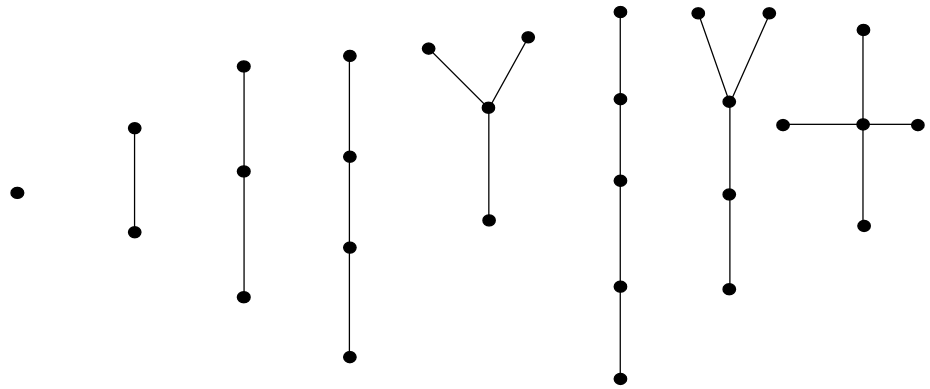
W_2 is walk but not trial.

2.2.1 Trees

One of the important classes of graphs is the trees. The importance of trees is evident fromtheir applications in various areas, especially theoretical computer science and molecular evolution.

Definition 2.2.1.1. A graph having no cycles is said to be acyclic. A forest is an acyclic graph.

Definition: A *tree* is a connected graph without any cycles, or a tree is a connected acyclic graph. The edges of a tree are called *branches*. It follows immediately from the definition that a tree has to be a simple graph (because self-loops and parallel edges both form cycles). Figure 4.1(a) displays all trees with fewer than six vertices.



(a)

Figure. 4.1(a).

The following result characterizes trees.

Theorem 2.2.1.1. A graph is a tree if and only if there is exactly one path between every pair of its vertices.

The next two results give alternative methods for defining trees.

Theorem 2.2.1.2. A tree with n vertices has $n-1$ edges.

Proof We prove the result by using induction on n, the number of vertices. The result is obviously true for $n = 1$, 2 and 3. Let the result be true for all trees with fewer than n vertices.

Let T be a tree with n vertices and let e be an edge with end vertices u and v. So the only path between u and v is e. Therefore deletion of e from T disconnects T. Now, $T - e$ consists of exactly two components T_1 and T_2 say, and as there were no cycles to begin with, each component is a tree. Let n_1 and n_2 be the number of vertices in T_1 and T_2 respectively, so that $n_1 + n_2 = n$. Also, $n_1 < n$ and $n_2 < n$. Thus, by induction hypothesis, number of edges in T_1 and T_2 are respectively $n_1 - 1$ and $n_2 - 1$. Hence the number of edges in $T = n_1 - 1 + n_2 - 1 + 1 = n_1 + n_2 - 1 = n - 1$.

Theorem 2.2.1.2. Any connected graph with n vertices and $n - 1$ edges is a tree.

Proof. Let G be a connected graph with n vertices and $n - 1$ edges. We show that G contains no cycles. Assume to the contrary that G contains cycles. Remove an edge from a cycle so that the resulting graph is again connected. Continue this process of removing one edge from one cycle at a time till the resulting graph H is a tree. As H has n vertices, so number of edges in H is $n - 1$. Now, the number of edges in G is greater than the number of edges in H. So $n - 1 > n - 1$, which is not possible. Hence, G has no cycles and therefore is a tree.

2.2.2 Rooted and Binary Trees

A tree in which one vertex (called the *root*) is distinguished from all the others is called a rooted tree.

Definition 2.2.2.1. A binary tree is defined as a tree in which there is exactly one vertex of degree two and each of the remaining vertices is of degree one or three.

Obviously, a binary tree has three or more vertices. Since the vertex of degree two is distinct from all other vertices, it serves as a root, and so every binary tree is a rooted tree.

Below are given some properties of binary trees.

Theorem 2.2.2.1. Every binary tree has an odd number of vertices.

Proof Apart from the root, every vertex in a binary tree is of odd degree. We know that there are even number of such odd vertices. Therefore when the root (which is of even degree) is added to this number, the total number of vertices is odd.

Corollary 2.2.2.2. There are $(n+1)$ pendant vertices in any binary tree with n vertices.

Proof Let T be a binary tree with n vertices. Let q be the number of pendant vertices in T. Therefore there are $n-q$ internal vertices in T and so $n-q-1$ vertices of degree 3. Thus the number of edges in $T = {}^{1}[3(n-q-1)+2+q]$. But the number of edges in T is $n-1$.

2.3 Introduction to Cryptography

Some basic concepts related to cryptography are discussed as follows.

2.3.1 Basic Concepts

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

Definition 2.3.1.1. [1] Cryptography is the design and analysis of mathematical techniques that enable secure communications in the presence of adversaries.

Definition 2.3.1.2. [1] Cryptosystem. A cryptographic system is specifically a set of methods (algorithms) for computing (implementing) the encryption and decryption.

Definition 2.3.1.3. [1] Cryptanalysis is the study of analyzing cryptosystem in order to study the hidden aspects of the systems.

Definition 2.3.1.4. [40] Plaintext. The information which we want to protect from other people (attackers).

Definition 2.3.1.5. [40] Security. It means that the difficulty to know the information which transferred over the channel easily.

2.3.2 Basic Communications Model

[1] 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.**

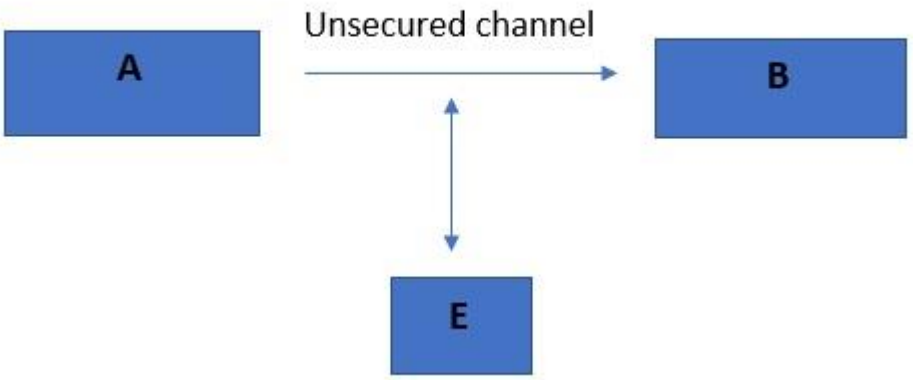


Figure 2.11. Basic communications model.

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

2.3.3. Some Important Kinds of Cryptosystems

2.3.3.1 Symmetric-Key Cryptosystems.

[1] 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.

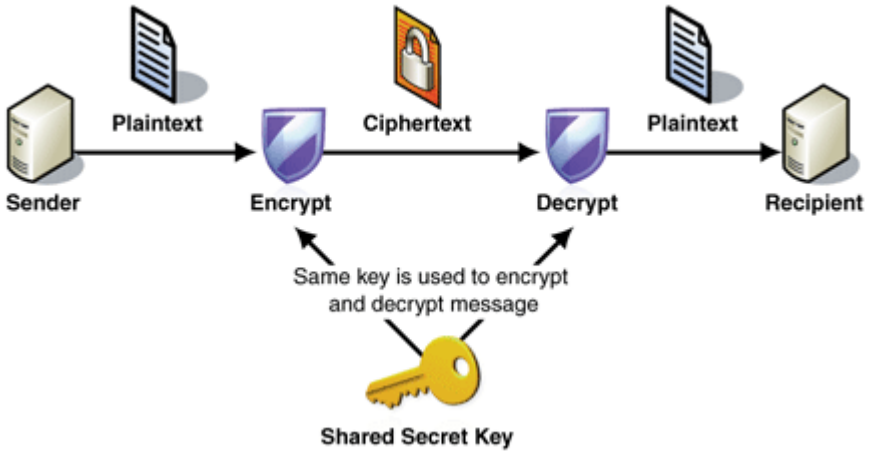


Figure 2.12. Symmetric-Key Cryptosystems.

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

[1] 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.

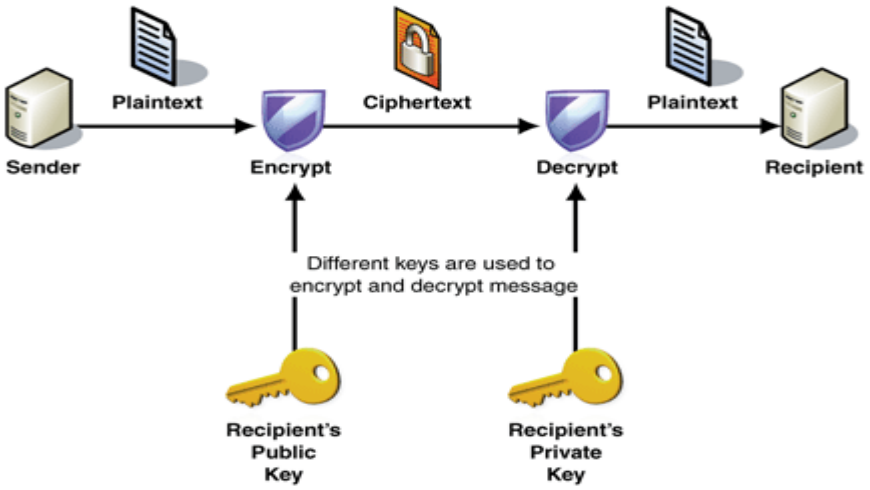


Figure 2.13 Asymmetric-Key Cryptosystems (Public-Key cryptosystems).

Chapter Three

Binary Tree Graph for Encryption Scheme

Chapter Three

A symmetric Encryption Schemes Based on the Binary Tree Graph

3.1 Introduction

The chapter presents new versions of symmetric encryption (SE) schemes which are used the binary tree graph (BTG) to compute the ciphertext of a plaintext that is represented by an English word or sentence. These versions are discussed as follows.

3.2 The SE Scheme Based on BTG Using the EAVs

Suppose M is plaintext that can be given in an English word or sentence is chosen by first user. In other words,

$M = \{m_1, m_2, \ldots, m_n\} = \{m_i\}_{i=1,2,\ldots,n}$, with length n. The message *m* is divided in to blocks m_1 and m_2 if $m_1 = (m_{11}, m_{12}, \ldots, m_{1l})$ then $m_2 = (m_{21}, \ldots, m_{2n})$. The English alphabetic values (EAV_S) is given n Table (3.1).

Table 3.1. English alphabet Table.

A	B	C	D	E	F	G	H	I	G	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		

Using the EAVs to convert the letters of the plaintext into the numbers modulo 26. He/ She also uses his/her shared secret key *k* to compute the ciphertext $C = (C_1,C_2)$ through the following relation

$$C_1 \equiv m_{1i} + k \ (mod\ 26) \equiv c_{1i} \text{ and } C_2 \equiv m_{2j} + k \ (mod\ 26) \equiv c_{2j}, \text{ for } i=1,2,\ldots,l \text{ and } j=1,2,\ldots,n.$$

These numbers, namely c_{1i} and c_{2j} are represented into English letters using the EAVs in Table (3.1). The ciphertext $C = (C_1,C_2)$ is represented by binary tree graph (BTG) and send to second user.

After second user receives the BTG, he /she do the following steps to recover the original message *m*. Based on the branches of BTG, he /she converts these letters into numbers as given in Table (3.1). He/She uses his/her shared secret key *k* to recover the message through the following relation

$$m_1 \equiv c_{1i} + k \ (mod\ 26) \equiv m_1 \text{ and } m_2 \equiv c_{2j} + k \ (mod\ 26) \equiv m_{2j}, \text{ for } i=1,2,\ldots,l \text{ and } j=1,2,\ldots,n.$$

So, the original message $m=(m_1,m_2)$.

3.3 Study Case 1 of the SE Scheme Based on BTG Using the EAVs

Suppose *m* is award "Cryptography". The massage *m* is divided in to blocks m_1 and m_2 if $m_1 = (m_{11}, m_{12}, m_{13}, m_{14}, m_{15})$ = (c, r, y, p, t) then $m_2 = (m_{21}, m_{22}, m_{23}, m_{24}, m_{25}, m_{26}, m_{27})$=(o, g, r, a, p, h, y). First user converts these letters in to numbers using the EAVs. So,

$$m_1 = (c,r,y,p,t) = (2,17,24,15,19)$$

and

$$m_2 = (o,g,r,a,p,h,y) = (14,6,17,0,15,7,24).$$

He/ She also uses his/her shared secret key $k = 4$ to compute the ciphertext $C = (C_1, C_2)$ through the following computations:

$$C_1 \equiv m_1 \pmod{26} \text{ and } C_2 \equiv m_2 \pmod{26}$$

$$2+4=6,\ 17+4=21,\ 24+4=28 \pmod{26} \equiv 2,\ 15+4=19,\ 19+4=23$$

and

$$14+4=16,\ 6+4=10,\ 17+4=22,\ 0+4=4,\ 15+4=19,\ 7+4=12,$$
$$24+4=28 \pmod{26} \equiv 2.$$

These numbers are represented into English letters using the EAVs:

$6 \rightarrow$ g, $21 \rightarrow$ v, $2 \rightarrow$ c, $19 \rightarrow$ t , $23 \rightarrow$ x, $18 \rightarrow$ s, $10 \rightarrow$ k, $21 \rightarrow$ v ,

$4 \rightarrow$e, $19 \rightarrow$ t , $11 \rightarrow$ l and $2 \rightarrow$ c

So, the ciphertext C of m is given by C_1= (gvctx) and C_2=(skvetlc). The ciphertext $C = (C_1, C_2)$ is represented by binary tree graph (BTG) as shown in Figure (3.1) and send to receiver.

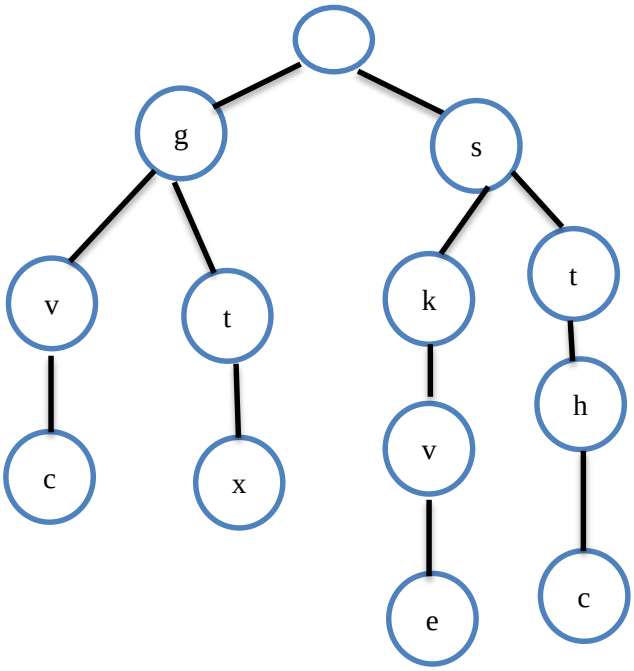


Figure 3.1.The ciphertext C_1=gvctx and C_2= skvetlc of *m* = cryptography.

After second user receives the BTG, he /she do the following steps to recover the original message *m*. Based on the branches of BTG, he /she converts these letters into numbers as follows:

C_1: g→6, v→ 10 , c→2,t→19, x→ 23 and

C_2: s→ 18, k→10, v→21, E→4 , t→14

l→11, c→2.

She/he uses his/her shared secret key $k = 4$ to recover the message through the following computations:

6-4=2→c ,21-4=17→ r, 2-4=-2(mod26)=24→y,

19-4=15→p. 23-4=19→t

m_1=crypt

Also, 18-4=14→o, 10-4=6→g , 21-4=17→ r,

4-4=0→ a, 19-4=15→ p , 11-4=7→ h,

2-4=-2(mod26)=24→y

m_2=ography

So, the original message $m=(m_1,m_2)$=cryptography.

3.4 Study Case2 of the SE Scheme Based on BTG Using the EAVs

Suppose m is award "Study law". the massage m is divided in to blocks m_1 and m_2 if $m_1=(m_{11},m_{12},m_{13},m_{14},m_{15})$=(s, t, u, d, y) and $m_2=(m_{21},m_{22},m_{23})$ = (l,a,w). First user converts these letters in to numbers using the EAVs. So,

$$m_1=(s,t,u,d,y)=(18,19,20,3,24)$$

and

$$m_2=(l,a,w)=(11,0,22)$$

He/She also user his/her shard secret key k=2 to compute the cipher text C=(C_1,C_2)through the following computations :

$$C_1 \equiv m_1 \pmod{26} \text{ and } C_2 \equiv m_2 \pmod{26}$$

18+2=20, 19+2=21, 20+2=22, 3+2=5, 24+2=26 (mod26)=0

and

11+2=13, 0+2=2, 22+2=24.

These numbers are represented into English letters using the EAVs:

20→ u ,21→v ,2 2→w, 5→f , 0→a, 13→n, 2→ c, and 24→ y

So, the ciphertexd C of m is given by C_1=(uvwfa)and C_2=(ncy)

the ciphartext C=(C_1,C_2)is represented by binary tree graph as shown in figure (3,1) and send to receiver.

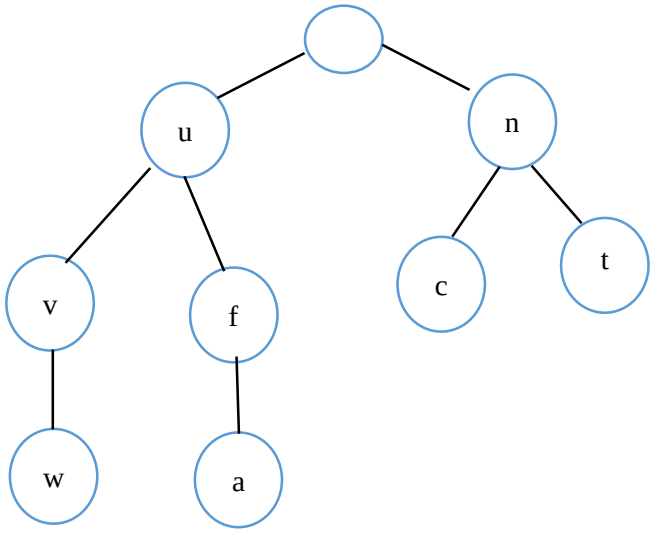


Figure 3.2 the cipher text C_1=uvwfa and C_2=ncy of m= study law.

After second user receives the BTG ,he /she do the following step to recover the original massage m.

Based on the branches of BTG ,he /she determines two lists of C_1 and C_2 by C_1=uvwfa and C_2=ncy using the EAVS he/she converts these letters in to numbers as follows:

C_1: u→20, v→21 , w→22, f→5, a→ 0 and

C_2: n→13, c→2, y→23.

He /she user his/her shored secret key k=2 to recover the massage through the following computation

20-2=18→s, 21-2=19→c, 22-2=20→u,

5-2=3→d, 26-2=24→y.

m_1=study

Also, 13-2=11→ l, 2-2=0→a , 24-2=22→w.

m_2=law

So the original message m=(m_1,m_2)=studylaw

3.5 The SE Scheme Based on BTG Using the ASCII Values

Suppose M is plaintext that can be given in an English word or sentence is chosen by first user. In other words,

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

The message m is divided in to blocks m_1 and m_2 if $m_1 = (m_{11}, m_{12}, \ldots, m_{1l})$ then $m_2 = (m_{21}, \ldots, m_{2n})$. The American Standard Code for Information Interchange (ASCII) is given n Table (3.2).

Using the ASCII to convert the letters of the plaintext into the numbers modulo 26. He/ She also uses his/her shared secret key k to compute the ciphertext C = (C_1,C_2) through the following relation

Table 3.2 ASCII Values 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

$$C_1 \equiv m_{1i} + k \ (mod\ 127) \equiv c_{1i} \text{ and } C_2 \equiv m_{2j} + k \ (mod\ 127\ ) \equiv c_{2j}, \text{ for } i=1,2,\ldots,l \text{ and } j=1,2,\ldots,n.$$

These numbers, namely c_{1i} and c_{2j} are represented into English letters using the ASCII values in Table (3.2). The ciphertext $C = (C_1, C_2)$ is represented by binary tree graph (BTG) and send to second user.

After second user receives the BTG, he /she do the following steps to recover the original message *m*. Based on the branches of BTG, he /she converts these letters into numbers as given in Table (3.2). He/She uses his/her shared secret key *k* to recover the message through the following relation

$$m_1 \equiv c_{1i} + k \ (mod\ 127) \equiv m_1 \text{ and } m_2 \equiv c_{2j} + k \ (mod\ 127\ ) \equiv m_{2j}, \text{ for } i=1,2,\ldots,l \text{ and } j=1,2,\ldots,n.$$

So, the original message $m=(m_1,m_2)$.

3.6 Study Case 1 of the SE Scheme Based on BTG Using the EAVs

Suppose *m* is award "Cryptography". The message *m* is divided in to blocks m_1 and m_2 if $m_1 = (m_{11}, m_{12}, m_{13}, m_{14}, m_{15})$ = (c, r, y, p, t) then $m_2 = (m_{21}, m_{22}, m_{23}, m_{24}, m_{25}, m_{26}, m_{27})$=(o, g, r, a, p, h, y). First user converts these letters in to numbers using the ASCII values. So,

$$m_1 = (c,r,y,p,t) = (67,114,121,112,116)$$

and

$$m_2 = (o,g,r,a,p,h,y) = (111,103,114,97,112,104,121).$$

He/ She also uses his/her shared secret key $k = 4$ to compute the ciphertext

$C = (C_1, C_2)$ through the following computations:

67+4=71, 114+4=118, 121+4=125, 112+4=116, 116+4=120

and

111+4=115, 103+4=107, 114+4=118, 97+4=101, 112+4=116,
104+4=108, 121+4=125 .

These numbers are represented into English letters using the ASCII values:

71 → g, 118→ v, 125 → }, 116 → t , 120 → x, 115 → s, 107 → k, 118→ v, 101→e, 116→ t , 108→ l and 125→ }

So, the ciphertext C of m is given by C_1= (gv}tx) and C_2=(skvetl}). The ciphertext $C = (C_1, C_2)$ is represented by binary tree graph (BTG) as shown in Figure (3.3) and send to receiver.

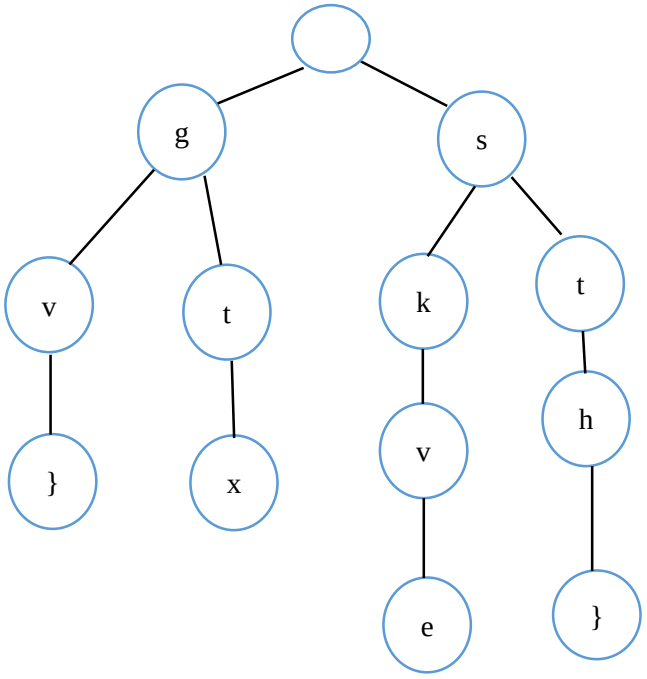


Figure 3.3. the ciphertext C_1=gv}tx and C_2= skvetl} of *m* = cryptography.

After second user receives the BTG, he /she do the following steps to recover the original message *m*. Based on the branches of BTG, he /she

converts these letters into numbers as follows:

C_1: g→71, v→ 118 , }→125,t→116, x→ 120 and

C_2: s→ 115, k→107, v→118, e→101 , t→116, l→106, }→125.

He/She uses his/her shared secret key $k = 4$ to recover the message through the following computations:

71-4=67→c ,118-4=114→ r, 125-4=121→y,

116-4=112→p. 116-4=112→t

m_1=crypt

Also, 115-4=111→o, 107-4=103→g, 118-4=114→ r,

101-4=97→ a, 116-4=112→ p, 108-4=104→ h,

125-4=121→y

m_2=ography

So, the original message m=(m_1,m_2)=cryptography.

Example 1

Suppose *m* is award "ali is clever". The massage *m* is divided in to blocks m_1 and m_2 if $m_1 = (m_{11}, m_{12}, m_{13}, m_{14}, m_{15}) = (A, l, i, i, s)$ then $m_2 = (m_{21}, m_{22}, m_{23}, m_{24}, m_{25}, m_{26}) = (c, l, e, v, e, r)$. First user converts these letters in to numbers using the ASCII. So,

m_1 = (A, l, i, i, s) = (65 ,108 ,105,32,105,115)

and

m_2 = (c, l, e, v, e, r) = (99,108,101 ,118,101,114).

He/ She also uses his/her shared secret key $k = 3$ to compute the ciphertext C = (C_1,C_2) through the following computations:

65 +3=68, 108 +3=111, 105+3=108,32+3=25, 105+3=108, 115+3=118

and

99+3=102, 108+3=111, 101 +3=104, 118+3=121, 101+3=104,
114+3=117 .

These numbers are represented into English letters using the ASCII:

68 → D, 111→ o, 108 → l, 35 → # , 108 → l, 118 → v, 102 → f, 111→ o, 104→h, 121→ y , 104→ h and 117→u }

So, the ciphertexd C of m is given by C_1= (Dol#lv) and C_2=(fohyhu). The ciphartext C = (C_1,C_2) is represented by binary tree graph (BTG) as shown in Figure (3.4) and send to receiver.

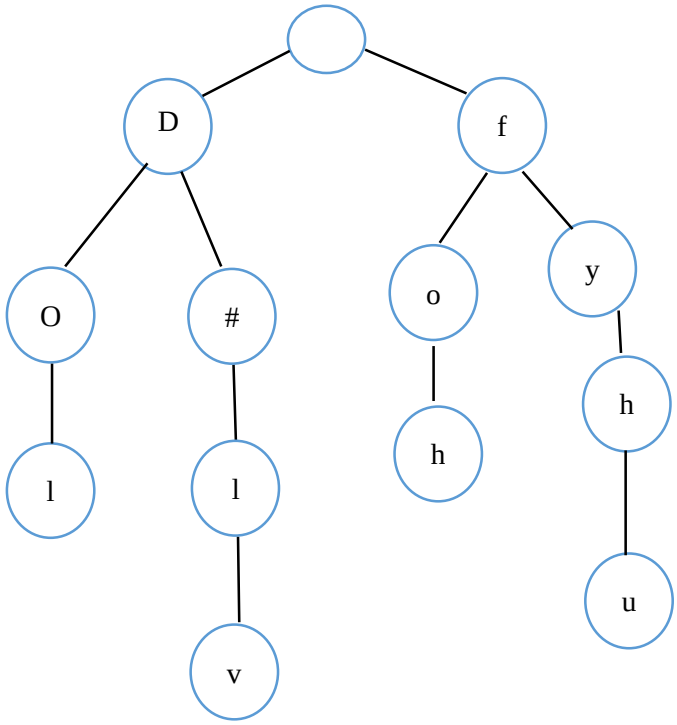


Figure 3.4 the ciphertext C_1= Dol#lv and C_2= fohyhu of *m* = Ali is clever.

After second user receives the BTG, he /she do the following steps to recover the original message *m*. Based on the branches of BTG, he /she converts these letters into numbers as follows:

C_1: D→68, o→ 111 , l→108,#→35, l→ 108,v →118 and

C_2: f→ 102, o→111, h→104, y→121 , h→104, u→117.

He/She uses his/her shared secret key $k = 3$ to recover the message through the following computations:

68-3=65 →A ,111-3=108 → l, 108-3=105→i,

35-3=32→space. 108-3=105→I , 118-3=1115 → s

m_1=Ali is

Also, 102-3=99→c, 111-3=108→l, 104-3=101 → e,

121-3=118→ v, 104-3=101→ e, 117-3=114→ r,

m_2=clever

So, the original message m=(m_1,m_2)=Ali is clever.

Conclusions and Future Works

The conclusions and future work of this work can be discussed as follows. The proposed BTG-SE scheme is more secure in compare with the previous SE schemes, since the ciphertext with proposed BTG-SE scheme is divided into two blocks and computed and sent as BTG, while in previous SE schemes, the ciphertext is computed as number modulo 26 or 127.

For future works, it is possible to use BTG with other kinds of the SE schemes.

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

في هذا العمل ، تم اقتراح إصدارات جديدة من مخططات التشفير المتماثل (SE) باستخدام الرسم البياني الشجري الثنائي (BTG). يتم حساب المفتاح السري المشترك. باستخدام تبادل مفاتيح Diffie- Hellman. هذا النص المشفر للنص العادي ، أي كلمة إنجليزية أو جملة إنجليزية ، يتم حسابه وإرساله في القناة باسم BTG. يواجه المهاجمون هنا مع مخطط SE المقترح صعوبة في استعادة النص العادي الأصلي. لذلك ، يعتمد أمان مخطط BTG-SE المقترح على كيفية إنشاء المفتاح السري. وبالتالي ، يعتبر مخطط BTG-SE مخطط SE أكثر أمانًا مقارنةً بالمخططات السابقة للاتصالات.

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

الرسوم البيانية التشجيرية لأنظمة التشفير

بحث مقدم الى

قسم الرياضيات -كلية التربية للعلوم الصرفة -جامعة بابل

و هو جزء من متطلبات نسل شهادة الدبلوم العالي تربية / رياضيات

من قبل
رهان محي هاشم

بأشراف

ا.م.د. رومى كريم خضرعجينة

1444 2022