Malaya Journal of Matematik, Vol. 9, No. 1, 470-473, 2021

https://doi.org/10.26637/MJM0901/0079

A new cryptographic method irrespective of code order using graph theory

Binoy Joseph[1]* and Bindhu K Thomas[2]

Abstract

Graph Theory plays an important role in various fields. Since Graph theory has an easy representation in computers as a matrix it is widely used as a tool for cryptographic techniques. In this paper we propose a new cryptographic technique irrespective of code order for encrypting and decrypting data securely with the benefits of newly defined graph G_β and a matrix using binary string of ASCII values of the given message.

Keywords

Cryptography, Simple Graph, Adjacency Matrix .

AMS Subject Classification

03B80, 05C22, 05C62, 05C99, 68P30, 68R10, 68R99.

[1,2]*Mathematics Research Center, Mary Matha Arts and Science College, Mananthavady-670645, affiliated to Kannur University, Kerala, India.*

***Corresponding author**: [1] binoy.sib@gmail.com; [2]bindhukthomas@gmail.com

Article History: Received **11** November **2020**; Accepted **23** January **2021**

Contents

1. Introduction

Cryptography is the art of protect information by transforming it to unreadable format called Cipher text. The process of converting plain text to cipher text called encryption, and the process of converting cipher text on its original plain text called decryption [1].

In this paper, we define a new edge weighted undirected graph denoted by G_β from an $8-$bit representation of ASCII values $(0-127)$ corresponding to the alphabets of given message

A graph in which each edge connects two different vertices and where no two edges connect the same pair of vertices is called a simple graph. Let $G=(V,E)$ be a simple graph with $V=v_1,v_2,...,v_n$,$E=e_1,e_2,...,e_m$ and the adjacency matrix of G is an $n\times n$ symmetric binary matrix $X=[x_{ij}]$ defined over the ring of integers such that

$$x_{ij}=\begin{cases}1 & ;\text{if } v_iv_j\varepsilon E\\ 0 & ;\text{Otherwise}\end{cases}$$

It is used to represent whether a pair of vertices in a given graph are connected or not. An adjacency matrix is used to represent a finite graph.[2]

2. Proposed Work

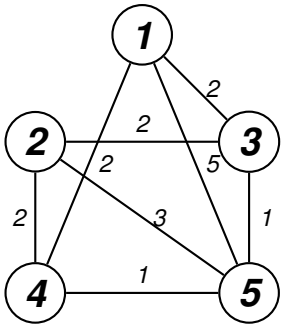
Let N be any positive integer and $N\neq 2^n, n=0,1,2.....$ Let k be the least positive integer such that $N<2^k$.Let $N[i]$ and $K[i]$ are the $k+1$-bit binary array of N and 2^k respectively.
Now define an XOR operation in following way

$$M[i]=N[i]\oplus K[i] \tag{2.1}$$

Let m be the number of $1'$s in $M[i]$.An edge weighted graph G_β using m is defined as follows. Let $v_1,v_2,v_3,...,v_m$ are the vertices of graph G_β corresponding to $1'$s in $M[i]$. Two vertices are adjacent in G_β when their corresponding $1'$s are not adjacent in the binary representation. The weight of each edge gives the following definition.

$$(w_{i,j})_{i\leq j}=\begin{cases}\text{Total numbers of zeros}\\ \text{following } i^{th} \text{ bit to bit } j & ;\text{if } 1\leq i<j\leq m\\ & \text{for}(i\neq 1 \text{ and } j\neq m)\\ \text{Total numbers of zeros}\\ \text{following } i^{th}bit & ;\text{if } i=1 \text{and } j=m\\ 0 & ;\text{ if i=j}\end{cases} \tag{2.2}$$

Example 2.1. *Consider $N=308$ we have $308<512=2^9$ and $k=9$.*
Therefore 10-bit representation of N is $N[i]=0100110100$ and 10-bit representation of 2^k is $K[i]=1000000000$.
Therefore $M[i]=N[i]\oplus K[i]=1100110100$. Since $M[i]$ has five $1's$ the corresponding edge weighted graph G_β has five vertices v_1,v_2,v_3,v_4 and v_5.
Using the definition in (2) we have $w_{1,2}=0$,$w_{1,3}=2$,$w_{1,4}=2$,$w_{1,5}=5$,$w_{2,3}=2$,$w_{2,4}=2$, $w_{2,5}=3$,$w_{3,4}=0$,$w_{3,5}=1$ and $w_{4,5}=1$.The graph is shown below.



Remark 2.2. *The graph G_β we defined using $M[i]$ is a simple graph.*

Remark 2.3. *If m in G_β be the number of $1's$ in $M[i]$.Then $m\geq 3$ and MSB(Most Significant Bit) of $M[i]$ is 1.*

Since N be a positive integer and $N\neq 2^n, n=0,1,2.....$ Let k be the least positive integer such that $N<2^k$. Then N has a $k+1$-bit binary array representation $N[i]$ with MSB is 0 and have at least two $1's$. Also 2^k has a $k+1$-bit binary array representation $K[i]$ with MSB is 1 and all other bits are $0's$. Then applying XOR operation we have

$$M[i]=N[i]\oplus K[i]$$

has $k+1$-bit binary array representation with at lest three $1's$ occurs in it with MSB is 1 . Since m be the number of $1's$ in $M[i]$. We have $m\geq 3$ ■.

Theorem 2.4. *Let G_β is defined as above If $M[i]$ as the $k+1$-bit binary expansion of $2^{k+1}-1$, then the resulting graph has $k+1$ vertices with $k+1$ components (There is no edge connecting any two vertices of the graph).*

Proof. Let $M[i]$ be the binary expansion of $2^{k+1}-1$, is a $k+1$-bit binary expansion contain all bits are $1's$.Since there is no $0's$ in the binary string we cannot find an edge connecting these $k+1$ vertices.
Therefore the resulting graph is totally disconnected and has $k+1$ components ■. □

Theorem 2.5. *Let G_β is defined as above If $M[i]$ is the expansion of $2^{k+1}-1$ then $N[i]$ is the expansion of 2^k-1.*

Proof. Let $M[i]$ be the binary expansion of $2^{k+1}-1$, is a $k+1$-bit binary expansion contain all bits are $1's$. Also $K[i]$ is the $k+1$-bit binary array of 2^k with MSB is 1 and all other bits are $0's$.
Now

$$M[i]\oplus K[i]=(N[i]\oplus K[i])\oplus K[i]=N[i]\oplus(K[i]\oplus K[i])=N[i].$$

Since $M[i]\oplus K[i]$ represent $k+1$-bit binary representation with MSB is zero and all other bits are $1's$ we have $N[i]$ is the expansion of 2^k-1 ■.

□

Theorem 2.6. *Let G_β is defined as above Then there exist a unique disconnected graph with 3 vertices and 3 components.*

Proof. There is two cases occure for the existence of a graph with 3 vertices.
Case 1: Consider the least value on $N=3$.Then $k=2$ such that $3<2^k$.Then 3-bit binary representation of $N=3$ is $N[i]=011$. Similarly 3-bit representation of 2^2 is $K[i]=100$ Then $M[i]=111$, which is the binary representation of 2^3-1 that is $2^{k+1}-1$ then by Theorem **??** the graph of $M[i]$ is disconnected and have 3 components.
Case 2: There are another possibilities for existing three $1's$ in $M[i]$. In such cases there exist at least one zero which is not a MSB.Which means there exist at least one edge connecting any of the two vertices.There of in this case the graph has at most 2 components.
From these two cases we conclude that there exist a unique graph with 3 vertices and 3 components is the graph corresponding to $N=3$ ■. □

Remark 2.7. *The graph G_β with 3 vertices and 3 components is the graph corresponding to $N=3$*

Definition 2.8. *Weighted Adjacency Matrix Let m is the number of $1's$ in the binary equivalent from the array $M[i]$ and we can define a $(m\times m)$ weighted adjacency matrix $A=(a_{ij})$ as follows.*

$$(a_{ij})_{i\leq j}=\begin{cases}\textit{Total numbers of zeros}\\ \textit{following } v_i^{th} & ;\textit{if } 1\leq i<j\leq m\\ \textit{vertex to vertex } v_j & \textit{for}(i\neq 1 \textit{ and } j\neq m)\\ \textit{Total numbers of zeros}\\ \textit{following } v_i^{th}\\ \textit{vertex} & ;\textit{if } i=1 \textit{and } j=m\\ 0 & ;\textit{ if i=j}\end{cases}$$

(2.3)

where a_{ij} denotes the element in the i^{th} row and j^{th} column of the matrix

Remark 2.9. *Since the graph G is a finite simple undirected graph the adjacency matrix is symmetric.*

The adjacency matrix of a graph defined in Example 2.1 is

$$\begin{pmatrix} 0 & 0 & 2 & 2 & 5 \\ 0 & 0 & 2 & 2 & 3 \\ 2 & 2 & 0 & 0 & 1 \\ 2 & 2 & 0 & 0 & 1 \\ 5 & 3 & 1 & 1 & 0 \end{pmatrix}$$

3. Proposed Algorithm

In this algorithm we converts the characters of given plain text into ASCII codes and convert the ASCII codes into 8−bit binary string. After the binary format of each ASCII code is achieved, they are XOR^{ed} with the binary equivalent of K. Where K is the key and must lies between 128 and 255 in such a way that the XOR^{ed} value should contain at least three $1'$s,and the XOR^{ed} code in 8−bit stored in an array $M[i]$. In the next step we define an adjacency matrix as follows.
Let m is the number of $1'$s in the binary equivalent from the array $M[i]$ and form an adjacency matrix $A = (a_{ij})$, where a_{ij} denotes the element in the i^{th} row and j^{th} column of the matrix and

$$(a_i a_j)_{i\leq j} = \begin{cases} \text{Numbers of zeros following } i^{th} \text{ to the next nonzero} + m & ;\text{if } 1 \leq i < j \leq m \text{ for}(i \neq 1 \text{ and } j \neq m) \\ \text{Numbers of zeros following } j^{th} \text{ vertex } +m+ \text{ position of the alphabet} & ;\text{if} i = 1 \text{and} j = m \\ 0 & ;\text{ if i=j} \end{cases} \tag{3.1}$$

The adjacency matrix is sent to the receiver.
In the decryption stage we stored the elements of the adjacency matrix in a temporary array $D[j]$. We may consider either the upper triangular matrix or the lower triangular matrix along the main diagonal. This is because of the symmetric nature of the adjacency matrix. Expand the elements of $D[j]$ and build the 8−bit binary string. To get back the original message, we again XOR^{ed} the 8−bit binary string with the 8−bit key string K.

3.1 Illustrative Example

Let our plain text be "SECRET".Convert each alphabet in the plain text into ASCII code and take the corresponding 8−bit binary representation.Consider the key as $K = 181$.Then XOR^{ed} the binary string of each alphabet with the binary representation of the key K. We get the following

Alphabet	ASCII	Binary Number	Key	XOR Value
S	83	01010011	10110101	11100110
E	69	01000101	10110101	11110000
C	67	01000011	10110101	11110110
R	82	01010010	10110101	11100111
E	69	01000101	10110101	11110000
T	84	01010100	10110101	11100001

Encryption Phase
Consider the adjacency matrix of each alphabet is constructed as follows.
For the alphabet S,there are five $1'$s in the XOR^{ed} column.Therefore the graph corresponding to the alphabet S has 5 vertices and hence its adjacency matrix is of order $m = 5$. The adjacency matrices of each alphabet in the plain text is given below

$$S = \begin{pmatrix} 0 & 5 & 0 & 0 & 7 \\ 5 & 0 & 5 & 0 & 0 \\ 0 & 5 & 0 & 7 & 0 \\ 0 & 0 & 7 & 0 & 5 \\ 7 & 0 & 0 & 5 & 0 \end{pmatrix}$$

$$E = \begin{pmatrix} 0 & 4 & 0 & 10 \\ 4 & 0 & 4 & 0 \\ 0 & 4 & 0 & 4 \\ 10 & 0 & 4 & 0 \end{pmatrix}$$

$$C = \begin{pmatrix} 0 & 6 & 0 & 0 & 0 & 10 \\ 6 & 0 & 6 & 0 & 0 & 0 \\ 0 & 6 & 0 & 6 & 0 & 0 \\ 0 & 0 & 6 & 0 & 7 & 0 \\ 0 & 0 & 0 & 7 & 0 & 6 \\ 10 & 0 & 0 & 0 & 6 & 0 \end{pmatrix}$$

$$R = \begin{pmatrix} 0 & 6 & 0 & 0 & 0 & 10 \\ 6 & 0 & 6 & 0 & 0 & 0 \\ 0 & 6 & 0 & 8 & 0 & 0 \\ 0 & 0 & 8 & 0 & 6 & 0 \\ 0 & 0 & 0 & 6 & 0 & 6 \\ 10 & 0 & 0 & 0 & 6 & 0 \end{pmatrix}$$

$$E = \begin{pmatrix} 0 & 4 & 0 & 13 \\ 4 & 0 & 4 & 0 \\ 0 & 4 & 0 & 4 \\ 13 & 0 & 4 & 0 \end{pmatrix}$$

$$T = \begin{pmatrix} 0 & 4 & 0 & 10 \\ 4 & 0 & 4 & 0 \\ 0 & 4 & 0 & 8 \\ 10 & 0 & 8 & 0 \end{pmatrix}$$

In the adjacency matrix each alphabet the value $a_{1,m}$ = Number of zeros following m^{th} bit $+m+$ Position of alphabet in the plain text. For example in the adjacency matrix of alphabet S the value $7 = 1+5+1 =$ similarly in E the value $13 = 4+4+5$.
All these matrices are sent to the receiver in any order along with the binary string of key K.

Decryption Phase
The matrices are received in any order. Assume the receiver consider the following matrix first.

$$\begin{pmatrix} 0 & 6 & 0 & 0 & 0 & 10 \\ 6 & 0 & 6 & 0 & 0 & 0 \\ 0 & 6 & 0 & 8 & 0 & 0 \\ 0 & 0 & 8 & 0 & 6 & 0 \\ 0 & 0 & 0 & 6 & 0 & 6 \\ 10 & 0 & 0 & 0 & 6 & 0 \end{pmatrix}$$

Because of the symmetric nature of the adjacency matrix the receiver can also taken either the upper triangular matrix or lower triangular matrix along with main diagonal.

The order of the matrix represents the number of $1'$s in the binary string. Here it is 6. Therefore the corresponding binary string has six $1'$s. Using the triangular matrix we can inserts zeros in between $1'$s and we get 11100111. Since $a_{1,6} = 10 = 0+6+4$, The corresponding alphabet is in the 4^{th} position of given plain text.
Now XOR^{ed} this 11100111 with the $8-$bit key string 10110101 we get 01010010.The ASCII code corresponding to this binary number is 82 and the corresponding alphabet is R as we have shown above it is the 4^{th} letter of the given plain text.In the same way we can regenerate all the alphabets in the plain text and hence the message "*SECRET*"

4. Conclusion

In this cryptographic technique, each character represent a symmetric matrix and we have the freedom to select any number between 127 and 255 as Key. The complexity and the uncertainty of the decryption and interpretation of the actual message is very high. The main advantage of this algorithm is that the sender can sent code in any order. This algorithm ensure the proper order of actual message during decryption.The sender has the freedom to choose all ASCII code characters ranging from 0 to 127 for writing secret message is another advantage of this algorithm. This algorithm ensures the safety and security of the data.

References

[1] Wael Mahmoud Al Etaiwi, Encryption Algorithm Using Graph Theory, *Journal of Scientific Research and Reports* 3(19)(2014), 2519–2527.

[2] P. Amudha, A.C. Charles Sagayaraj, A.C. Shantha Sheela T, An Application of Graph Theory in Cryptography, *International Journal of Pure and Applied Mathematics* 119(13)(2018), 375–383.

★★★★★★★★★
ISSN(P):2319 – 3786
Malaya Journal of Matematik
ISSN(O):2321 – 5666
★★★★★★★★★