**Application of Graph Theory in Cryptography**

COURSE- ​ DISCRETE MATHEMATICS IT-203​

**ANURAG KUMAR- 201IT209**

**ROHIT TAPARIA-201IT151**

**VANSHIKA JOLLY-201IT263**

**Department of Information Technology, NITK Surathkal**

***Date of Submission: 17 December 2021***

in partial fulfillment for the award of the degree of

**Bachelor of Technology in Information Technology**



**At Department of Information Technology**

**National Institute of Technology Karnataka, Surathkal**

DECEMBER 2021

**Department of Information Technology, NITK Surathkal Discrete Mathematics Project Final Semester Evaluation Report**

**Course Code**: IT203

**Course Title**: Discrete Mathematics Project

**Title**: Application of Graph Theory in Cryptography

**Project Group:**

|  |  |  |
| --- | --- | --- |
| **NAME** | **ROLL NO.** | **EMAIL** |
| ANURAG KUMAR | 201IT209 | anuragkumar.201it209@nitk.edu.in |
| ROHIT TAPARIA | 201IT151 | Rohitktaparia.201it151@nitk.edu.in |
| VANSHIKA JOLLY | 201IT263 | Vanshikajolly.201it263@nitk.edu.in |

**Place:** NITK, Surathkal

**Date:** 13th November, 2020

**Instructors: Dr. BHAWANA RUDRA**​

**Mrs.TRUPTI CHANDAK**​

**CONTENTS**

**PAGE NO.**

1. **Abstract 4**
2. **Introduction 5**
3. **Literature survey 7**
4. **Methodology 8**
5. **Results 17**
6. **Conclusion and future work 20**
7. **References 21**
8. **Github link 21**

**ABSTRACT**

Cryptography has become an important aspect in today's world, especially during the transfer of important data, as data is becoming “the new oil”. We need to make a new non-standard secure encryption algorithm using the concepts of graph theory to prevent any traditional opportunity to sniff data. The proposed algorithm represents a new encryption algorithm to encrypt and decrypt data securely with the benefits of graph theory properties.​

**INTRODUCTION**

**Cryptography** is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. The prefix "crypt-" means "hidden" or "vault" and the suffix "-graphy" stands for "writing." In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and confidential communications such as credit card transactions and email. Nowadays, it is used everyday by billions of people for securing electronic mail and payment transactions.

The science of cryptography touches on many other disciplines, both within mathematics and computer science and in engineering. In mathematics, cryptology uses, and touches on, algebra, number theory, graph and lattice theory, algebraic geometry and probability and statistics. Analysis of cryptographic security leads to using theoretical computer science especially complexity theory. The actual implementation of cryptosystems, and the hard work of carrying out security analysis for specific cryptosystems falls into engineering and practical computer science and computing. In this paper, Graph Theory is being used to create a secure Encryption - Decryption algorithm.

An undirected Graph is denoted by G(V, E) where V is the set of vertices and E is a set of edges that connect vertices with each other. Information can be stored in each of the vertices. There are two ways in which we can represent Graphs: Adjacency matrix and adjacency list. In graph theory and computer science, an adjacency list is a collection of unordered lists used to represent a finite graph. Each list describes the set of neighbors of a vertex in the graph. An adjacency matrix is a square matrix used to represent a finite graph.

The elements of the matrix indicate whether pairs of vertices are adjacent or not in the graph. Weighted graphs are those graphs in which every edge is assigned with some weight. Weighted graphs can also be stored using adjacency matrices. Here each cell at position M[u, v] is holding the weight of the edge from vertex u to vertex v.

In Graph Theory, a spanning tree T of an undirected graph G is a sub graph that is a tree which includes all of the vertices of G, with a minimum possible number of edges. A minimum spanning tree is a spanning tree whose sum of edge weights is as small as possible. In this paper, an encryption algorithm has been proposed which uses Graph Theory. Weighted graphs have been used to store, encode and decode the data. Adjacency matrices have been used to represent the graphs. Various other concepts like Minimum Spanning Tree (MST), Prim’s Algorithm, matrix operations etc. have been used in the algorithm to encode/ decode data. This algorithm provides an efficient and secure method to encode important data like passwords and other sensitive information and send the data to the receiver where the data will be decoded and used for further processing.

**LITERATURE SURVEY**

* “Encryption algorithm using graph theory” by Wael Mahmoud Al Etaiwi: [Link](https://www.researchgate.net/publication/269803082_Encryption_Algorithm_Using_Graph_Theory)​

This is our base paper. We have picked up some encryption techniques to encrypt and decrypt data securely with the benefits of graph theory properties, and use the concepts of cycle graph, complete graph and minimum spanning tree to generate a complex cipher text using a shared key.​

​

* “Some graph based encryption algorithms” by Shafiq ur Rehman and Ghulam Farid: [Link](https://www.researchgate.net/publication/349459366_Some_Graph-Based_Encryption_Schemes)​

This paper explains about different encryption algorithms, use of them in different fields and encryption algorithms in cryptography for data security. This paper proposes some new encryption algorithms for secure transmission of messages using some special bipartite graph.

**METHODOLOGY**

In this section, the algorithm and the working of the proposed cryptography method will be mentioned. Detail, flowcharts and examples related to our proposed method will also be mentioned here.

1. **PROPOSED ALGORITHM**

When the message has been fetched from the user, the characters in the message are represented as vertices in a graph. All the vertices are added in the graph sequentially so as to generate a cyclic graph. Then, edge weights are assigned to each of the edges in the cycle created by using a particular scheme which will be discussed shortly. All the remaining edges, i.e. the diagonals of the cycle are then drawn and weights are assigned to them. We add an extra vertex and an extra edge with a special character, suppose ‘A’ to point to the starting character of the message. Thus, now we have a complete weighted undirected graph. Now, the next step is to compute the Minimum Spanning Tree(MST) of the generated complete graph. The MST is represented in the adjacency matrix and its diagonal stores the order of the characters in the original message. Adjacency-matrix of the complete graph is then multiplied to the adjacency-matrix of MST. The resultant matrix is multiplied to the key matrix. The final matrix is the encryption data to be sent to the recipient.

**Scheme for assigning weights to the edges:**

● Start with the character that has been used to point to the 1st character of the input string (‘A’ in our case). Calculate the difference between the ASCII values of the 1st character of the input string and this pointer character and assign this weight to the edge between these two vertices by adding one.

● If the edge is a side of the polygon(cycle) or between the special character and the starting character, then for computing the edge weights, ASCII values of the characters are considered and the edge weight of any such edge is computed by calculating the difference between the ASCII values of the characters and then adding one to it. Calculate this difference for each edge in a cyclic manner. (See the example part for more info).

● The reason for adding one in the above method is to avoid the edge weight of two same characters from becoming zero. And if the edge weight becomes zero, then while computing the MST the program will consider that no edge lies between these vertices which is a wrong assumption.

● If the edge is a diagonal of the polygon, then edge weights are sequentially assigned starting from 256 and increasing the weight by 1 each time.

**Encryption Algorithm:**

● Add a special character to indicate the starting character (Let’s say A).

● Add vertex for each character in the plain text to the graph sequentially.

● Link vertices together by adding an edge between each sequential character in the plain text until we form a cycle graph.

● At this point the graph should look like a cycle with one edge sticking out.

● Assign weight to each edge using the scheme as discussed earlier.

● Add more edges (diagonals) to form a complete graph M2 , each new added edge has a sequential weight starting from 256.

● Then compute the Minimum Spanning Tree: M2 .

● Then store the vertices in proper order in the M2 matrix in the diagonal places

● Next multiply matrices M1 by M2 to get M3

● After that we multiply M3 by a predefined Shared-Key K to form Cipher.

● After the encryption process, the Cipher matrix and the M1 matrix are to be sent as the encoded message.

**Decryption Algorithm**:

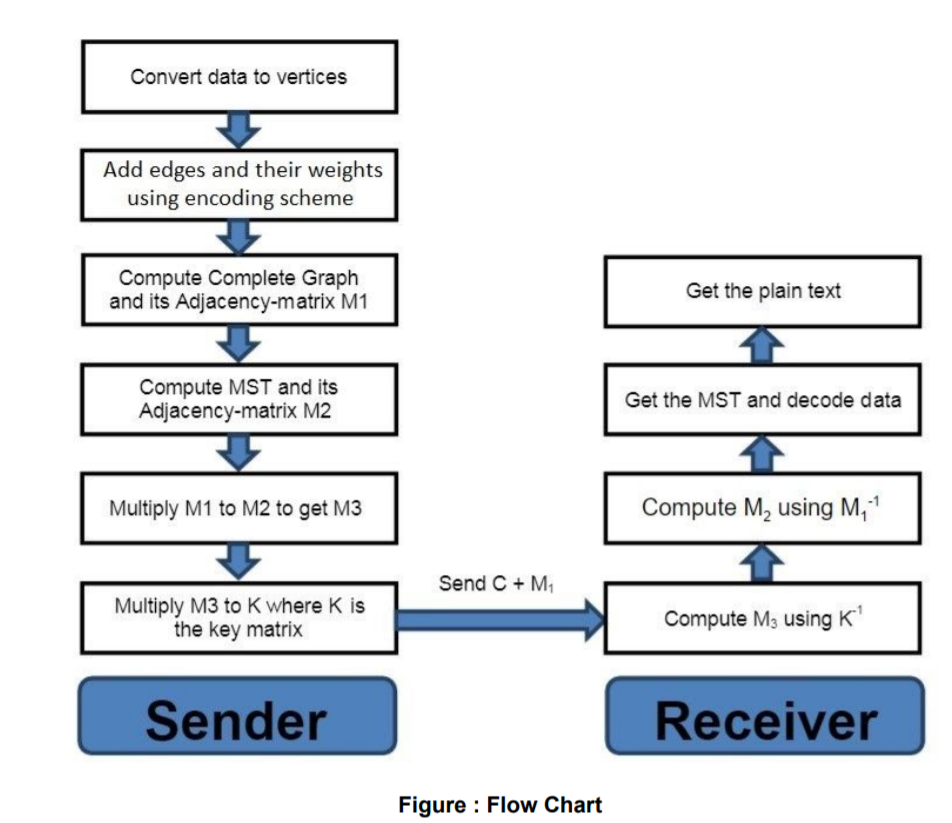
● The receiver receives the cipher and the M1 matrix separately from the sender. ● The receiver computes M3 by using the inverse form of the Shared-Key: K -1 and then multiplying the matrix with C.

● Then compute M2 by using the inverse form of M1 , i.e. M1 -1 multiplied with matrix M3 .

● Now, the receiver end has computed the MST matrix, M2 .

● Then compute the original text by decoding M2 using the encoding scheme.

● This original text is then displayed at the receiver end.



**B. EXAMPLE 1**

Let’s encrypt the message “WAEL”.

INPUT STRING = “WAEL”

**ENCODING**:

**Step1: Converting characters of the message to vertices of graph**

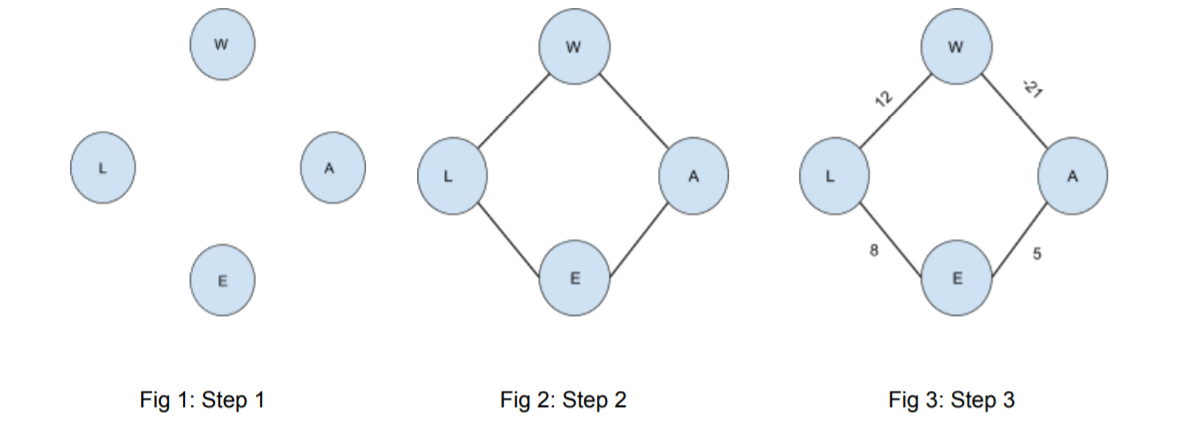
The first step is to convert the message to a graph, by converting each character to a vertex as shown in Fig. 1.

**Step 2: Adding edges to form a complete cycle of the input**

Then, link each two sequential characters together to form a cycle graph. Now the graph should look like a cyclic polygon. (See Fig 2)

**Step 3: Add weights to each of the edges of the cycle**

Add weights for each of the edges using the weight scheme discussed in the algorithm section (Using difference of ASCII values of adjacent vertices- See Fig 3)

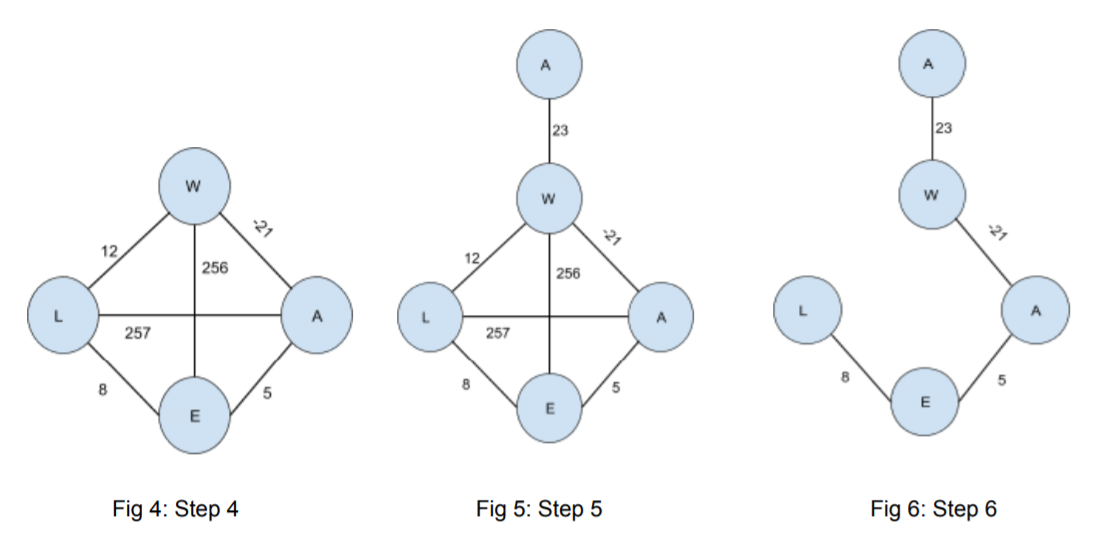


**Step 4: Add weights to the diagonals to make the complete graph**

After that, keep adding edges to form a complete graph. This can be done by connecting all the diagonals. Each new added edge has sequential weight starting from the maximum weight i.e. 256. The weights of the diagonals will be 256, 257, 258… (See Fig 4)

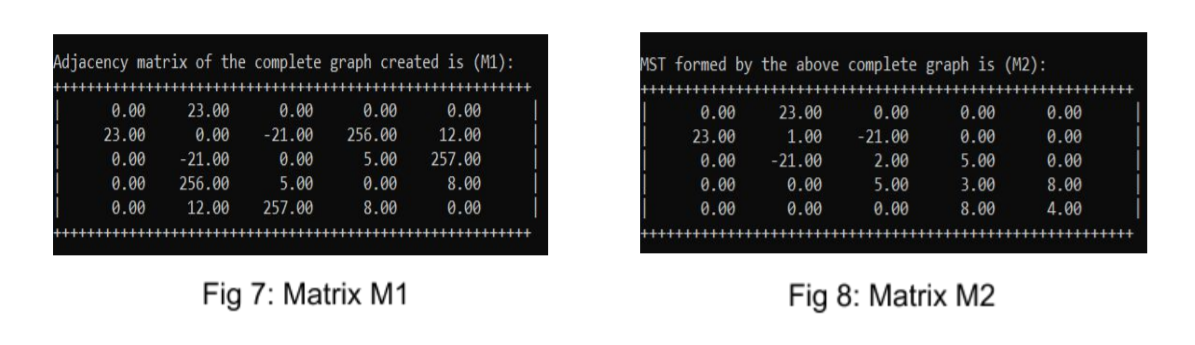
**Step 5: Add a special character to indicate the starting character**

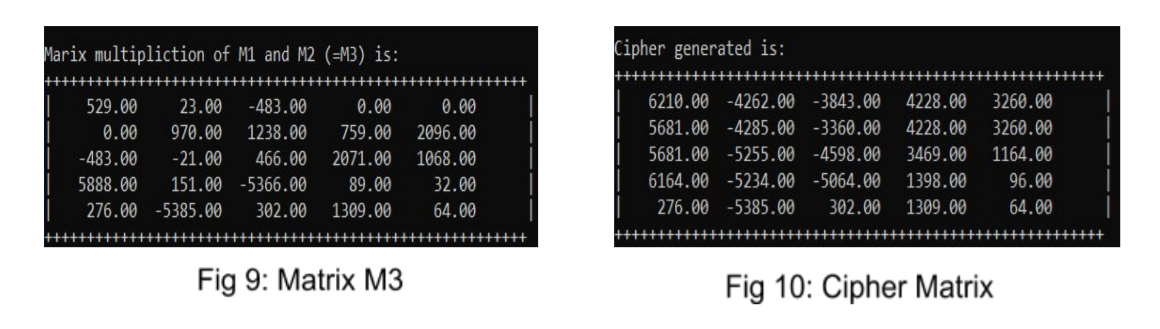
Now, add an extra vertex label “A” to the first character of the message and then compute the edge weight of this newly created edge using the encoding scheme. (See Fig 5) The complete adjacency matrix, M1 , is shown in Fig 7.



**Step 6: Compute MST and its adjacency matrix M2**

As we have the complete graph now, compute the MST by using the Prim’s Algorithm. (See Fig 6) The adjacency matrix for this MST, M2 , is shown in Fig 8.





**Step 7: Computing Matrix M3**

We calculate matrix M3 by matrix multiplication of M1 and M2 . The matrix M3 for “WAEL” is shown in Fig.9 above.

**M3 = M1 \* M2**

**Step 8: Computing Cipher Matrix**

This is the final step in encrypting the input message. Here, the Cipher matrix is generated by matrix multiplication of the pre-defined Key and M3. Now the Cipher and M1 are ready to be sent to the receiver. Fig.10 above shows the Cipher for our input message.

**Cipher = Key \* M3**

Send ( Cipher + M1 ) to Receiver.

**DECODING:**

**Step 1: Receive the data, compute inverse of Key**

The receiver gets the encoded message and separates the message to retrieve the Cipher matrix (Fig 10) and the M1 matrix (Fig 7). The receiver node then calculates the inverse of the pre- shared Key. The Key is shown in Fig 11 and the Key -1 (Key- inverse) is shown in Fig 12.

**Step 2: Compute M3 using Key -1 and Cipher**

Now, the matrix M3 is reconstructed using the key- inverse (Key -1 ) matrix. M3 is calculated by the matrix multiplication of Key -1 and Cipher matrices.

**M3 = Key -1 \* Cipher**

**Step 3: Compute M2 using M1 -1 and M3**

Next, Matrix M2 is reconstructed using the inverse of matrix M1 . M2 is calculated by the matrix multiplication of M1 -1 and M3 matrices**.**

**M2 = M1 -1 \* M3**

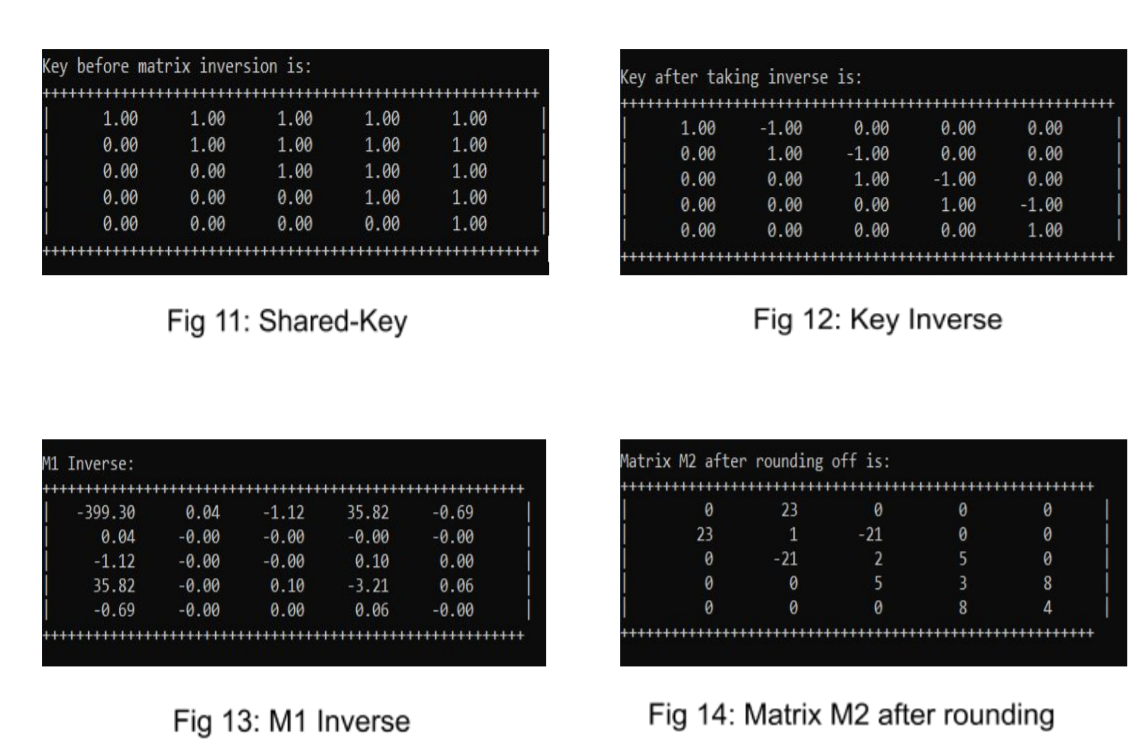
After calculation of Matrix M2, the each value in the double- data type M2 matrix has to be converted to the nearest integer by rounding off.

Matrix M1 -1 is shown in Fig 13 and Matrix M2 after rounding off to the nearest integer is shown in Fig 14.

**Step 4: Get the MST and decode data**

The matrix M2 (Fig 14) itself represents the MST. After the MST has been extracted, the original message is decoded from it. To get the original message back, first we traverse through the right part of the MST (Fig 6) starting from the top and keep adding the weights every time and find the ASCII character corresponding to the added weight at each edge. Thus a new character is found by adding the weight at each node and this character is concatenated to the end of the reconstructed string.

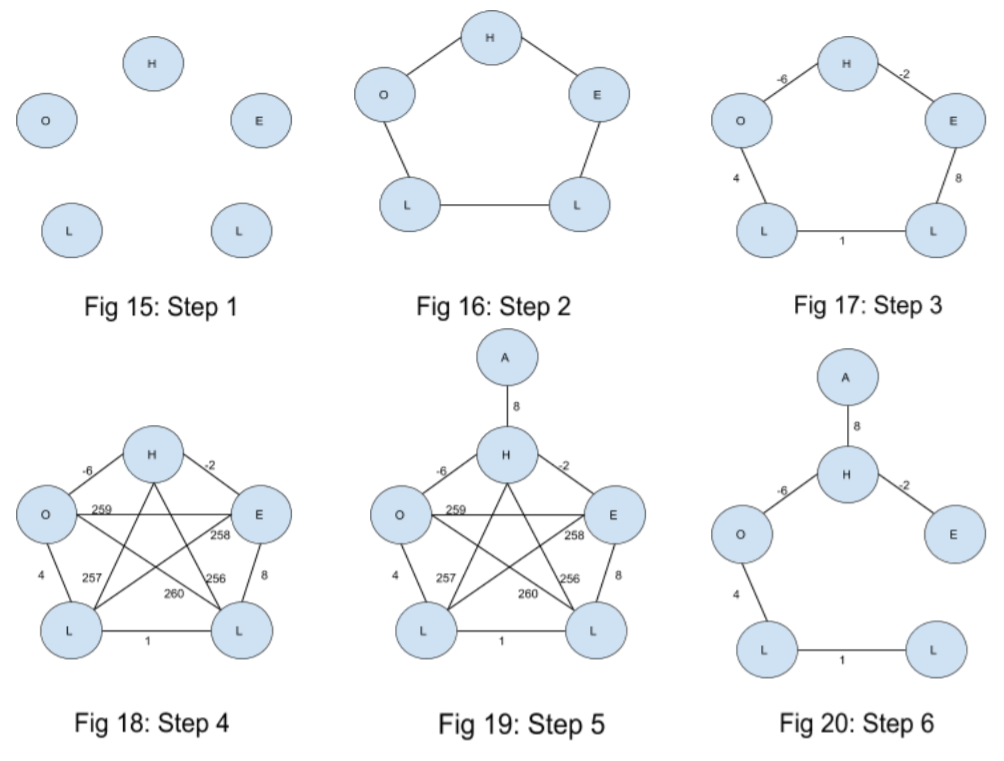
But, this method of decoding the data from MST (Step 4 in decoding) will not work for all messages. This method worked for the message “WAEL” because the MST of this graph is cyclic (excluding the special character- See Fig 6). But, in some messages the computed MST may not be entirely cyclic. The MST can also be branched. In that case, we need to change our Step 4 a little bit. In example 2 the Step 4 of decoding, has been extended further to cover all cases.



1. **EXAMPLE** **2**

In the previous example, the MST corresponding to the constructed graph of the word “WAEL” is cyclic (Fig 6). So, the Step-4 of decoding (Get the MST and decode data) was quite simple. But in many messages, the generated MST can be branched. This can be visualised by using the algorithm for the word “HELLO”. Fig 15- 20 show the various steps involved in extracting the MST corresponding to the message “HELLO”.

We can see that the generated MST (Fig 20) is actually branched (neglecting the 1st special character). So, the final decoding process has to be extended to cover all such cases. In this case, first traverse through the right branch of the MST and follow the normal process of adding the weights at each node and getting the corresponding. Then if an edge is absent (denoted by 0 in adjacency matrix), stop the traversing. Come back to the first character (H in this case) and this time traverse through the left branch and every time subtract the weight from the ASCII value of the 1st character (H). The character corresponding to this new ASCII value has to be concatenated to a new string. This is done till we reach the end of the left branch. Finally reverse this string and concatenate this string with the string generated during traversal of the right branch. This will give the final decoded message.



Message Decoded in trip 1:​

String 1 = “HE”​

Message Decoded in trip 2:​

String 2 = “OLL​”

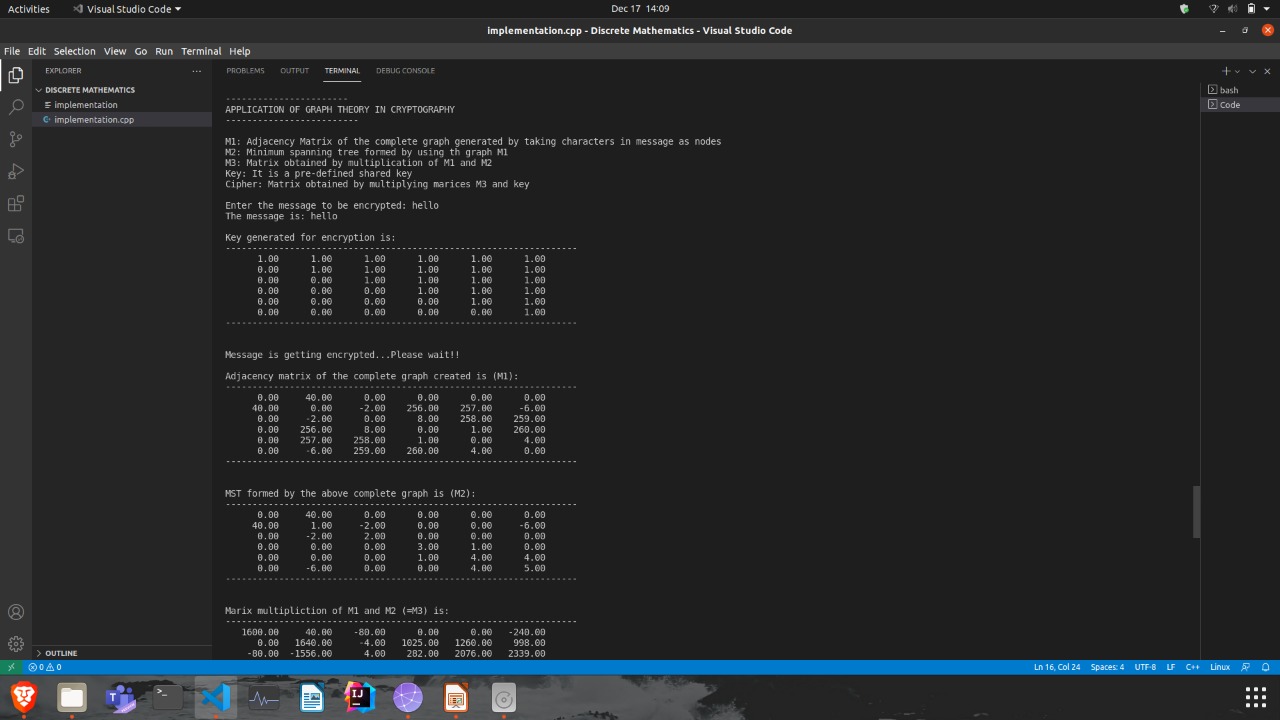
Final Decode message:​

String 1 + reverse(String 2)​

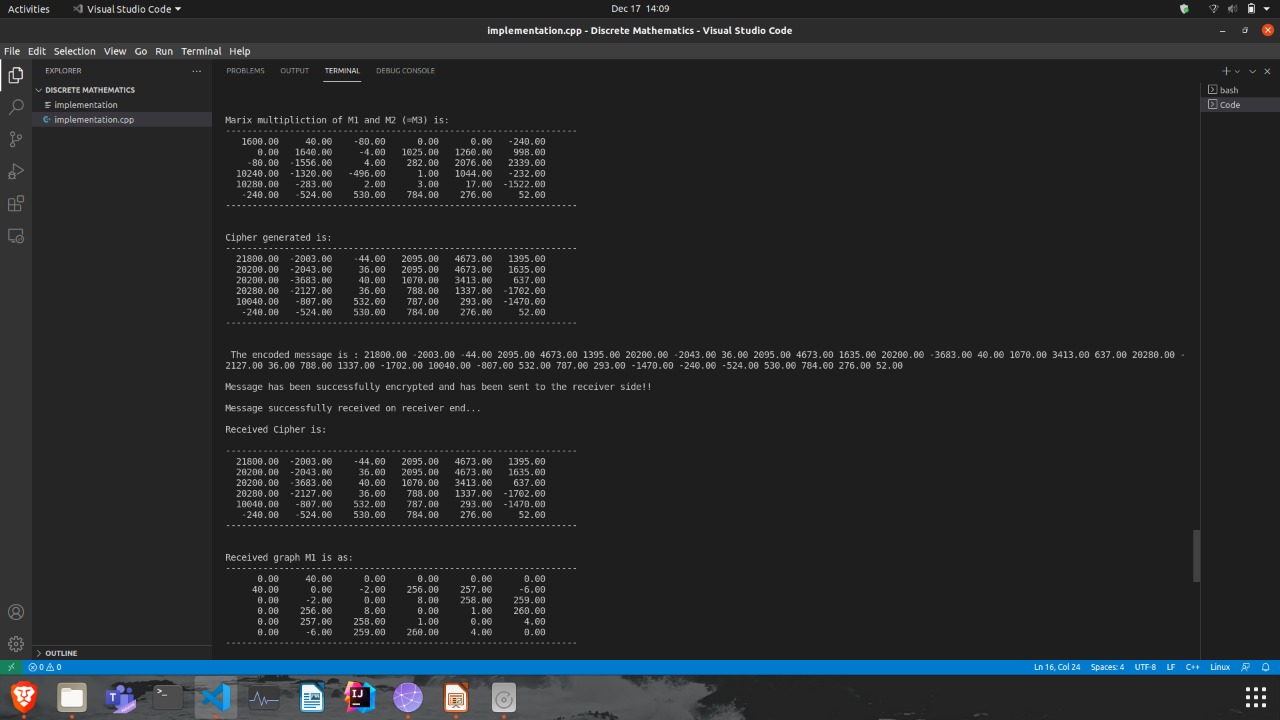
HELLO

**RESULTS**

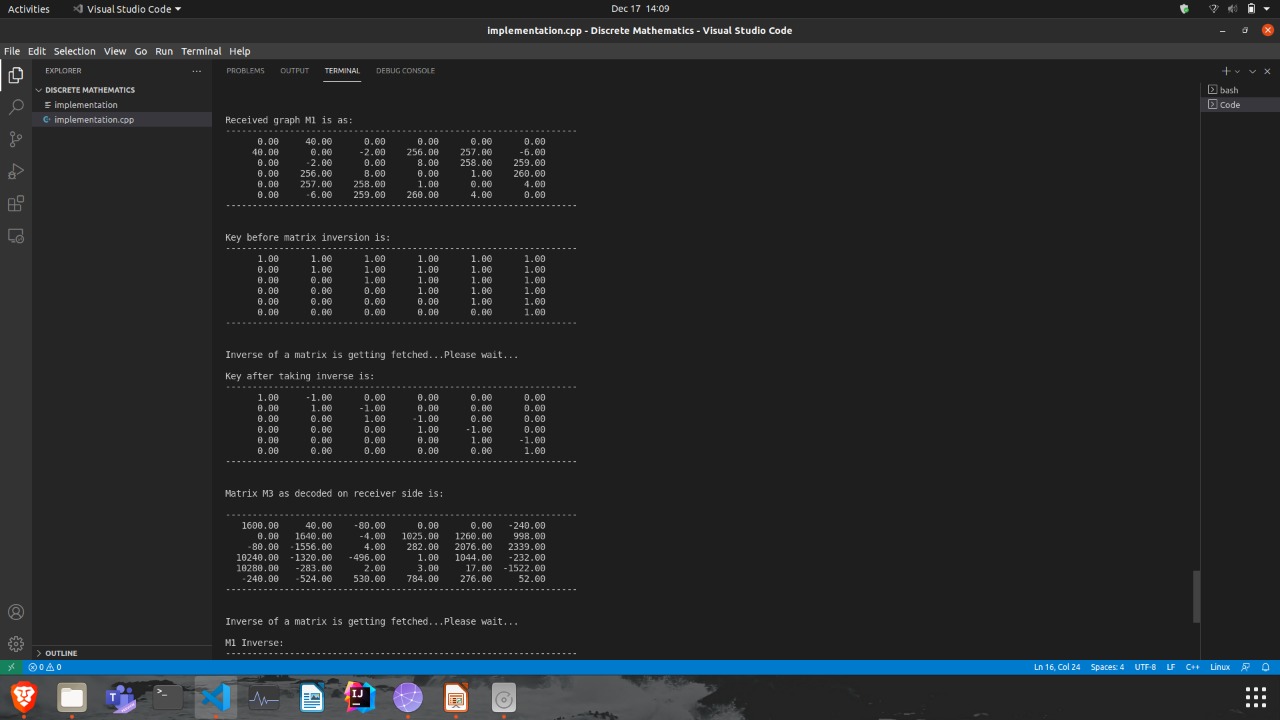
This proposed algorithm was implemented by us using C++ programming language. Our implementation takes the message as input. First the program encodes the input message using the encoding algorithm. Then this encoded message is passed on to the decoding module of our program. The decoding module decodes the message and finally displays the decoded message. The snapshots when the word “HELLO” was given as input message to our implementation are shown below:

****

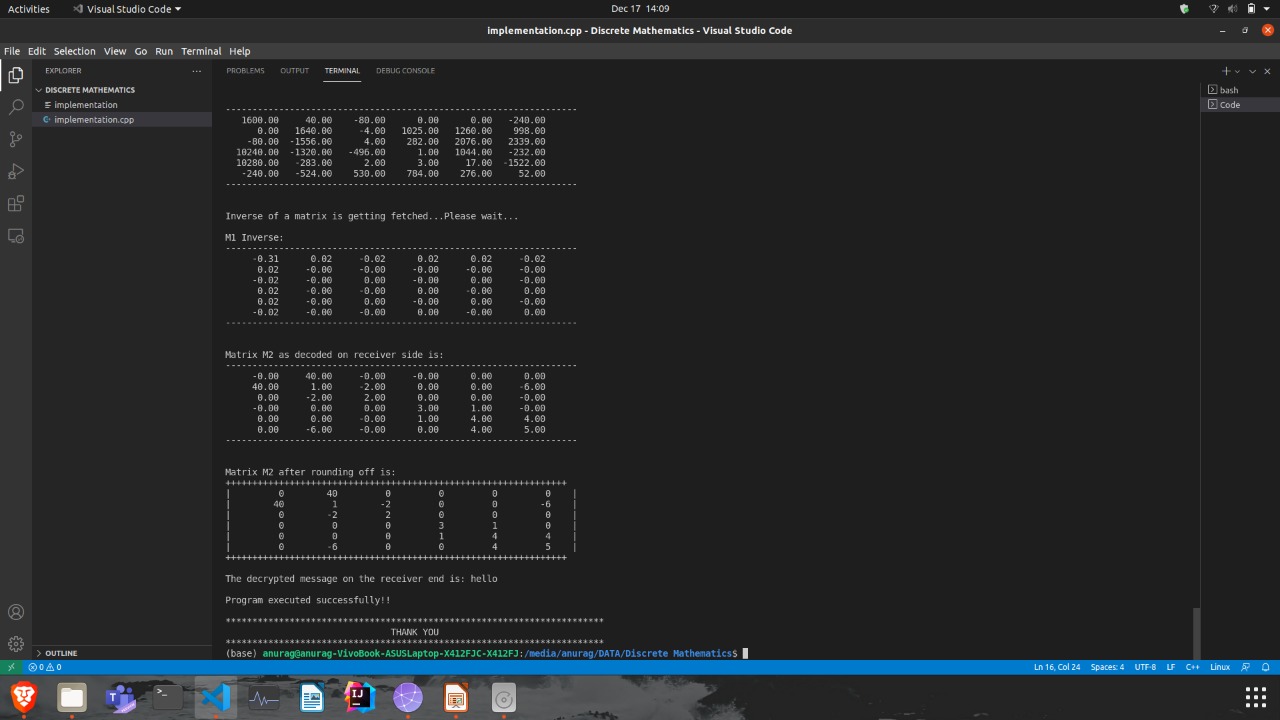
**Fig** : Message is fetched, which is to be sent



**Figure :** Message Encrypted

****

**Figure :** Cipher and M1 are received and Decryption starts

****

**Figure :** Decrypted Message is displayed at receiver end

**CONCLUSION**

In this paper, we have proposed a technique to encrypt a message using concepts of Graph theory like Minimum Spanning Trees (MST), Prim’s algorithm, adjacency matrix etc. Cryptography is necessary in the modern era to send and receive data safely and securely and our proposed algorithm is able to encrypt the messages with high security.

We have used a secure pre-defined key which is shared between the sender and the recipient only. The cipher is then generated and passed on to the receiver along with the graph. Once the recipient receives the necessary data, the MST is re-constructed by the receiver and the message is regenerated by re-tracing the encryption algorithm in the reverse order. The order of the characters in the message are determined by traversing the values in the correct order in the diagonal of the computed MST by the receiver. This algorithm almost works for all types of characters in the range of ASCII and can be safely used to encrypt passwords and secure data of short lengths.

**FUTURE WORK**

● For messages of greater lengths, the computational time is comparatively higher as time is consumed in calculating the inverse of a matrix which takes O(n 3 ) time complexity.

● In such cases the data of greater lengths can be divided into smaller sub parts and then encrypted. The smaller sub parts decrypted on the receiver end can then be concatenated to form the original message. This will increase the efficiency of the algorithm to a large extent.

● Further, we can try to optimize our algorithm by reducing the complexity of various modules of our algorithm.

**REFERENCES**

1. Encryption Algorithm Using Graph Theory. 2014. N.p.: Wael Etaiwi.

<https://www.researchgate.net/publication/269803082_Encryption_Algorithm_Using_Graph_Theory>

2. “Some graph based encryption algorithms” by Shafiq ur Rehman and Ghulam Farid: [Link](https://www.researchgate.net/publication/349459366_Some_Graph-Based_Encryption_Schemes)​

**GITHUB LINK**

Github repository of our project: