Creating Ciphertext and Decipher using Graph Labeling Techniques

B. Deepa , V. Maheswari, V. Balaji

Abstract: In this paper, we design plaintext through product edge labeling for a Cycle Graph. The edge labels thus obtained is further processed through Caesar cipher method. The ciphertext thus obtained is subjected to Bifid Cipher for which we apply matrix multiplication. The decryption is performed using inverse matrix multiplication and subsequent application of Bifid cipher and Caesar Cipher yields our plaintext. This methodology is considered highly efficient and secure as it combines Cryptographic technique together with Graph Labeling thereby making it difficult for any Adversary to hack the plaintext. We investigate the above technique using Non-singular square matrices.

Keywords: Plaintext, Ciphertext, Encryption, Decryption, Bifid cipher, Rotation letters, Inverse matrix, Cycle Graphs.
AMS subject classification MSC (2010) No: 05C78

I. INTRODUCTION

Dinesh Goyal, Naveen Hemrajani, Kritika Paliwal introduced the concept GPH Algorithm: Improved CBC improved BIFID cipher Symmetric Key Algorithm[1], and also [2],[3].

Inspired by this work, we introduce a methodology of forming a plaintext by applying product labeling for a given \( \mathcal{G} \) – Cycle graph \( G \) and then converting the plaintext to ciphertext by using Caesar and Bifid cipher method.

In traditional Caesar cipher the plaintext letters are shifted to a certain number of places down the alphabet. A Caesar Cipher is a simple form of Substitution Cipher were merely the letters are substituted in the place of original letters. But here we start numbering the alphabets beginning with the alphabet \( u, v, w \ldots \), \( a, b \ldots \), \( s, t \) and we assign the value 1 to \( u \), 2 to \( v \), and so on.

The Bifid cipher is considered a more secure cipher because it breaks the message apart into two separate streams and then recombines them. Bifid is a cipher technique which combines the Polybius square with transposition and uses fractionation to achieve diffusion.

It was invented by Felix Delastelle a Frenchman who invented several ciphers including the bifid, trifid, and four-square ciphers. Keys for the Bifid cipher consist of a 26 letter ‘key square’. To encode a message, the letters are written in column wise "uvwx", then the plaintext is figured out the row and column for each letter.

A. Definition

Cryptography is passing confidential message from sender to the recipient, the conversion of information from a cryptic state to readable state. The originator of an encrypted message shares the decoding technique only with intended recipients to preclude access from the attacker.

B. Definition

A square matrix K, with a determinant not equal to zero, then there exists an inverse matrix of

\[
K = \frac{\text{adj} K}{\text{det} K}
\]

C. Definition

In cryptography readable material is known as plaintext.

D. Definition

Encrypting the message into an unreadable format is called Ciphertext.

E. Definition

A Graph \( G \) \((V, E)\) is said to be product labeled graph, i.e.: \( V(G) \rightarrow 3N \) is an one-one mapping such that the resultant edge labels are \( f’(e = uv) = (u \times v) \mod 26 \).

F. Definition

\( C^n \) Graph

The cycle graph with \( n \) number of vertices connected in a closed chain is known as \( C^n \) Graph.

Kolam is an artistic creation. It is a ubiquitous art form predominant in South India, while also seen in a few places in northern India and South East Asia. Kolam holds a rich tradition of cultural and medicinal significance. Kolams are generated using kolam grammar.

Kolam is an artistic creation. It is a ubiquitous art form predominant in South India, while also seen in a few places in northern India and South East.
Creating Ciphertext and Decipher using Graph Labeling Techniques

II. OUTLINE OF ENCRYPTION AND DECRYPTION TECHNIQUE

TO ENCRYPT

Step 1: Draw a Cycles graph \( G = (V, E) \) with vertices \( V = \{v_1, v_2, v_3, ..., v_n\} \) and edges \( E = \{e_1, e_2, e_3, ..., e_{n-1}\} \).

Step 2: Obtain the Edge labels by definition through Caesar cipher.

Step 3: Use bifid cipher to encipher our plaintext message.

Step 4: A matrix multiplication to get our cipher text message.

TO DECIPHER

Step 1: The receiver will decipher the message by using inverse matrix multiplication and bifid cipher.

Step 2: Thus, the receiver will get a plaintext through which Caesar Cipher.

IV. THEOREM

Any Cycle graph is a product labeled Graph.

Proof: Let \( C_p \) be the Cycle graph with different vertices \( v_1, v_2, v_3, ..., v_n \).

Consider \( f: V(k_n) \rightarrow 3N \) by \( f(u_i) = 3i \) for all \( i=1, 2...n \).

Then by definition \( f^*(e=uv) = (u \times v) \) mod 26 the edge labels are 18,2,4,24,10, 2……etc.

Fig a: \( C_p \) Graph with \( p \) vertices and 2\( p \) edges

For the above Cycle Graph, we apply product edge labeling and making use of Caesar cipher with additive key 6, obtained the edge labels thus obtained forms our initial Ciphertext.In the overall thirty edges we are using the some of the edges only rest of edges are known as the jumped edges.

| Table I: Additive 6 Caesar Cipher |

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

Retrieval Number: A10371091S192019©BEIESP
DOI:10.35940/ijeat.A1037.1091S19

Published By: Blue Eyes Intelligence Engineering & Sciences Publication
Now let’s we explain the process by illustrations,

V. ILLUSTRATION:

let our Plaintext be: go abroad for job

Table II: Conversion of Plaintext using Additive 6 Caesar Cipher

<table>
<thead>
<tr>
<th>13</th>
<th>21</th>
<th>7</th>
<th>8</th>
<th>24</th>
<th>21</th>
<th>7</th>
<th>10</th>
<th>12</th>
<th>21</th>
<th>15</th>
<th>21</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>a</td>
<td>b</td>
<td>r</td>
<td>o</td>
<td>a</td>
<td>d</td>
<td>f</td>
<td>o</td>
<td>r</td>
<td>j</td>
<td>o</td>
<td>b</td>
</tr>
</tbody>
</table>

Thus, the plaintext is converted into ciphertext which is our initial plaintext.

BIFID CIPHER

Now here we are going to use the Bifid Cipher technique which is invented by Felix Blessed Virgin Delastelle in 1840-1902. In the Bifid cipher we use square matrix of order 5 by 5 where each matrix element has a corresponding row and column entity.

\[
\begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 \\
1 & u & z & e & j & o \\
2 & v & a & f & k & p \\
3 & w & b & g & l & q \\
4 & x & c & h & m & r \\
5 & y & d & i & n & s, t \\
\end{array}
\]

Fig.b Bifid Cipher

So, for our Plain text: go abroad for job

The corresponding row and column entity are as follows, Row Value:3 1 2 3 4 1 2 5 2 1 4 1 1 3 Column Value: 3 5 2 2 5 2 3 5 5 4 5 2

Notice just how the letter "g" has the value of 33. "o" is 15 meanwhile it is found in row 1, column 5. s and t share theposition of (5,5) in the matrix above. After the message has been written out, with row and column values written as shown above, we encode the converted edge labels using matrix multiplication.

VI. ENCODING OF EDGE LABELING

We consider a 3 x10 matrix and the labels are written into three number blocks and to complete the matrix we add null values at the end

Table III:

| 3 | 1 | 2 | 3 | 4 | 1 | 2 | 5 | 2 | 1 |

Thus, the message is "UWxXZJZDEFGHIJKMNOPQRST"

Let us consider a key matrix \( K = \begin{pmatrix} 7 & 2 & 1 \\ 0 & 3 & -1 \\ -3 & 4 & -2 \end{pmatrix} \mod 26 \)

Now we use the key matrix multiplication to encrypt message. The key matrix should be selected such that its inverse exits.

\[
k_p = \begin{pmatrix} 7 & 2 & 1 \\ 0 & 3 & -1 \\ -3 & 4 & -2 \end{pmatrix} \mod 26 = \begin{pmatrix} 5 & 11 & 19 \\ 10 & 1 & 0 \\ 3 & 23 & 18 \end{pmatrix}
\]

Now, the receiver will decipher the message by using inverse matrix multiplication and Bifid Cipher

VII. DECODING OF EDGE LABELING

To decrypt the message to the original one, we use the inverse of key matrix such

that \( K^{-1} = \begin{pmatrix} -2 & 8 & -5 \\ 3 & -11 & 7 \\ 9 & -34 & 21 \end{pmatrix} \mod 26 \)

Now multiplying the inverse matrix with column matrices which generated from matrix operations \( K \cdot C \mod 26 \).

Thus
Creating Ciphertext and Decipher using Graph Labeling Techniques

Converting the above matrix in the form of table we get,

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>u</td>
<td>z</td>
<td>e</td>
<td>j</td>
<td>o</td>
</tr>
<tr>
<td>2</td>
<td>v</td>
<td>a</td>
<td>f</td>
<td>k</td>
<td>p</td>
</tr>
<tr>
<td>3</td>
<td>w</td>
<td>b</td>
<td>g</td>
<td>l</td>
<td>q</td>
</tr>
<tr>
<td>4</td>
<td>x</td>
<td>c</td>
<td>h</td>
<td>m</td>
<td>r</td>
</tr>
<tr>
<td>5</td>
<td>y</td>
<td>d</td>
<td>i</td>
<td>n</td>
<td>s, t</td>
</tr>
</tbody>
</table>

Thus, the plaintext is converted into ciphertext which is our initial plaintext.

**BIFID CIPHER**

Now here we are going to use the Bifid Cipher technique

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>u</td>
<td>z</td>
<td>e</td>
<td>j</td>
<td>o</td>
</tr>
<tr>
<td>2</td>
<td>v</td>
<td>a</td>
<td>f</td>
<td>k</td>
<td>p</td>
</tr>
<tr>
<td>3</td>
<td>w</td>
<td>b</td>
<td>g</td>
<td>l</td>
<td>q</td>
</tr>
<tr>
<td>4</td>
<td>x</td>
<td>c</td>
<td>h</td>
<td>m</td>
<td>r</td>
</tr>
<tr>
<td>5</td>
<td>y</td>
<td>d</td>
<td>i</td>
<td>n</td>
<td>s, t</td>
</tr>
</tbody>
</table>

So, for our Plain text: “a man had good wool bag”

The corresponding row and column entity are as follows,

Row Value: 242542531153113323

Column: Value: 242432235521554223

the letter "a" has the value of 22, "m" has the value of 44, it is found in row 4, column 4 in the matrix above. After the message has been written out, with row and column values written as shown above, we encode the converted edge labels using matrix multiplication.

**IX. ENCODING OF EDGE LABELING**

We consider a 3 x12 matrix and the labels are written into three number blocks and to complete the matrix we add null values at the end

Now let’s we explain the process by illustrations, let our Plaintext be: a man had good wool bag
Let us consider a key matrix 
\[ K = \begin{pmatrix} 7 & 2 & 1 \\ 0 & 3 & -1 \\ -3 & 4 & -2 \end{pmatrix} \]

Now we use the key matrix multiplication to encrypt message. The key matrix should be selected such that its inverse exits.

\[ kp = \begin{pmatrix} 7 & 2 & 1 \\ 0 & 3 & -1 \\ -3 & 4 & -2 \end{pmatrix} \begin{pmatrix} 2 & 4 & 2 & 5 & 4 & 2 & 5 & 3 & 1 & 5 & 3 & 1 & 5 & 3 \\ 1 & 1 & 3 & 3 & 2 & 2 & 3 & 2 & 4 & 2 & 3 & 2 \\ 2 & 3 & 5 & 5 & 2 & 1 & 3 & 5 & 5 & 4 & 2 & 2 & 3 \end{pmatrix} \mod 26 \]

\[ c = \begin{pmatrix} 18 & 7 & 25 & 20 & 8 & 21 & 18 & 8 & 15 & 17 & 17 & 2 \\ 10 & 0 & 4 & 4 & 4 & 8 & 1 & 7 & 2 & 10 & 7 & 3 \\ 20 & 12 & 22 & 13 & 18 & 4 & 9 & 23 & 23 & 9 & 19 & 19 \end{pmatrix} \]

The ciphertext thus obtained is arranged in the following table

<table>
<thead>
<tr>
<th>Table VIII: FINAL CIPHERTEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>20</td>
</tr>
</tbody>
</table>

Converting the above matrix in the form of table we get,

<table>
<thead>
<tr>
<th>Table VIII: FINAL CIPHERTEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>

Rewriting the above text in the form of rows and columns

Row Value: 2 4 2 5 4 2 5 3 1 5 3 1 3 3 2 3

Column: Value: 2 4 2 4 3 2 3 5 5 2 1 5 5 4 2 2 3

**BIFID CIPHER:**

To decrypt the message to the original one, we use the inverse of key matrix such

\[ K^{-1} = \begin{pmatrix} -2 & 8 & -5 \\ 3 & -11 & 7 \\ 9 & -34 & 21 \end{pmatrix} \]

Now multiplying the inverse matrix with column matrices which generated from matrix operations \( k^{-1} C \mod 26 \). Thus

\[ k^{-1}C = \begin{pmatrix} 2 & 4 & 2 & 5 & 4 & 2 & 5 & 3 & 1 & 5 & 3 & 1 & 5 & 3 \\ 1 & 1 & 3 & 3 & 2 & 3 & 2 & 4 & 2 & 3 & 2 \\ 2 & 3 & 5 & 5 & 2 & 1 & 3 & 5 & 5 & 4 & 2 & 2 & 3 \end{pmatrix} \mod 26 \]

Converting the above matrix in the form of table we get,

<table>
<thead>
<tr>
<th>Table VIII: FINAL CIPHERTEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>

Now, the receiver will decipher the message by using inverse matrix multiplication and Bifid Cipher.
Creating Ciphertext and Decipher using Graph Labeling Techniques

Creating Ciphertext and Decipher using Graph Labeling Techniques

Using Bifid Cipher, the corresponding row and column values are noted down. Our plaintext is recovered after the decryption using additive 6 Caesar Cipher technique.

Then the decrypted message is “a man had good wool bag”.

XI. CONCLUSION

In this paper we have illustrated a new method called Product mod labeling to create edge labels. For making the encryption and decryption of plaintext we use Cipher techniques namely Caesar, Bifid Cipher with usage of matrix multiplication technique. The messages made by this process are difficult to hack by any intruder. We can also extend our work further by applying various Graph labelings to create secret messages with different cryptographic procedures along with matrix applications. Also, further work can be developed by improving the edge labels to maintain secrecy.

APPLICATION

Modular Arithmetic is the main process used in encoding and decoding the messages. The concept of RSA in computer science is implemented using modulo property. Chinese remainder modulo function are used to create crypto systems. Cryptography is used in digital transfer of message through signature, verifying the authentication while signing in any application, integrity of transmitting data in banking sector and electronic money transfer.

REFERENCES


2. Volume 01 – No.60 Issue: 07 Aug 2013, ISSN NUMBER: 2278-9723


AUTHORS PROFILE

B. Deepa, Research Scholar, Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Pallavaram, Chennai-117, Tamilnadu, India. She continues her career in Sindhi Arts and Science College as an Assistant professor in Department of Mathematics since 2013. She has also Guest Lectured in Department of Mathematics at Indira Gandhi Engineering College, Chengalpattu, Tamilnadu. Interesting area in Mathematics is Graph theory, Cryptography. She is now pursuing her Ph.D. in VISTAS, Chennai.

Dr. VMaheswari She is working at Vels Institute of Science, Technology & Advanced Studies (VISTAS) Chennai since 2017 to till date. She completed M.Sc., M.Phil. in Mathematics and her Ph.D. in Graph Theory) Mathematics in Manonmaniyan Sundaranar University, Tirunelveli. She has sixteen years of Teaching experience. Her research interests are Graph Labelings, Cryptography, she has published more than 15 research articles in both National and International journals. She has guided 3MPhil Scholars and is guiding 5Ph.D scholars.
Dr. V. Balaji, was born and brought up at Rajapalayam, Virudhunagar District, Tamil Nadu, India. He completed M.Sc. and M.Phil. Mathematics in ANJAC College (Autonomous) Sivakasi, Virudhunagar District. He did his Ph.D. in (Graph Theory) Mathematics in ManomeManiyam Sundraran University, Tirunelveli. He has 23 years of Teaching experience. He has experience both from Arts and Science; and as well as Engineering colleges. Since 2010 he is teaching at Sacred Heart Arts and Science College (Autonomous). His area of interest in Mathematics are Graph Theory and its applications. He has guided more than 5 MPhil Scholars. He has completed a Minor Project from University Grants Commission.