Mathematics and Statistics 10(2): 431-435, 2022
DOI: 10.13189/ms.2022.100218

http://www.hrpub.org

Data Encryption Using Face Antimagic Labeling and Hill Cipher

B. Vasuki[1,2], **L. Shobana**[1,*], **B. Roopa**[3]

[1]Department of Mathematics, College of Engineering and Technology, Faculty of Engineering and Technology,
SRM Institute of Science and Technology, India

[2]Department of Mathematics, SRM Valliammai Engineering College, India

[3]Department of Mathematics, PERI Institute of Technology, India

Corresponding Author: shobanal@srmist.edu.in

Received January 27, 2022; Revised March 16, 2022; Accepted March 27, 2022

Cite This Paper in the following Citation Styles

***(a)**: [1] B. Vasuki, L. Shobana, B. Roopa, "Data Encryption Using Face Antimagic Labeling and Hill Cipher," Mathematics and Statistics, Vol.10, No.2, pp. 431-435, 2022. DOI: 10.13189/ms.2022.100218*

***(b)**: B. Vasuki, L. Shobana, B. Roopa, (2022). Data Encryption Using Face Antimagic Labeling and Hill Cipher. Mathematics and Statistics, 10(2), 431-435. DOI: 10.13189/ms.2022.100218*

Abstract An approach to encrypt and decrypt messages is obtained by relating the concepts of graph labeling and cryptography. Among the various types of labelings given in [3], our interest is on face antimagic labeling introduced by Mirka Miller in 2003[1]. Baca[2] defines a connected plane graph G with edge set E and face set F as (a,d)- face antimagic if there exist positive integers a and d and a bijection $g : E \to \{1,2,3,\ldots,|E|\}$ such that the induced mapping $\Psi_g : F \to \{a, a+d, \ldots, a+(|F(G)|-1)d\}$, where for a face f, $\Psi_g(f)$ is the sum of all $g(e)$ for all edges e surrounding f is also a bijection.

In cryptography there are many cryptosystems such as affine cipher, Hill cipher, RSA, knapsack and so on. Amongst these, Hill cipher is chosen for our encryption and decryption. In Hill cipher[8], plaintext letters are grouped into two-letter blocks, with a dummy letter X inserted at the end if needed to make all blocks of the same length, and then replace each letter with its respective ordinal number. Each plaintext block P_1P_2 is then replaced by a numeric ciphertext block C_1C_2, where C_1 and C_2 are different linear combinations of P_1 and P_2 modulo 26: $C_1 \equiv aP_1 + bP_2 \pmod{26}$ and $C_2 \equiv cP_1 + dP_2 \pmod{26}$ with condition as $gcd(ad-bc, 26)$ is one. Each number is translated into a cipher text letter which results in cipher text.

In this paper, face antimagic labeling on double duplication of graphs along with Hill cipher is used to encrypt and decrypt the message.

Keywords Encryption, Decryption, Face Antimagic Labeling, Double Duplication Graphs, Hill Cipher

1 Introduction

Labeling is an area in which graph theoretic researchers have shown great interest and have come up with different types of labeling. The concept of face antimagic labeling of plane graphs was introduced by Mirka Miller in 2003[1].

Let $G = (V, E, F)$ be a finite connected plane graph without loops and multiple edges, where V, E and F are its vertex set, edge set and face set respectively. A labeling of type (0,1,0) assigns labels from the set $\{1,2,3,\ldots,|E(G)|\}$ to the edges of a graph G. The weight of a face under this labeling is the sum of the labels of the edges surrounding that face. A labeling of type (0,1,1) assigns labels from the set $\{1,2,3,\ldots,|E(G)+F(G)|\}$ to the edges and faces of a graph G. The weight of a face under this labeling is the sum of the labels of the edges surrounding that face and also the label of the same face.

Recent developments in computer technology and sophisticated techniques in cryptology have revolutionized information security, protecting secret communications over insecure channels such as telephone lines and microwaves from being accessed by unauthorized users. Plaintext is the original message that is to be transmitted in secret form. Ciphertext is its secret version. A cipher is a method of translating plaintext to ciphertext. The key is an explicit formulation of the cipher, so the job of the cryptanalyst is to discover the key and then

break the code. The process of converting plaintext to ciphertext is enciphering (or encrypting). The reverse process by the intended recipient who knows the key is deciphering (or decrypting). Thus, the method used by an unintended receiver to recover the original message is cryptanalysis. In this paper, the graph labeling technique along with hill cipher is used to encrypt and decrypt the message.

In [9], it is proved that the double duplication graph $DD_{VV}(C_m \odot 2P_n), m \geq 4, n \geq 3$ admits (0,1,0) and (0,1,1) face antimagic labeling.

Definition 1.1 *[7] **The double duplication of vertices by edges of a graph** is defined as a duplication of a vertex v_k by an edge $e = v'_k v''_k$ in a graph G produces a graph G', in which $N(v'_k) = \{v_k, v''_k\}$ and $N(v''_k) = \{v_k, v'_k\}$. Again duplication of vertices v_k, v'_k and v''_k by edges $e' = u_k w_k$, $e'' = u'_k w'_k$ and $e''' = u''_k w''_k$ respectively in G' produces a new graph G'' such that, $N(u_k) = \{w_k, v_k\}$, $N(w_k) = \{u_k, v_k\}$, $N(u'_k) = \{w'_k, v'_k\}$, $N(w'_k) = \{u'_k, v'_k\}$, $N(u''_k) = \{w''_k, v''_k\}$ and $N(w''_k) = \{u''_k, v''_k\}$. Double duplication of vertices by edges respectively of a graph G is denoted by $DD_{VV}(G)$.*

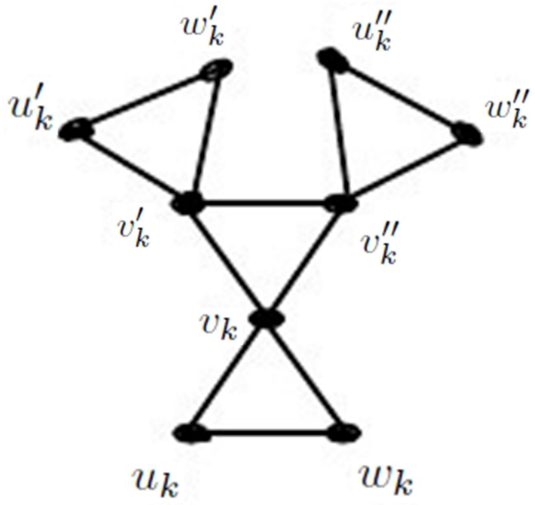

Figure 1. $DD_{VV}(v_k)$

The following definition is taken from [5]

Definition 1.2 *Bi-armed crown $(C_m \odot 2P_n)$, is a graph obtained from a cycle C_m, by identifying the pendant vertices of two vertex disjoint paths of the same length $m-1$ at each vertex of the cycle.*

2 Main Results

In this section, a combinatorial technique to encrypt the original message using face antimagic labeling is obtained. Let G'' be the double duplication of all vertices by edges of the graph $(C_m \odot 2P_n), m \geq 4, n \geq 3$. The graph G'' along with the original message is given as an input. From G'', the number of vertices, edges, faces and the first term of arithmetic progression for three sided faces are obtained which are used as a, b, c and d in Hill cipher cryptosystem to get a sequence of encrypted numbers with the condition that gcd $(ad - bc, 26)$ is one.

Converting these numbers to letters using the normal chart which is given by converting the alphabets A through Z to the numbers 00 to 25 respectively results in the encrypted message. The encrypted message contains two letters in a block. Consider the relation $P \equiv A^{-1}C \pmod{26}$, where $P = \begin{bmatrix} P_1 \\ P_2 \end{bmatrix}$ and $C = \begin{bmatrix} C_1 \\ C_2 \end{bmatrix}$ to decipher such an encrypted message. While decrypting the message, combine the letters to obtain the meaningful words as the letters in the encrypted messages are arranged two in a block.

2.1 Working Algorithm for Encrypting Message

Input: The original message M and $DD_{VV}(C_m \odot 2P_n), m \geq 4, n \geq 3$,
which is face antimagic
Output: The encrypted message E

- Let $G = (C_m \odot 2P_n)$, $n \geq 3$, $m \geq 4$ be a graph with

  $V = \{v_i | 1 \leq i \leq mn\} \cup \{w_i | 1 \leq i \leq mn - m\}$,

  $E = \{v_i v_{i+1} | 1 \leq i \leq mn - 1$ except for $n, 2n, 3n, \ldots, (m-1)n\} \cup \{w_i w_{i+1} | 1 \leq i \leq m(n-1) - 1$ except for $(n-1), (2(n-1), (3(n-1), \ldots, (m-1)(n-1)\} \cup \{v_{ni-n+1} v_{in+1} | 1 \leq i \leq m-1\} \cup \{v_{nm-n+1} v_1\} \cup \{v_{ni-n+1} w_{(i-1)(n-1)+1} | 1 \leq i \leq m\}$ and

  $F = (v_1 v_{n+1} v_{2n+1} \ldots v_{(m-1)n+1} v_1)$.

- Let $G'(V', E', F')$ be the graph obtained from G by duplication of all vertices by edges of G with

  $V' = \{a_i, b_i | 1 \leq i \leq 2mn - m\} \cup V$,

  $E' = \{v_i a_i, v_i b_i, a_i b_i | 1 \leq i \leq mn\} \cup \{w_i a_{mn+i} w_i b_{mn+i}, a_{mn+i} b_{mn+i} | 1 \leq i \leq mn - m\} \cup E$ and

  $F' = \{v_i a_i b_i | 1 \leq i \leq mn\} \cup \{w_i a_{mn+i} b_{mn+i} | 1 \leq i \leq mn - m\} \cup F$.

- Let $G''(V'', E'', F'')$ be the graph obtained from G' by the duplication of all vertices by edge of G' with

  $V'' = \{c_i, d_i, e_i, f_i, g_i, h_i | 1 \leq i \leq 2mn - m\} \cup V'$,

  $E'' = \{c_i d_i, e_i f_i, c_i a_i, b_i f_i, d_i a_i, b_i e_i | 1 \leq i \leq 2mn - m\} \cup \{g_i v_i, v_i h_i, g_i h_i | 1 \leq i \leq$

$mn\} \cup \{w_ig_{mn+i}, w_ih_{mn+i}, g_{mn+i}h_{mn+i} | 1 \leq i \leq mn-m\} \cup E'$ and

$F'' = \{a_ic_id_i, b_ie_if_i | 1 \leq i \leq 2mn-m\} \cup \{g_iv_ih_i | 1 \leq i \leq mn\} \cup \{w_ih_{mn+i}g_{mn+i} | 1 \leq i \leq mn-m\} \cup F'$.

Consider a mapping $g : E'' \cup F'' \rightarrow \{1, 2, 3, ..., 34mn - 17m + 2\}$ as follows:

- For $1 \leq i \leq mn$,
  $g(v_ia_i) = 3i-2; \quad g(v_ib_i) = 3i-1; \quad g(a_ib_i) = 3i.$

For $1 \leq i \leq mn-m$,

$g(w_ia_{mn+i}) = 3mn + 3i - 2;$
$g(w_ib_{mn+i}) = 3mn + 3i - 1;$

$g(b_{i+mn}a_{mn+i}) = 3mn + 3i.$

For $1 \leq i \leq 2mn-m$,

$g(c_ia_i) = 6mn - 3m + 3i - 2;$
$g(d_ia_i) = 6mn - 3m + 3i - 1;$

$g(c_id_i) = 6mn - 3m + 3i;$
$g(b_ie_i) = 12mn - 6m + 3i - 2;$

$g(b_if_i) = 12mn - 6m + 3i - 1;$
$g(f_ie_i) = 12mn - 6m + 3i.$

For $1 \leq i \leq mn$,

$g(g_iv_i) = 18mn - 9m + 3i - 2;$
$g(h_iv_i) = 18mn - 9m + 3i - 1;$

$g(g_ih_i) = 18mn - 9m + 3i.$

For $1 \leq i \leq mn-m$,

$g(w_ig_{mn+i}) = 21mn - 9m + 3i - 2;$
$g(w_ih_{mn+i}) = 21mn - 9m + 3i - 1;$

$g(h_{mn+i}h_{mn+i}) = 21mn - 9m + 3i;$

$g(v_iv_{i+1}) = 24mn - 12m + i$, $1 \leq i \leq mn-1$ except for $n, 2n, 3n, \ldots, (m-1)n$

$g(v_{ni-n+1}v_{ni+1}) = 24mn - 12m + ni$, $1 \leq i \leq m-1$
$g(v_1v_{nm+1-n}) = 25mn - 12m$

$g(w_iw_{i+1}) = 25mn - 12m + i$, $1 \leq i \leq m(n-1)-1$ except for $(n-1), (2(n-1), (3(n-1), \ldots, (m-1)(n-1)$

$g(v_{1+ni-n}w_{1+(i-1)(n-1)}) = 25mn - 12m + i(n-1)$, $1 \leq i \leq m$.

$g(f'_{i1}) = 26mn - 13m + i; 1 \leq i \leq mn;$

$g(f'_{i2}) = 27mn - 13m + i; 1 \leq i \leq mn - m;$

$g(f''_{i1}) = 28mn - 14m + i; 1 \leq i \leq 2mn - m;$

$g(f''_{i2}) = 30mn - 15m + i; 1 \leq i \leq 2mn - m;$

$g(f''_{i3}) = 32mn - 16m + i; 1 \leq i \leq mn;$

$g(f''_{i4}) = 33mn - 16m + i; 1 \leq i \leq mn - m.$

where f'_{i1}, f'_{i2} are the faces obtained from first duplication and $f''_{i1}, f''_{i2}, f''_{i3}, f''_{i4}$ are the faces obtained from second duplication.

- The face labeling of m sided face is $34mn - 17m + 1$. The calculated face weights are as follows

$\beta(f'_{i1}) = g(v_ia_i) + g(a_ib_i) + g(v_ib_i) + g(f'_{i1}) = 26mn - 13m + 10i - 3, 1 \leq i \leq mn$

$\beta(f'_{i2}) = g(w_ia_{mn+i}) + g(w_ib_{mn+i}) + g(b_{i+mn}a_{mn+i}) + g(f'_{i2}) = 36mn - 13m + 10i - 3, 1 \leq i \leq mn - m$

$\beta(f''_{i1}) = g(c_ia_i) + g(d_ia_i) + g(c_id_i) + g(f''_{i1}) = 56mn - 23m + 10i - 3, 1 \leq i \leq 2mn - m$

$\beta(f''_{i2}) = g(b_ie_i) + g(b_if_i) + g(f_ie_i) + g(f''_{i2}) = 66mn - 33m + 10i - 3, 1 \leq i \leq 2mn - m$

$\beta(f''_{i3}) = g(vg_i) + g(v_ih_i) + g(g_ih_i) + g(f''_{i3}) = 86mn - 43m + 10i - 3, 1 \leq i \leq mn$

$\beta(f''_{i4}) = g(w_ig_{mn+i}) + g(w_ih_{mn+i}) + g(h_{mn+i}g_{mn+i}) = 96mn - 43m + 10i - 3$, $1 \leq i \leq mn - m$, which forms an arithmetic progression $\{23mn - 13m + 7, 23mn - 13m + 7 + (1 \times 10), 23mn - 13m + 7 + (2 \times 10), \ldots, 23mn - 13m + 7 + 4[m(2n-1)] \times 10\}$ and the face weight of m sided face is $\frac{m}{2}[49mn - 24m + n] + 34mn - 17m + 1$.

- From the graph $DD_{VV}(C_m \odot 2P_n), m \geq 4, n \geq 3$ number of vertices = $9[m(2n-1)]$, number of edges = $13[m(2n-1)]$, number of faces = $4[m(2n-1)]+1$ and the first term of arithmetic progression for three sided faces = $26mn - 13m + 7$ are calculated.

- Convert the letters in the original message M to its ordinal numbers using the normal chart. Let us assume the obtained sequence of ordinal numbers to be P_1 and P_2 in a block.

- Compute $C_1 \equiv aP_1 + bP_2 \pmod{26}$ and $C_2 \equiv cP_1 + dP_2 \pmod{26}$, where a, b, c and d are the number of vertices, edges,faces and the first term of arithmetic progression for three sided faces of the given graph $DD_{VV}(C_m \odot$

$2P_n), m \geq 4, n \geq 3$, with the condition that $gcd(ad - bc, 26) = 1$.

- Convert each block into a ciphertext numeric block so that the sequence of encrypted numbers is obtained.
- Convert the encrypted numbers into its corresponding letters from the normal chart, resulting in the encrypted message.

2.2 Working Algorithm for Decrypting Message

Input: The received encrypted message E.
Output: The original message M.

- Convert the received encrypted message to ordinal numbers using the normal chart.
- Solve, $P \equiv A^{-1}C \pmod{26}$, where $P = \begin{bmatrix} P_1 \\ P_2 \end{bmatrix}$, $C = \begin{bmatrix} C_1 \\ C_2 \end{bmatrix}$ and $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$
- For every block of C_1 and C_2, we get a unique solution for P_1 and P_2 of the block. Transforming the other block in a similar way yields the numeric string.
- Convert the sequence of numbers obtained into its corresponding letters using normal chart, which in turn result in the original message.

2.3 Illustration

2.3.1 Encryption

Input: The original text SECRET MESSAGE and $DD_{VV}(C_5 \odot 2P_3)$
Output: The encrypted message UA VW DE WS UU AQ DG.

1. Assemble the plaintext into blocks of length two: SE CR ET ME SS AG EX and replace each letter by its cardinal number - 1804 0217 0419 1204 1818 0006 0423. Let us assume the obtained sequence of cardinal numbers to be P_1 and P_2 in a block.
2. From the graph $DD_{VV}(C_5 \odot 2P_3)$ number of vertices = $9[m(2n-1)] = a = 225$, number of edges = $13[m(2n-1)] = b = 325$, number of faces = $4[m(2n-1)]+1 = c = 101$ and The first term of arithmetic progression for three sided faces = $26mn - 13m + 7 = d = 332$ are calculated.
3. Convert each block into a numeric block using the linear system,

   $C_1 \equiv 225P_1 + 325P_2 \pmod{26}$

   $C_2 \equiv 101P_1 + 332P_2 \pmod{26}$,

   For example, $P_1 = 18$ and $P_2 = 04$,

   $C_1 \equiv (225)(18) + (325)(04) \pmod{26}$

   $C_2 \equiv (101)(18) + (332)(04) \pmod{26}$,

   By solving, $C_1 = 20$ and $C_2 = 00$ are obtained.

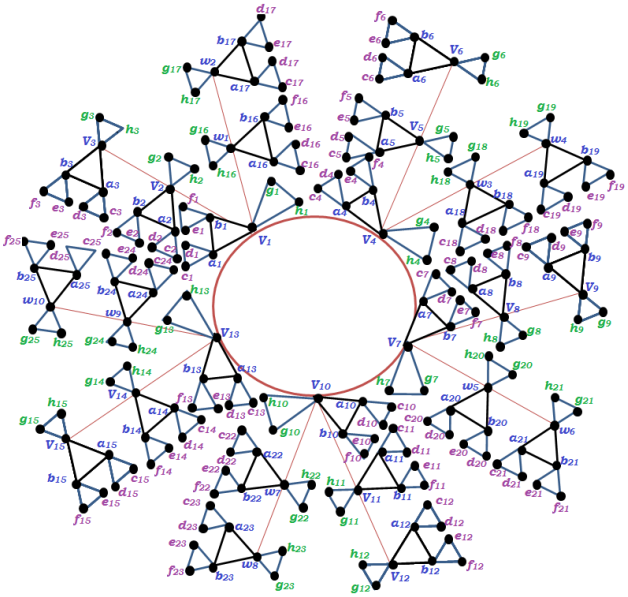

Figure 2. $DD_{VV}(C_5 \odot 2P_3)$

4. Transforming the other blocks in a similar way yields the numeric string - 2000 2122 0304 2218 2020 0016 0306.
5. The cardinal numbers are converted into its corresponding letters, and the resulting ciphertext is - UA VW DE WS UU AQ DG.

2.3.2 Decryption

Input: The received encrypted message UA VW DE WS UU AQ DG
Output: The decrypted message SE CR ET ME SS AG EX

1. Convert the received encrypted message UA VW DE WS UU AQ DG by using normal chart as 2000 2122 0304 2218 2020 0016 0306.
2. Solve the linear system,

$$P \equiv A^{-1}C \pmod{26}, \text{ where } P = \begin{bmatrix} P_1 \\ P_2 \end{bmatrix}, C = \begin{bmatrix} C_1 \\ C_2 \end{bmatrix}$$

   and

$$A = \begin{bmatrix} 225 & 325 \\ 101 & 332 \end{bmatrix}$$

3. For each block of C_1 and C_2, we get a unique solution of P_1 and P_2.

   For example, $C_1 = 20$ and $C_2 = 00$

$$\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \equiv \begin{bmatrix} 225 & 325 \\ 101 & 332 \end{bmatrix}^{-1} \begin{bmatrix} C_1 \\ C_2 \end{bmatrix}$$

$$\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \equiv \begin{bmatrix} 10 & 13 \\ 21 & 15 \end{bmatrix} \begin{bmatrix} 20 \\ 00 \end{bmatrix}$$

On solving, $P_1 = 18$ and $P_2 = 04$ are obtained.

Proceeding in the same manner for the sequence with respect to C, obtain the sequence P.

4. Convert the sequence of numbers - 1804 0217 0419 1204 1818 0006 0423 obtained in to its corresponding letters by using normal chart.
5. The corresponding plain text is SE CR ET ME SS AG EX, that is SECRET MESSAGE.

3 Observation

Cryptography has been an important part of warforce for a longtime. It is a way a military can securely transmit messages without its enemies intercepting the messages. In this way we can encrypt the secret messages along with the graphs. Using face antimagic labeling technique to the given graph the keys for hillcipher can be found for decrypting the message. So this can be the real time exchange of messages between the users of workstations.

4 Conclusion

An approach to encrypt and decrypt the message using Hill cipher cryptosystem along with face antimagic labeling of a double duplication of all vertices by edges of $(C_m \odot 2P_n), m \geq 4, n \geq 3$ is achieved. In future, this technique can be used in electronic banking to maintain the secrecy.

REFERENCES

[1] M. Baca and M. Miller, "On d-antimagic labeling of type (1, 1, 1) for prisms", J. Combin. Main. Combin. Comput., 44, pp 199-207, 2003.

[2] M. Baca, "Face antimagic labeling of convex polytypes", Util, Mam, 55, pp 221-226, 1999.

[3] J. Gallian, "A dynamic survey of graph labeling", The Electronic Journal of Combinatorics, DS6, 2019.

[4] N. Hartsfield and G. Ringel, "Pearls in Graph Theory", Academic Press, Boston – San Diego – New York – London, 1990.

[5] P. Jeyanthi, D. Ramya and P. Thangavelu, "On Super mean graphs", AKCE Journal of Graphs and Combinatorics.6, No-1, pp 103-112, 2009.

[6] Martin Baca, Edy.T.Baskoro, Ljiljana Brankovic, Stanislav Jendrol, Yuqing Lin,Oudone Phanalasy, Joe Ryan, Andrea Semanicova-Fe novcıkova, Slamin, Kiki A.Sugeng, "A survey of face-antimagic evaluations of graphs", Australasian journal of combinatorics, Volume 69(3), pp 382-393, 2017.

[7] Roopa. B, Shobana. L and Kalaiyarasi. R, "On Face Magic Labeling of Duplication of a Tree", Applied Mathematics and Information Sciences, 13, No. S1, pp. 275-278, 2019.

[8] Thomas Kohsy, "Elementary Number Theory with Applications", Second Edition, Academis Press,Elsevier, 2007.

[9] B. Vasuki and L. Shobana, "Face Antimagic Labeling for Double Duplication of Barycentric and Middle graphs", Iraqi Journal of Science [Accepted].