A New Algorithm for Encryption and Decryption Using AUM Block Sum Labeling

A. Uma Maheswari and C. Ambika

1 Introduction

The theory of cryptography is developing rapidly in recent years. The appropriate integration of the cryptographic technique with the graph labeling [1] helps to ensure safe communication by preventing the intrusion of any secret messages during conversion. In 1949, Shannon [2] made a proposal for modern cryptography. In [3], Gallian gave a review of graph labeling. Uma Maheswari and Azhagarasi [4] established the concept of AUM block labeling. AUM block sum labeling is the new block labeling technique developed in the scope for applications to heterogeneous field. In [5–11], the discussion of AUM block sum labeling for various graph families is given. New encoding and decoding methods involving AUM block sum labeling are presented in [12, 13]. Here, we present a new technique using AUM block sum labeling on any block graph by relating the numbers into the perfect square number. A key is required to ensure confidentiality during the encryption and decryption operations. Here, we have given a key as a matrix form, ensuring more secure transmission.

2 Preliminaries

We present the basic graph theory and cryptography concepts relevant for the proposed technique in this part.

A. U. Maheswari
PG & Research Department of Mathematics, Quaid-E-Millath Government College for Women (Autonomous), Chennai, India

C. Ambika (✉)
Department of Mathematics, Ethiraj College for Women, Chennai, India
e-mail: ambika_c@ethirajcollege.edu.in

J. K. Mandal et al. (eds.), *Proceedings of International Conference on Network Security and Blockchain Technology*, Lecture Notes in Networks and Systems 738,
https://doi.org/10.1007/978-981-99-4433-0_5

2.1 Definition: Block Graph [14, 15]

A maximal non-separable subgraph of the graph is the block graph of G.

2.2 Definition: Triangular Snake Graph [16]

The triangular snake T_n is a graph that is obtained by replacing each edge of the path graph P_n with a triangle C_3.

2.3 Definition: Plain Text [17]

The original message that the sender desires to communicate to the receiver is in plain text.

2.4 Definition: Cipher Text [17]

The encrypted message that contains the plain text in an unreadable format is called cipher text.

2.5 Definition: Encryption [17]

Encryption is the process of converting plain text into cipher text. A key and an encryption algorithm is needed for the encryption process.

2.6 Definition: Decryption [17]

Decryption is the process of reversing encryption. It is the transformation of cipher text into plain text. A decryption algorithm and a key are needed for the decryption process.

2.7 Definition: Key [17]

A key is a particular symbol or a text with numbers or letters. The key is used to encrypt plain text and decrypt cipher text, respectively.

2.8 Definition: AUM Block Sum Labeling [4]

Consider a graph G with p vertices and a vertex set $V(G)$, q edges and an edge set $E(G)$ and block set with b blocks, $p, q, b \geq 1$.

We say that the graph G admits AUM block sum labeling if there exists a bijection. $f : V(G) \to \{1, 2, 3, \ldots p\}$ and $f^* : E(G) \to Z^+$ induced from f by $f^*(uv) = f(u) + f(v)$ and $f^{**} : B(G) \to Z^+$ defined as follows:

Let B_j be incident with the vertices $v_{j_1}, v_{j_2}, \ldots..v_{j_k}, 1 \leq j_k \leq p$ and edges $e_{j_1}, e_{j_2}, \ldots e_{j_m}, 1 \leq j_m \leq q$.

Then, $f^{**}(B_j) = \sum_{i=1}^{k} f(v_{j_i}) + \sum_{i=1}^{m} f^*(e_{j_i})$ and $f^{**}\left(B_j\right) \neq f^{**}(B_i)$ for $1 \leq i, j \leq b$ and $i \neq j$.

2.9 AUM Block Sum Labeling - Triangular Snake Graph [4]

Consider the triangular snake graph, $T_n, n \geq 2$.

Define $f^{**} : B(T_n) \to Z^+$ by $f^{**}(B_i) = 18i, 1 \leq i \leq n-1$.

For $i \neq j$, $f^{**}\left(B_j\right) \neq f^{**}(B_i)$ as $18j \neq 18i$ implying the block labels $f^{**}(B_i)$ are distinct.

3 Main Results

3.1 New Encryption and Decryption Algorithm with Illustration

In [13], we have presented various coding algorithms based on the concept of relating numbers to geometric mean to encode and decode a message. In this section, we devise a new encryption and decryption algorithm by taking any block graph and assign AUM block sum labeling in the beginning to encode the message. For the illustration, we have considered the triangular snake graph T_{n+1}.

3.2 Encryption Algorithm

- Consider any block graph with n blocks and assign AUM block sum labeling where n indicates message length. The block labels are served as a key in the first row of the matrix.
- Assign numbers from 0 to 25 to the alphabets in the order of 0, 1, 2, … 12 to *N*, *O*… *Z* and 13, 14, … 25 to *A*, *B*, *C*, … *M*.
- Find the corresponding number for each alphabet using the encoding table and take it as x_i for $i = 1, 2, 3\ldots n$.
- Find any positive integer y_i to make $x_i + y_i = z_i$ for $i = 1, 2, 3 \ldots n$ a perfect square number. The numbers y_i are the second row of the key matrix.
- Find the difference between the block label B_i and z_i, i.e., $w_i = (B_i - z_i)(\text{mod}26)$ for $i = 1, 2, 3 \ldots n$.
- Find the alphabet corresponding to each w_i for $i = 1, 2, 3 \ldots n$.
- Send the sequence of the text w_i as cipher text for decryption.

Key

The key is the matrix with 2 rows and n (message length) columns containing block labels in the first row and values of $y_i's$ in the second row.

Decryption Algorithm

- From the cipher text, using the encoding table, determine the number that represents each character, and take it as w_i for $i = 1, 2, 3 \ldots n$.
- Find $z_i = (B_i - w_i)(\text{mod}26)$ for $i = 1, 2, 3 \ldots n$.
- Using key numbers y_i, find $x_i = z_i - y_i$ for $i = 1, 2, 3 \ldots n$.
- Find the alphabet that corresponds to each x_i to get the plain text through the encoding table.

Illustration I

Encryption

Consider the plain text "**RAINBOW**", which is to be converted.

The message length is 7.

Therefore, consider the triangular snake graph T_8 with 7 blocks.

AUM block sum labeling in triangular snake graph T_8 is given in Fig. 1.

Find the corresponding number for each alphabet using the encoding table.

R	A	I	N	B	O	W
4	13	21	0	14	1	9

Denote $x_1 = 4,\ x_2 = 13,\ x_3 = 21,\ x_4 = 0,\ x_5 = 14,\ x_6 = 1,\ x_7 = 9.$

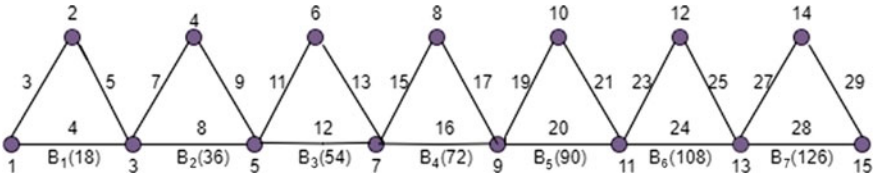

Fig. 1 T_8 AUM block sum labeling

Table 1 Encoding table

A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12

Find any positive integer y_i to make $x_i + y_i = z_i$ for $i = 1, 2, 3 \ldots 7$ a perfect square number.

Therefore,

$$x_1 + y_1 = 4 + 5 = 9 = z_1$$

$$x_2 + y_2 = 13 + 3 = 16 = z_2$$

$$x_3 + y_3 = 21 + 4 = 25 = z_3$$

$$x_4 + y_4 = 0 + 1 = 1 = z_4$$

$$x_5 + y_5 = 14 + 2 = 16 = z_5$$

$$x_6 + y_6 = 1 + 3 = 4 = z_6$$

$$x_7 + y_7 = 9 + 7 = 16 = z_7$$

The values of y_i are 5, 3, 4, 1, 2, 3, 7.

Find the difference between the block label B_i and z_i.

$$\text{i.e., } w_i = (B_i - z_i)(\text{mod}26) \text{ for } i = 1, 2, 3 \ldots 7.$$

$$w_1 = (B_1 - z_1)(\text{mod}26) = (18 - 9)(\text{mod } 26) = 9$$

$$w_2 = (B_2 - z_2)(\text{mod}26) = (36 - 16)(\text{mod}26) = 20$$

$$w_3 = (B_3 - z_3)(\text{mod } 26) = (54 - 25)(\text{mod}26) = 3$$

$$w_4 = (B_4 - z_4)(\text{mod } 26) = (72 - 1)(\text{mod } 26) = 19$$

$$w_5 = (B_5 - z_5)(\text{mod } 26) = (90 - 16)(\text{mod } 26) = 22$$

$$w_6 = (B_6 - z_6)(\text{mod } 26) = (108 - 4)(\text{mod } 26) = 0$$

$$w_7 = (B_7 - z_7)(\text{mod}26) = (126 - 16)(\text{mod}26) = 6$$

From the encoding table, the letters that correspond to the above numbers are WHQGJNT.

Therefore, the cipher text for the given message is WHQGJNT.

$$\textbf{Key}: \begin{bmatrix} 18 & 36 & 54 & 72 & 90 & 108 & 126 \\ 5 & 3 & 4 & 1 & 2 & 3 & 7 \end{bmatrix}$$

Decryption

Apply the above decryption procedure to the encrypted text you received to retrieve the plain text.

From the cipher text, the message length is 7.

Here, the cipher text is WHQGJNT.

Using the encoding table, identify the number that each character corresponds to and take it as

$$y_i \text{ for } i = 1, 2, 3 \ldots 7.$$

W	H	Q	G	J	N	T
9	20	3	19	22	0	6

Take $w_1 = 9,\ w_2 = 20,\ w_3 = 3,\ w_4 = 19,\ w_5 = 22,\ w_6 = 0,\ w_7 = 6.$
Find $z_i = (B_i - w_i)(\text{mod}26)$ for $i = 1, 2, 3 \ldots 7.$

$$z_1 = (B_1 - w_1)(\text{mod}26) = (18 - 9)(\text{mod}26) = 9$$

$$z_2 = (B_2 - w_2)(\text{mod}26) = (36 - 20)(\text{mod } 26) = 16$$

$$z_3 = (B_3 - w_3)(\text{mod}26) = (54 - 3)(\text{mod}26) = 25$$

$$z_4 = (B_4 - w_4)(\text{mod}26) = (72 - 19)(\text{mod}26) = 1$$

$$z_5 = (B_5 - w_5)(\text{mod } 26) = (90 - 22)(\text{mod}26) = 16$$

$$z_6 = (B_6 - w_6)(\text{mod}26) = (108 - 0)(\text{mod}26) = 4$$

$$z_7 = (B_7 - w_7)(\text{mod}26) = (126 - 6)(\text{mod}26) = 16$$

Consider the second row of the key matrix, 5, 3, 4, 1, 2, 3, 7, as the values of y_i. Find $x_i = z_i - y_i$ for $i = 1, 2, 3 \ldots 7$ where y_i's are key numbers.

$$x_1 = z_1 - y_1 = 9 - 5 = 4$$

$$x_2 = z_2 - y_2 = 16 - 3 = 13$$

$$x_3 = z_3 - y_3 = 25 - 4 = 21$$

$$x_4 = z_4 - y_4 = 1 - 1 = 0$$

$$x_5 = z_5 - y_5 = 16 - 2 = 14$$

$$x_6 = z_6 - y_6 = 4 - 3 = 1$$

$$x_7 = z_7 - y_7 = 16 - 7 = 9$$

Using the encoding table, we can infer that the plain text represented by the above numbers is "**RAINBOW**".

4 Conclusion

We devised a unique algorithm for the transmission of plain text into cipher text and vice versa. AUM block sum labeling on any block graph and a perfect square number are integrated in this coding for transmission. A triangular snake graph is considered

for the illustration. The theory developed can be further extended to other standard graphs by employing new coding techniques.

References

1. Ni B, Qazi R, Rehman SU, Farid G (2021) Some graph-based encryption schemes. J Math 2021:1–8. Article ID 6614172
2. Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Tech J 28(4):656–715
3. Gallian JA (2021) A dynamic survey of graph labeling. Electron J Comb
4. Uma Maheswari A, Azhagarasi S (2022) New labeling for graphs-AUM block sum labeling. Int J Curr Sci 12(1):574–584. ISSN: 2250-1770
5. Uma Maheswari A, Azhagarasi S (2022) AUM block labeling for cycle cactus block graphs. Compl Eng J 13(4):84–96
6. Uma Maheswari A, Azhagarasi S (2002) AUM block sum labeling for some special graphs. Int J Mech Eng 7(Special Issue 5):102–110. ISSN: 0974-5823
7. Uma Maheswari A, Bala Samuvel J (2022) New coloring for blocks—AUM block coloring for standard graphs. J Compl Eng J 13(5):68–77. ISSN: 0898-3577
8. Uma Maheswari A, Azhagarasi S (2022) AUM block sum labelling & AUM block labelling for perfect binary tree $T_{(3,1)}$ $T_{(4,1)}$ & $T_{(5,1)}$. In: Advances in graph labelling, colouring and power domination theory, vol 1. NFED Publications, pp 1–17. E-ISBN: 978-81-95499-8-5
9. Uma Maheswari A, Bala Samuvel J (2022) AUM block coloring for triangular snake graph family. In: Advances in graph labelling, colouring and power domination theory, vol 1. NFED Publications, pp 72–91. E-ISBN: 978-81-95499-8-5
10. Uma Maheswari A, Purnalakshimi AS (2022) Aum block labelling for friendship, tadpole and cactus graphs. Neuro Quantol 20(6):7876–7884. eISSN 1303-5150
11. Uma Maheswari A, Purnalakshimi AS (2022a) AUM block labelling for snake graphs and Dutch windmill graph. Neuro Quantol 20(9):414–421
12. Uma Maheswari A, Azhagarasi S (2022) A new algorithm for encoding and decoding using Aum block labelling. Compl Eng J 13(4):264–274. ISSN No: 0898-3577
13. Uma Maheswari A, Ambika C (2022) New coding algorithms using AUM block SUM labeling. Neuro Quantolgy 20(9):377–385. eISSN 1303-5150
14. Bondy JA, Murty USR (1976) Graph theory with applications. Elsevier Science Publishing Co., Inc., pp 1–264. ISBN: 0-444-19451-7
15. Harary F (1972) Graph theory. Addison-Wesley, Reading, Mass
16. Ponraj R, Sathish Narayanan S (2013) Difference cordiality of some graphs obtained from double alternate snake graphs. Global J Math Sci Theory Pract 5(2013):167–175
17. Agrawal M, Mishra P (2012) A comparative survey on symmetric key encryption techniques. Int J Comput Sci Eng 4(05):877–882. ISSN: 0975-3397