BAREKENG: Journal of Mathematics and Its Applications
March 2023 Volume 17 Issue 1 Page 0029–0036
P-ISSN: 1978-7227 E-ISSN: 2615-3017
https://doi.org/10.30598/barekengvol17iss1pp0029-0036

ON SUPER $(3n + 5, 2) -$ EDGE ANTIMAGIC TOTAL LABELING AND IT'S APPLICATION TO CONSTRUCT HILL CIPHER ALGORITHM

Rafiantika Megahnia Prihandini*[1,2], Robiatul Adawiyah[1,3]

[1]*Department of Mathematics Education, University of Jember, Indonesia*
[2]*SCOpe Research Group, University of Jember, Indonesia*
[3]*CoMed Research Group, University of Jember, Indonesia*

Jl. Kalimantan Tegalboto, No. 37, Krajan Timur, Sumbersari, Kec. Sumbersari, Kabupaten Jember,
Jawa Timur, 68121, Indonesia

*Corresponding author's e-mail:*rafiantikap.fkip@unej.ac.id*

ABSTRACT

Article History:

Received: 16th July 2022
Revised: 8th November 2022
Accepted: 7th January 2023

Keywords:

Graph Labeling;
$\boldsymbol{GShack(TB_2, v, n)}$;
Hill Cipher.

Graph labeling can be implemented in solving problems in various fields of life. One of the applications of graph labeling is in security systems. Information security is needed to reduce risk, data manipulation, and unauthorized destruction or destruction of information. Cryptographic algorithms can be used to build security systems. One of the cryptographic algorithms is Hill Cipher. Hill Cipher is a cryptographic algorithm that uses a matrix as a key to perform encryption, decryption, and modulo arithmetic. This study discusses the use of Super (3n+5,2)- edge antimagic total labeling to construct the Hill Cipher algorithm. The variation of the edge weight function and the corresponding edge label on the $GShack(TB_2, v, n)$ graph, will make the constructed lock more complicated to hack.

How to cite this article:

R. M. Prihandini and R. Adawiyah, "ON SUPER $(3n + 5,2) -$ EDGE ANTIMAGIC TOTAL LABELING AND IT'S APPLICATION TO CONSTRUCT HILL CIPHER ALGORITHM," *BAREKENG: J. Math. & App.*, vol. 17, iss. 1, pp. 0029-0036, March, 2023.

Journal homepage: *https://ojs3.unpatti.ac.id/index.php/barekeng/*
Journal e-mail: *barekeng.math@yahoo.com; barekeng.journal@mail.unpatti.ac.id*

Research Article • Open Access

1. INTRODUCTION

There are various topics in graph theory. One of them is graph labeling. The concept of labeling graphs was first introduced by Sedlacek in 1964. The concept of labeling initially discussed the objects of a graph which were usually represented by vertices and edges, and there was a set of natural numbers called labels [1]. Graph labeling continued to develop so that new scientists emerged who discussed graph labeling, including Stewart in 1966 and Kotzig and Rosa in 1970. The label on the concept of graph labeling is an injective mapping that maps a set of vertex and or a set of edges to a set of natural numbers [2]. Labeling on a graph is distinguished based on the selection of the domain. If the domain is a vertex then it is called vertex labeling; if the domain is an edge then it is called edge labeling; and if the selected domain is vertex and edge, then it is called total labeling [3]. The labels that are known to date include harmony labeling, graceful labeling, total irregular labeling, magic labeling, and antimagic labeling. In the development of magic labeling, there are also known magic-vertex total labeling, super magic vertex total labeling, edge-magic total labeling, and super-magic edge total labeling [4]. Hsiao has also conducted research related to antimagic labeling, his research discusses the new class of sparse antimagic graphs built through Cartesian products and lexicographic products [5]. Other research related to labeling on graphs can also be seen in [6] and [7].

Graph labeling can be implemented to solve problems in various fields, one of them is a security system. Information security is needed to reduce risk, data manipulation, and unauthorized destruction or destruction of information [8]. The aspects that must be met in information security include aspects of confidentiality, data integrity, and availability [9]. One technique that can guarantee the confidentiality of the information communicated is cryptography. The information to be conveyed will be protected because the original message will be converted into a cipher message using a certain key so that this message cannot be known by parties who have no interest. There are several cryptographic algorithms that can be used to build a security system, one of which is Hill Cipher. Hill Cipher was created by Lester S. Hill in 1929. Hill Cipher is a cryptographic algorithm that uses a matrix as a key to perform encryption, decryption, and modulo arithmetic. Each character in the plaintext and ciphertext is converted into numbers [4]. The encryption process is carried out by multiplying the key matrix with the plaintext matrix while the decryption process is carried out by multiplying the inverse of the key matrix with the ciphertext. Therefore, in the Hill Cipher algorithm, the only matrix that can be used is a square matrix. The use of a matrix as a key makes the Hill Cipher algorithm difficult to solve [10]. Several studies related to the use of the Hill Cipher algorithm include [5], [11]–[13].

Previously, there have been several studies related to the use of SEATL in building cryptosystems. Mulisatul et al. [14] showed that $Shack(F_6, c_4^1, n)$ admit a Super (a, d)- Edge Antimagic Total Labeling for $d = 0,1,2$. It was also concluded that the labeling on the Shack graph $Shack(F_6, c_4^1, n)$ can be used to develop a polyalphabetic cryptosystem. Muhlisatul et al. have also analyzed the SEATL linkage of connecting and disconnecting graphs as well as applications in the development of a polyalphabetic cipher cryptosystem. Another research related to the development of a cryptosystem from graph labeling is the implementation of the ciphertext polyalphabetic cryptosystem for super labeling $(a, d) - P_2 \rhd H$ - antimagic total covering of graph $G = C_5 \rhd W_5$ by using the cipher block chaining (CBC) method [15]. Based on this description, to increase the security of the key in the Hill Cipher algorithm, the key to be used is a label obtained from the Super $(3n+5,2) -$ Edge Antimagic Total Labeling of the $GShack(TB_2, v, n)$ graph.

2. RESEARCH METHODS

The method used is the axiomatic deductive method. The axiomatic deductive method is used by deriving existing theorems and lemmas and then applying them to Super (a, d)- Edge Antimagic Total Labeling on a $GShack(TB_2, v, n)$ connected graph. After that, the use of the Hill Cipher algorithm will be developed for the secret messages from the labels found. The Hill Cipher algorithm consists of two processes, namely, the encryption process and the decryption process. The following is the research flow:

a. Determine the cardinality of the vertices and edges of the graph $GShack(TB_2, v, n)$;
b. Determine the upper bound of the difference d;
c. Determine the labels of the vertices and edges of the graph $GShack(TB_2, v, n)$;
d. Determine the cardinality of the vertices and edges of the graph $GShack(TB_2, v, n)$;
e. Develop a bijective function of vertex label, edge label, and edge total weight function;

f. Proving the truth of the function and developing a theorem;

g. Determining the Hill Cipher algorithm. The steps of forming the Hill Cipher algorithm are as follows:
   - Converting each character to a number;
   - Developing the key. The key of Hill Cipher is a matrix $m \times m$ with m as the size of a block. Matrix K that becomes the key must fulfill the requirement as follow: The matrix must be invertible, which means that the matrix must have an inverse K^{-1} thus: $K.K^{-1} = I$ and the value of the determinant of the matrix must be coprime / relatively prime to 26;
   - Encryption Process: $C = KP \ mod \ 26$ with $C =$ Ciphertext, K= key and P =Plaintext;
   - Decryption Process: $P = K^{-1}C \ mod \ 26$.

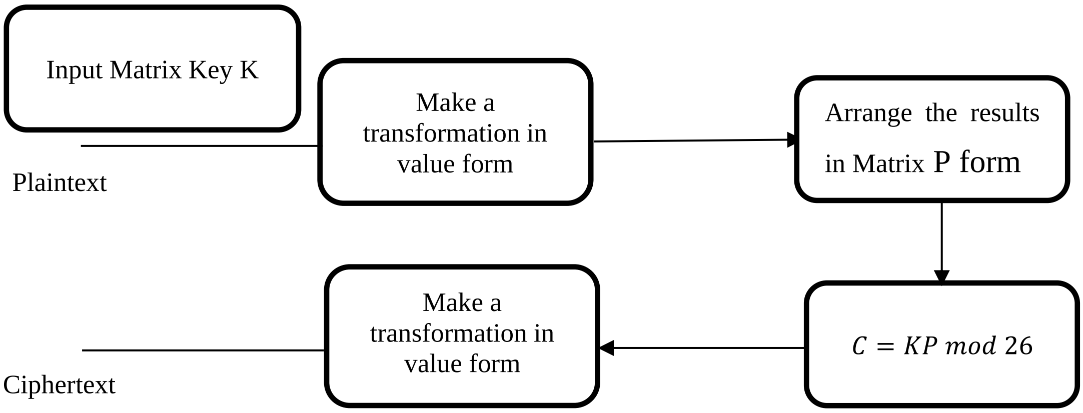
Input Matrix Key K
Plaintext
Make a transformation in value form
Arrange the results in Matrix P form
Make a transformation in value form
Ciphertext
$C = KP \ mod \ 26$

Figure 1. Illustration of Hill Cipher Encryption

3. RESULTS AND DISCUSSION

In this section, we explain the research results, which contain one lemma, one theorem, and the step for developing Super $(a, d) -$ Edge Antimagic Total Labeling in constructing Hill Cipher Algorithm.

Lemma 1. If a Generalized Shackle of Triangular Book Graph, $GShackle(TB_2, v, n)$, admits a super (a, d)-edge-antimagic total labeling then $d \leq 2$.

Proof. The first step in proving Lemma 1, we assume that a $GShackle(TB_2, v, n)$ admits a super (a, d)-edge-antimagic total labeling with a bijective function: $f: V(G) \cup E(G) \to \{1,2, \ \ldots, p + q\}$ and the set of edge weights: $\{a, a + d, a + 2d, \ldots a + (q - 1)d\}$. $GShackle(TB_2, v, n)$ is the development of shackle operation of n graph Triangular Book then we assign all of the vertices y_{i+1} and z_i connected of with an edge, thus there $n - 1$ edge addition. The set of edge and vertex of $GShackle(TB_2, v, n)$ are as follows:

$V = \{x_i \mid 1 \le i \le n+1\} \cup \{y_i \mid 1 \le i \le n\} \cup \{z_i \mid 1 \le i \le n\}$ dan $E = \{x_i y_i \mid 1 \le i \le n\} \cup \{x_i z_i \mid 1 \le i \le n\}$ $\cup \{y_i z_i \mid 1 \le i \le n\} \cup \{x_{i+1} y_i \mid 1 \le i \le n\} \cup \{x_{i+1} z_i \mid 1 \le i \le n\} \cup \{y_{i+1} z_i \mid 1 \le i \le n-1\}$. Hence, we got the cardinality of the vertex and the edge as follows: $|V| = p = 3n+1$ and $|E| = q = 6n-1$. The lower bound of d is $d \le \dfrac{2p+q-5}{q-1} \Leftrightarrow d \le \dfrac{2(3n+1)+(6n-1)-5}{(6n-1)-1} \Leftrightarrow d \le 2 \ldots$□ .

Theorem 1. If $n \geq 2$ then $GShackle(TB_2, v, n)$ admits a super $(3n + 5, 2)$-edge-antimagic total labeling.

Proof. The determination of the vertex label and edge label of $GShackle(TB_2, v, n)$ is the first step of this research. The edge and vertex label of $GShackle(TB_2, v, n)$ is a bijective function, which means one-to-one mapping of the domain in the form of vertices and edges of the graph $GShackle(TB_2, v, n)$ into the codomain in this case, is a positive integer. The bijective function of vertex labeling and edge labeling of $GShackle(TB_2, v, n)$ are as follows:

$$\begin{aligned} g(x_i) &= 3i-2 & g(x_i y_i) &= 3n+6i-4 \\ g(y_i) &= 3i-1 & g(x_i z_i) &= 3n+6i-3 \\ g(z_i) &= 3i & g(y_i z_i) &= 3n+6i-2 \\ & & g(y_i x_{i+1}) &= 3n+6i-1 \\ & & g(z_i x_{i+1}) &= 3n+6i \\ & & g(z_i y_{i+1}) &= 3n+6i+1 \end{aligned}$$

After we got the vertex label of $GShackle(TB_2, v, n)$, then we got the edge weight function of graph G. The edge weight function is the addition of two vertex labels with the corresponding edges. We can see the edge weight function of $GShackle(TB_2, v, n)$ in the following formula:

$$\begin{aligned} wg(x_i y_i) &= 12i + 3n - 7 \\ wg(x_i z_i) &= 12i + 3n - 5 \\ wg(y_i z_i) &= 12i + 3n - 3 \\ wg(y_i x_{i+1}) &= 12i + 3n - 1 \\ wg(z_i x_{i+1}) &= 12i + 3n + 1 \\ wg(z_i y_{i+1}) &= 12i + 3n + 3 \end{aligned}$$

From the edge weight function of $GShackle(TB_2, v, n)$, we can easily show that the smallest weight of $GShackle(TB_2, v, n)$ lies on $wg(x_1 y_1)$ which is $15n + 1$. Thus, it can be shown that the edge weight function of $GShackle(TB_2, v, n)$ form the arithmetic sequence with the arrangement as follow: $wg = \{3n + 5, 3n + 7, 3n + 9, \ldots, 15n + 1\}$. The difference is $d = 2$. Thus, it can be concluded that $GShackle(TB_2, v, n)$ admits a super $(3n + 5, 2)$-edge-antimagic total labeling □. The super $(3n + 5,2)$-edge-antimagic total labeling of $GShackle(TB_2, v, 4)$ shown in Figure 2.

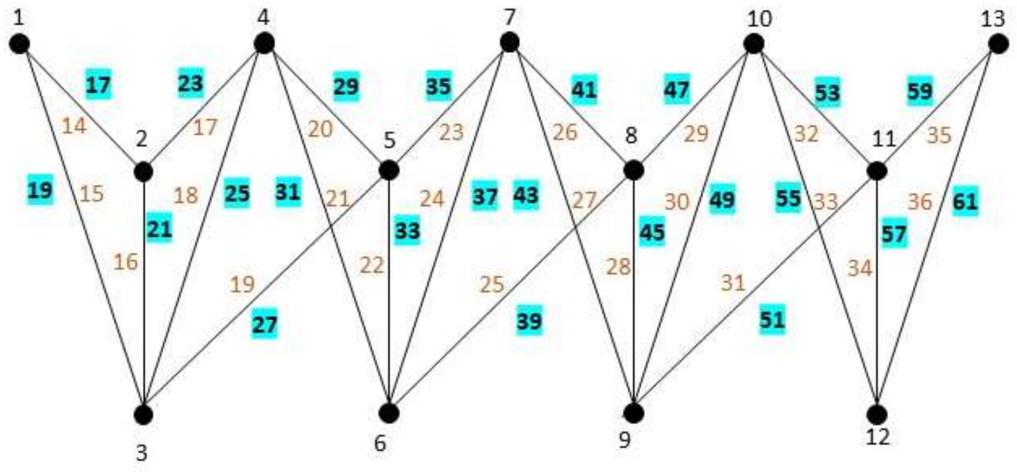

Figure 2. The Super $(3n + 5, 2)$-edge-antimagic total labeling of $GShackle(TB_2, v, 4)$

Furthermore, it will be explained the implementation of labeling on the $GShackle(TB_2, v, 4)$ graph to construct the Hill Cipher Algorithm both from the encryption process and the decryption process. Suppose we choose the plaintext **"INDONESIAMERDEKA"**. The modulus used to retrieve the letter index values for plaintext and cipher text uses an A-Z alphabetical arrangement, namely modulo 26. The conversion of alphabets into numbers can be seen in Table 1.

Table 1. Letter index number

A	B	C	D	E	F	G	H	I	J	K	L	M	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	13	14	15	16	17	18	19	20	21	22	23	24	25

The matrix key ordo 2×2 taken from the value of d in Super $(3n+5,2)$-edge-antimagic total labeling of $GShackle(TB_2, v, 4)$ which is $d = 2$. The element of the matrix taken from the smallest first weight and the corresponding edges thus the requirement of $K \times K^{-1} = I$ and $GCD(\det K, 26) = 1$ are fulfilled. Here is the matrix key (K):

$$K = \begin{bmatrix} 15 & 14 \\ 17 & 19 \end{bmatrix}$$

It can be proven that $K \times K^{-1} = I$ and $GCD(\det K, 26) = 1$.

$$K^{-1} = \begin{bmatrix} \frac{19}{47} & -\frac{14}{47} \\ -\frac{17}{47} & \frac{15}{47} \end{bmatrix} \rightarrow KK^{-1} = \begin{bmatrix} 15 & 14 \\ 17 & 19 \end{bmatrix} \begin{bmatrix} \frac{19}{47} & -\frac{14}{47} \\ -\frac{17}{47} & \frac{15}{47} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$$\det K = ad - bc = 285 - 238 = 47 \rightarrow GCD(\det K, 26) = GCD(47, 26) = 1$$

The first step is arranging the plaintext by following the key block because the selected key matrix has the order of 2×2, then the plaintext was placed in eight blocks, each block consisting of two letters.

Table 2. The place of plaintext in the key block

I N	D O	N E	S I	A M	E R	D E	K A
Block Matrix 1	Block Matrix 2	Block Matrix 3	Block Matrix 4	Block Matrix 5	Block Matrix 6	Block Matrix 7	Block Matrix 8

The second step is converting letters into numbers modulo 26. The given plaintext is converted into numbers using the data in Table 1.

Table 3. Converting letters to numbers

I	N	D	O	N	E	S	I	A	M	E	R	D	E	K	A
8	13	3	14	13	4	18	8	0	7	4	17	3	4	10	0
p_0		p_1		p_2		p_3		p_4		p_5		p_6		p_7	
Block Matrix 1		Block Matrix 2		Block Matrix 3		Block Matrix 4		Block Matrix 5		Block Matrix 6		Block Matrix 7		Block Matrix 8	

The third step is performing the Encryption Process. The formulation in the encryption process is $C = KP$

$$c_0 = \begin{bmatrix} 15 & 14 \\ 17 & 19 \end{bmatrix} \begin{bmatrix} 8 \\ 13 \end{bmatrix} \bmod 26 = \begin{bmatrix} 302 \\ 383 \end{bmatrix} = \begin{bmatrix} 16 \\ 19 \end{bmatrix}$$

$$c_1 = \begin{bmatrix} 15 & 14 \\ 17 & 19 \end{bmatrix} \begin{bmatrix} 3 \\ 14 \end{bmatrix} \bmod 26 = \begin{bmatrix} 241 \\ 317 \end{bmatrix} = \begin{bmatrix} 7 \\ 5 \end{bmatrix}$$

$$c_2 = \begin{bmatrix} 15 & 14 \\ 17 & 19 \end{bmatrix} \begin{bmatrix} 13 \\ 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 251 \\ 297 \end{bmatrix} = \begin{bmatrix} 17 \\ 11 \end{bmatrix}$$

$$c_3 = \begin{bmatrix} 15 & 14 \\ 17 & 19 \end{bmatrix} \begin{bmatrix} 0 \\ 7 \end{bmatrix} \bmod 26 = \begin{bmatrix} 382 \\ 458 \end{bmatrix} = \begin{bmatrix} 18 \\ 16 \end{bmatrix}$$

$$c_4 = \begin{bmatrix} 15 & 14 \\ 17 & 19 \end{bmatrix} \begin{bmatrix} 4 \\ 17 \end{bmatrix} \bmod 26 = \begin{bmatrix} 98 \\ 133 \end{bmatrix} = \begin{bmatrix} 20 \\ 3 \end{bmatrix}$$

$$c_5 = \begin{bmatrix} 15 & 14 \\ 17 & 19 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 298 \\ 391 \end{bmatrix} = \begin{bmatrix} 12 \\ 1 \end{bmatrix}$$

$$c_6 = \begin{bmatrix} 15 & 14 \\ 17 & 19 \end{bmatrix} \begin{bmatrix} 10 \\ 0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 101 \\ 127 \end{bmatrix} = \begin{bmatrix} 23 \\ 23 \end{bmatrix}$$

$$c_7 = \begin{bmatrix} 15 & 14 \\ 17 & 19 \end{bmatrix} \begin{bmatrix} 8 \\ 13 \end{bmatrix} \bmod 26 = \begin{bmatrix} 150 \\ 170 \end{bmatrix} = \begin{bmatrix} 20 \\ 14 \end{bmatrix}$$

Then, we determine the ciphertext.

Table 4. Ciphertext

c_0		c_1		c_2		c_3		c_4		c_5		c_6		c_7	
16	**19**	**7**	**5**	**17**	**11**	**18**	**16**	**20**	**3**	**12**	**1**	**23**	**23**	**20**	**14**
Q	**T**	**H**	**F**	**R**	**L**	**S**	**Q**	**U**	**D**	**M**	**B**	**X**	**X**	**U**	**O**
Block Matrix 1		Block Matrix 2		Block Matrix 3		Block Matrix 4		Block Matrix 5		Block Matrix 6		Block Matrix 7		Block Matrix 8	

The second process is the decryption process. The decryption process is the process of converting ciphertext into plaintext. This process begins by calculating the inverse of the key matrix K

$$K^{-1} = \frac{1}{\det K} \bmod 26 \begin{bmatrix} 19 & -14 \\ -17 & 15 \end{bmatrix} = \frac{1}{21} \bmod 26 \begin{bmatrix} 19 & -14 \\ -17 & 15 \end{bmatrix}$$

After that, we calculate the modular invers

$$(21\times 0) \bmod 26 = 0$$
$$(21\times 1) \bmod 26 = 21$$
$$(21\times 2) \bmod 26 = 16$$
$$(21\times 3) \bmod 26 = 11$$
$$(21\times 4) \bmod 26 = 22$$
$$(21\times 5) \bmod 26 = 1$$

we can choose $X = \det K = 47 \bmod 26 = 21$ $Y = 5, Z = 26$. Since $(XX^{-1}) \bmod Z = (21\times 21^{-1}) \bmod 26 = 1$ and $(XY) \bmod Z = (21\times 5) \bmod 26 = 1$ thus $21^{-1} \bmod 26 = 5$

Thus, we can obtain the value of K^{-1}

$$K^{-1} = \frac{1}{21} \bmod 26 \begin{bmatrix} 19 & -14 \\ -17 & 15 \end{bmatrix} = 5 \begin{bmatrix} 19 & -14 \\ -17 & 15 \end{bmatrix} \bmod 26 = \begin{bmatrix} 17 & 8 \\ 19 & 23 \end{bmatrix}$$

Process description is obtained by multiplying the formula in the encryption process by K^{-1}.

$$C = KP$$
$$K^{-1}C = K^{-1}KP$$
$$K^{-1}C = IP$$
$$K^{-1}C = P$$

The description process are as follow:

$$p_0=\begin{bmatrix}17 & 8\\ 19 & 23\end{bmatrix}\begin{bmatrix}16\\ 19\end{bmatrix}\bmod 26=\begin{bmatrix}424\\ 741\end{bmatrix}=\begin{bmatrix}8\\ 13\end{bmatrix}$$

$$p_1=\begin{bmatrix}17 & 8\\ 19 & 23\end{bmatrix}\begin{bmatrix}16\\ 19\end{bmatrix}\bmod 26=\begin{bmatrix}159\\ 248\end{bmatrix}=\begin{bmatrix}3\\ 14\end{bmatrix}$$

$$p_2=\begin{bmatrix}17 & 8\\ 19 & 23\end{bmatrix}\begin{bmatrix}17\\ 11\end{bmatrix}\bmod 26=\begin{bmatrix}377\\ 576\end{bmatrix}=\begin{bmatrix}13\\ 14\end{bmatrix}$$

$$p_3=\begin{bmatrix}17 & 8\\ 19 & 23\end{bmatrix}\begin{bmatrix}18\\ 16\end{bmatrix}\bmod 26=\begin{bmatrix}434\\ 710\end{bmatrix}=\begin{bmatrix}18\\ 8\end{bmatrix}$$

$$p_4=\begin{bmatrix}17 & 8\\ 19 & 23\end{bmatrix}\begin{bmatrix}20\\ 3\end{bmatrix}\bmod 26=\begin{bmatrix}364\\ 449\end{bmatrix}=\begin{bmatrix}0\\ 7\end{bmatrix}$$

$$p_5=\begin{bmatrix}17 & 8\\ 19 & 23\end{bmatrix}\begin{bmatrix}12\\ 1\end{bmatrix}\bmod 26=\begin{bmatrix}212\\ 251\end{bmatrix}=\begin{bmatrix}4\\ 17\end{bmatrix}$$

$$p_6=\begin{bmatrix}17 & 8\\ 19 & 23\end{bmatrix}\begin{bmatrix}23\\ 23\end{bmatrix}\bmod 26=\begin{bmatrix}575\\ 966\end{bmatrix}=\begin{bmatrix}3\\ 4\end{bmatrix}$$

$$p_7=\begin{bmatrix}17 & 8\\ 19 & 23\end{bmatrix}\begin{bmatrix}20\\ 14\end{bmatrix}\bmod 26=\begin{bmatrix}452\\ 702\end{bmatrix}=\begin{bmatrix}10\\ 0\end{bmatrix}$$

Then, we determined the plain text and we got the plain text in the **Table 5**.

Table 5. Plaintext

p_0		p_1		p_2		p_3		p_4		p_5		p_6		p_7	
8	**13**	**3**	**14**	**13**	**4**	**18**	**8**	**0**	**7**	**4**	**17**	**3**	**4**	**10**	**0**
I	**N**	**D**	**O**	**N**	**E**	**S**	**I**	**A**	**M**	**E**	**R**	**D**	**E**	**K**	**A**
Block Matrix 1		Block Matrix 2		Block Matrix 3		Block Matrix 4		Block Matrix 5		Block Matrix 6		Block Matrix 7		Block Matrix 8	

4. CONCLUSIONS

Based on the research results, we got the following conclusion: $GShack(TB_2,v,n)$ admits a super $(3n+5,2)-$ Edge Antimagic Total Labeling with values $a=3n+5$ and $d=2$. The key used in the Hill Cipher algorithm uses the first two smallest weights of the graph $GShack(TB_2,v,n)$and their corresponding edges. The variation of the edge weight function and the corresponding edge label on the $GShack(TB_2,v,n)$ graph, will make the constructed lock more complicated to hack. Variations in the location of the corresponding edge and edge weights on the key in the form of a matrix will also produce quite a number of combinations. This will make the probability of the key being hacked difficult to estimate.

AKNOWLEDGEMENT

We would like to thanks for the support from Scope Research group, Mathematics Education Department, Faculty of Teacher Training and Education, University of Jember.

REFERENCES

[1] J. A. Gallian, "*A Dynamic Survey Of Graph Labeling*," *Electron. J. Comb.*, vol. 1, no. Dynamic Surveys, 2018.

[2] Dafik., Slamin., D. Tanna, A. Semanicova-Fenovcikova, and M. Baca, "*Constructions of H-Antimagic Graphs Using Smaller Edge-Antimagic Graphs*," *Ars Comb.*, vol. 133, pp. 233–245, 2017.

[3] M. Bača, Y. Lin, M. Miller, and M. Z. Youssef, "*Edge-Antimagic Graphs*," *Discrete Math.*, vol. 307, no. 11–12, pp. 1232–1244, 2007, doi: 10.1016/j.disc.2005.10.038.

[4] M. Javaid, "*On Super Edge-Antimagic Total Labeling of Subdivided Stars*," *Discuss. Math. - Graph Theory*, vol. 34, no. 4, pp. 691–705, 2014, doi: 10.7151/dmgt.1764.

[5] T. M. W. and C. C. Hsiao, "*On Anti-Magic Labeling for Graph Products*," *Discret. Math*, vol. 308, pp. 3624–3633, 2008.

[6] R. M. Prihandini, I. H. Agustin, and Dafik, "The Construction of P2 ▹ H-antimagic graph using smaller edge-antimagic vertex labeling," *J. Phys. Conf. Ser.*, vol. 1008, no. 1, 2018, doi: 10.1088/1742-6596/1008/1/012039.

[7] J. L. Shang, C. Lin, and S. C. Liaw, "*On The Antimagic Labeling Of Star Forests*," *Util. Math*, vol. 97, pp. 373–385, 2015.

[8] N. Prasanna, … K. S.-O. J. of, and undefined 2014, "Applications of graph labeling in communication networks," *Computerscijournal.Org*, vol. 7, no. 1, 2014, [Online]. Available: http://www.computerscijournal.org/pdf/vol7no1/OJCSV07I1P139-145.pdf

[9] K. Madhusudhan Reddy, A. Itagi, S. Dabas, and B. K. Prakash, "*Image Encryption Using Orthogonal Hill Cipher Algorithm*," *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 59–63, 2018, doi: 10.14419/ijet.v7i4.10.20707.

[10] A. Hidayat and T. Alawiyah, "*Enkripsi Dan Dekripsi Teks Menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang*," *J. Mat. Integr.*, vol. 9, no. 1, p. 39, 2013, doi: 10.24198/jmi.v9i1.10196.

[11] A. Putera, A. P. U. Siahaan, and R. Rahim, "*Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm*," *Int. J. Secur. its Appl.*, vol. 10, no. 8, pp. 173–180, 2016, doi: 10.14257/ijsia.2016.10.8.15.

[12] S. Saeednia, "*How To Make The Hill Cipher Secure*," *Cryptologia*, vol. 24, no. 4, pp. 353–360, 2000.

[13] R. T. Tarigan, "*Pengamanan Pesan Rahasia Menggunakan Metode Algoritma Hill Cipher*," *Publ. Ilm. Teknol. …*, vol. 3, no. November, pp. 161–165, 2018, [Online]. Available: http://jurnalnya.stmikneumann.ac.id/index.php/pitin/article/download/61/62

[14] M. Mahmudah, "Super Edge Antimagic Total pada Generalisasi Shackle Graf Kipas dan Aplikasinya dalam Pengembangan Cryptosystem (On super edge-antimagicness of generalized shackle".

[15] R. M. Prihandini, I. H. Agustin, and Dafik, "*Ciphertext Stream Construction By Using Super Total Labeling (A; D)-P2 B H-Antimagic Of Comb Product Graph*," *J. Phys. Conf. Ser.*, vol. 1211, no. 1, 2019, doi: 10.1088/1742-6596/1211/1/012013.