Chipertext stream construction by using super total labeling \((a, d)\)-\(P_2\triangleright \mathcal{H}\)-antimagic of comb product graph

R M Prihandini\textsuperscript{1,4}, I H Agustin\textsuperscript{1,3}, Dafik\textsuperscript{1,2}

\textsuperscript{1}CGANT University of Jember, Indonesia
\textsuperscript{2}Mathematics Edu. Depart., University of Jember
\textsuperscript{3}Mathematics Depart. University of Jember, Indonesia
\textsuperscript{4}Elementary School Teacher Edu, University of Jember, Indonesia

E-mail: rafiantikap.fkip@unej.ac.id, ikahestiagustin@gmail.com, d.dafik@unej.ac.id

Abstract. Development of ciphertext can be developed through labeling concept. Graphical labeling is a mapping of the elements of the graph (vertex or edge) to a set of positive integers. Mapping is called a functional function if each element on the graph is numbered with different positive integers. The process in ciphertext development can be called a cryptosystem. Ciphertext aims to make the message delivered by the message sender unreadable by the person who was not intended as the recipient of the message. There are several ways to change the secret message, one of which is Cipher Block Chaining (CBC) method. In this system, plaintext or \(P\) is divided into blocks and sequential keys \(K\). One of the science fields of discrete mathematics that can be applied to the development of ciphertext is graph theory, with the topic of labeling of the graph. In this article, we discussed about the development of ciphertext which is developed from the labeling of comb product graph, namely \(G = C_5 \triangleright W_5\).

1. Introduction
Digital technology is becoming increasingly sophisticated and the use of technology is not only in certain classes but also to the low society. This is indicated by the use of mobile phones and internet. However, network complexity and data transfer demand more optimization and security accuracy. Therefore, the coding between each element must be very complicated to avoid being tampered with by the hackers which is caused the result in data transfer between elements to be inaccurate. These problems can be solved through the development of secret messages or ciphertext. The process in ciphertext development can be called a cryptosystem. Ciphertext aims to make the message delivered by the message sender unreadable by the person not intended as the recipient of the message. There are several ways to change the secret message, one of
which is Cipher Block Chaining (CBC) method. In this system, plaintext or \( P \) is divided into blocks and sequential keys \( K \). One of the fields of science of discrete mathematics that can be applied to the development of ciphertext is graph theory, with the topic of labeling of the graph. Some of the ciphertext related studies that have been developed include, [2], [9], [17] and [10].

In this article, we discussed about ciphertext development developed from graph labeling. Graph labeling is a mapping a set of graph elements (vertex or edge) to a set of positive integers. Mapping is called a functional function if each element on the graph is numbered with different positive integers [12]. The graph of the result of comb product graph \( G = C_5 \triangleright W_5 \). Graph operation is one of the techniques to obtain a new graph by conducting an operation against two or more graphs. Suppose that \( G \) and \( H \) are connected graphs and \( o \) are points at \( H \), the comb products of the \( G \) and \( H \) graphs are denoted by \( G \triangleright H \) are the graphs obtained by taking a copy of \( G \) and \( |V(G)| \) a copy of \( H \) and and paste the copy into \( i \) from the graph \( H \) at the graft point \( o \) at the point \( i \) of the graph \( G \). Thus, the set of vertex and edge of the graph \( G \triangleright H \) are as follows: \( V(G \triangleright H) = \{(a, v) | a \in V(G); v \in V(H)\} \) and \( E(G \triangleright H) = \{(a, v)(b, w) | a, b \in V(G); v, w \in V(H)\} \) jika \( a = b \) dan \( vw \in E(H) \) atau \( ab \in E(G) \) and \( v = w = o \) [11].

Cryptography comes from greek language consisting of two syllables, namely crypto and graphia. Crypto means hide, while graphia means writing. Cryptography is a science that studies mathematical techniques related to information security aspects such as data confidentiality, data validity, data integers, and data authentication, but not all aspects of information security can be solved by cryptography. In principle, cryptography has six main components: Plaintext, which is a read message, Ciphertext, an unreadable random message, Key, the key to performing cryptographic techniques, Algorithms, which is the main components: Plaintext, which is a read message, Ciphertext, an unreadable random message, Confidentiality, data validity, data integers, and data authentication, but not all aspects of information security can be solved by cryptography. In principle, cryptography has six main components: Plaintext, which is a read message, Ciphertext, an unreadable random message, Key, the key to performing cryptographic techniques, Algorithms, which is the method for encryption and decryption, Encryption is a process of making a plaintext message becomes a ciphertext, and Decryption is the inverse process of encryption where this process will convert (ciphertext) into a plaintext by using an inverting algorithm with the same key [8].

Ciphertext techniques are categorized into two, namely classic cryptography and modern cryptography. Classical cryptography is character-based cryptography (encryption and decryption performed on each character) and modern cryptography is cryptography that operates in bit mode [6].

2. A Useful Lemma, Theorem, and Corollary

In this study, we focus for the connected version of the graph \( G = L \triangleright H \). Let \( L, H \) be two graphs of order \( |V(L)|, |V(H)| \) and size \( |E(L)|, |E(H)| \) respectively. The graph \( G = L \triangleright H \) is a connected graph with \( |V(G)| = |V(L)||V(H)| \) and \( |E(G)| = |V(L)||E(H)| + |E(L)| \). When \( L = C_n \), thus \( |V(L)| = |E(L)| = n \). Let \( p_H = |V(H)|, q_H = |E(H)| \), the vertex set and edge set of the graph \( G = C_n \triangleright H \) can be split in the following sets: \( V(G) = \{x_j; 1 \leq j \leq n\} \cup \{x_{ij}; 1 \leq i \leq p_H - 1, 1 \leq j \leq n\} \) and \( E(G) = \{x_jx_{j+1}, x_1x_n; 1 \leq j \leq n-1\} \cup \{e_{ij}; 1 \leq i \leq q_H, 1 \leq j \leq n\} \). Thus \( |V(G)| = np_H \) and \( |E(G)| = nq_H + n \) [3].

The upper bound of feasible \( d \) for \( G = C_n \triangleright H \) to be a super \((a, d)\)-\( P_2 \triangleright H \)-antimagic total labeling follows the following lemma, proved by [3].
IOP Conf. Series: Journal of Physics: Conf. Series 1211 (2019) 012013 doi:10.1088/1742-6596/1211/1/012013

Lemma 1. [3] Let $G$ be a simple graph of order $p$ and size $q$. If $G$ is super $(a, d)$-$H$-antimagic total labeling then

$$d \leq \frac{(p_G - p_H) p_H + (q_G - q_H) q_H}{n-1}$$

for $p_G = |V(G)|$, $q_G = |E(G)|$, $p_H = |V(H)|$, $q_H = |E(H)|$, and $n = |H|$.

If $G = C_n \bowtie H$, the upper bound of feasible $d$ follows the following corollary.

Corollary 1. [5] Let $K = P_2 \bowtie H$, for odd integer $n \geq 3$, if the graph $G = C_n \bowtie H$ admits super $(a, d)$-$K$-antimagic total labeling with $p_K = 2p_H$ and $q_K = 2q_H + 1$, then

$$d \leq (p_K^2 + q_K^2) - (\frac{n}{n-1})(\frac{1}{2}p_K^2 + \frac{1}{2}q_K^2)$$

Furthermore, a partition theorem have been developed by Dafik et.al in [4]. This theorem is used to have a different permutation of partition technique.

Lemma 2. [4] Let $n$ and $m$ be positive integers. The sum of $P_{m,d_1}(i, j) = \{(i - 1)n + j, 1 \leq i \leq m\}$ and $P_{m,d_2}(i, j) = \{(j - 1)m + i, 1 \leq i \leq m\}$ form an aritmatic sequence of difference $d_1 = m, d_2 = m^2$, respectively.

Based on Lemma 2 we can derive two new lemmas with $d_1 = m$ and $d_2 = m^2$, but different bijective function with Lemma 2.

Lemma 3. [5] Let $n, m$ be positive integers. For $1 \leq j \leq n$, the sum of

$$P_{m,d_1}(i, j) = \left\{ \begin{array}{ll}
(i+1) + (i - 1)n; & 1 \leq i \leq m; j \text{ odd} \\
\left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{1}{2} + (i - 1)n; & 1 \leq i \leq m; j \text{ even}
\end{array} \right.$$ 

form an aritmatic sequence of difference $d_1 = m$.

Lemma 4. [5] Let $n, m$ be positive integers. For $1 \leq j \leq n$, the sum of

$$P_{m,d_2}(i, j) = \left\{ \begin{array}{ll}
(i+1)m + i; & 1 \leq i \leq m; j \text{ odd} \\
\left\lfloor \frac{m}{2} \right\rfloor + i + (i - 2)m; & 1 \leq i \leq m; j \text{ even}
\end{array} \right.$$ 

form an aritmatic sequence of difference $d_2 = m^2$.

Corollary 2. [5] Let $K = P_2 \bowtie H$, and let $p_H = m_1 + m_2$ and $q_H = r_1 + r_2$ be the number of vertices and edges of graph $H$, respectively. For odd integer $n \geq 3$, if we assign the linear combination of $P_{m,m}^n$ and $P_{m,m^2}^n$ as a label of all elements in $G$, then $G = C_n \bowtie W_4$ admits a super $(a, d)$-$P_2 \bowtie H$ antimagic total labeling with $d = m_1 + m_2^2 + r_1 + r_2^2 + 1$.

3. Method

The key is got from edge label that is used to build the key stream. The key stream is a flowing and unlimited key. In addition it is also sensitive to initial values, so the secret key of the initial value when replaced produces a different key stream. Furthermore, the key stream obtained is used to build ciphertext using cipher block chaining (CBC) method. The steps to form ciphertext are as follows:

a. Define and select a graph that has size more than plaintext characters, for example 26. Suppose $r$ is the number of characters created by ciphertext.
b. Labeled the vertex and edge \((a, d) - K\) \(- antimagic\) total \covering{} on the graph \(G = C_5 \triangleright W_5\). The selected graph must meet \(|E(G)| \geq r\) since there is a \(r\) character where each character is represented by an edge. There should be no unanswered characters against the sides. The characters examined one by one explicitly state that the characters are individually referenced to the side label that will be formed ciphertext. Illustration of vertex and edge labeling from The graph \(G = C_5 \triangleright W_5\) is shown in Figure 1.

c. Eliminating the side that has the label \(f_e > |V| + r\).

The character used as \(r\) so the ciphertext needed is as much as \(r\). The starting code is a number so the rules need to be made to transform the numbers into ciphertext so use the number \((mod r)\). One of the existing rules is the rule of Julius Caesar where each alphabet corresponds to a sequence of numbers \((mod 26)\). The edge that have the label \(f_e > |V(G)| + r\) are eliminated. This coefficient is done so that no similarity or repetition of the mod of \(r\) thus does not occur in chipertext equality. If the side has been eliminated then the side is not used for the tree diagram.

d. To make a tree diagram of the graph \(G = C_5 \triangleright W_5\) with the smallest label of the smallest point, in this study the smallest label of the selected point is 1, while the next root follows the pattern of the graph. The elimination side is unnecessary. Figure 2 is the tree diagram of the graph \(G = C_5 \triangleright W_5\).

e. List the side label on the tree diagram from the graph \(G = C_5 \triangleright W_5\) according to the labeling on the graph used and change the number on that side label to the mode number 26.

f. Build the key stream using \(k_{i+26} = k_i + k_{i+1} \text{mod} 26\).

g. Use the label series as a stream stream or stream key to be used to construct encryption keys.

And then, key streams or flow keys will be used to construct encryption keys using the Chiper Block Chainig (CBC) method as the steps of the method are as follows:

a. \(plaintext \ P = (p_i), 1 \leq i \leq h\).

b. Let’s say the key sequence is \(K = (k_i); 1 \leq i \leq m\).

1) if \(m < h\), so the key \(K\) repeated \(|K| = |P|\).

2) if \(m > h\), then \(K = K - \{k_{h+1}, ..., k_m\}\).

c. divide \(P\) into block with length \(b\).

d. divide \(K\) into block with length \(b\).

e. for \(i = 1\) until \(\lceil \frac{h}{b}\rceil\), do the calculations ciphertext blocks with the calculation below:

\[C_i = C_{i-1} + P_i + K_i \mod 26\]

with \(P_i\) and \(K_i\) respectively are the \(i\)-block of plaintext and the key line and \(C_i\) is the ciphertext of modulo 26 for \(i = 1\), \(C_i - 1\) is zero vector \([1]\). The decryption process is the process for retrieving plaintext. The steps of the method are as follows:

a. suppose \(chipertext \ C = (c_i), 1 \leq i \leq h\).

b. Let \(K = (k_i)\) be the key line; \(1 \leq i \leq m\).

1) if \(m < h\), then the key \(K\) repeated \(|K| = |C|\).
Figure 1. Super \((a,d)-\text{P}_{2} \triangleright \mathcal{H}\)-Antimagic Antimagic Total Covering of Graph \(G = C_{5} \triangleright W_{5}\)

2) if \(m > h\), then \(K = K - \{k_{h+1}, \ldots, k_{m}\}\).

c. divide \(C\) into block with length \(b\).

d. divide \(K\) into block with length \(b\).

e. for \(i = 1\) until \(\lceil \frac{h}{b} \rceil\), do the calculations ciphertext blocks with the calculation below:

\[
P_{i} = C_{i} - K_{i} - C_{i-1} \mod 26
\]

\(P_{i}\) and \(K_{i}\) respectively are the \(i\)-block of plaintext and the key row and \(C_{i}\) is the ciphertext of modulo 26 for \(i = 1\), \(C_{i} - 1\) is zero.

4. Results and Discussion

In this section, we will discuss the steps in the chipertext development process. The method used to form chipertext is a chiper block chaining (CBC) method. This mode implements the feedback mechanism on a block. The previous block encryption results are used as feedback for block encryption now. The key is the side label that will then be used to build the key stream. The key stream is a flowing and unlimited key. In addition it is also sensitive to initial values, so the secret key of the initial value when replaced will result in a different key stream. Furthermore, the key stream obtained will be used to build chipertext using chiper block chaining (CBC) method.

Figure 1 is a graph \(G = C_{5} \triangleright W_{5}\) with \(d = 39\) to be applied to form chipertext alfabet. In Figure 1 it is shown that the vertex label starts from 1 to 30 and the side...
label starts from 31 to 85. The initial step is to sum up the number of points on the
graph $G = C_5 \triangleright W_5$ with the many letters used and eliminate side labels larger than
the number resulting, so the side label larger than 30 + 26 = 56 is 57, 58, 59, . . . , 85
should be eliminated so that no recurring mode of 26 is present. Next is to build a tree
diagram with 1 as the root of the tree diagram Figure 2 is a tree diagram of the graph
$G = C_5 \triangleright W_5$.

The next step is to place the side label on the tree diagram according to the side label
on the graph $G = C_5 \triangleright W_5$. The side label changed to modulo 26, then the edge label
is arranged sequentially from left to right and starts from the top layer. Contained side
labels will be used to build keystream. Based on Figure 2, the main key arrangement
is $k = \{5, 6, 10, 15, 17, 9, 22, 18, 13, 4, 20, 14, 19, 8, 22, 23, 25, 3, 24, 7, 16, 11, 1, 2, 21, 16\}$. Eventually the main key element will be used to build the key stream using the
$k_{i+26} = k_i + k_{i+1}$ mod 26 with $i \geq 1$, $k_i$ is the key to the main locks. Table 1 presents
the keystream obtained.

Furthermore, key streams or flow keys will be used to construct encryption keys using
the Chiper Block Chaining (CBC) method as the steps of the method are as follows:

a. suppose plaintext $P = (p_i), 1 \leq i \leq h$.
   In this research the length of plaintext is 26.

b. let $K = (k_i)$ be the key line; $1 \leq i \leq m$.
   the length of the lock will adjust to length plaintext is 26.
   1) if $m < h$, then the key $K$ repeated $|K| = |P|$.
   2) if $m > h$, then $K = K - \{k_{h+1}, \ldots, k_m\}$.

c. divide $P$ into block with length $b$. In this study, determined block length block $b = 3$
d. divide $K$ into block with length $b$. In this study, determined block length block $b = 3$
Table 1. The development of keystream from graph $G = C_5 \triangleright W_5$

| $k_i$ | $k_{i+26} = k_i + k_{i+1}$ | $k_{i+26} \mod 26$ |
|------|-----------------|------------------|
| 5    | $k_{27} = k_1 + k_2$ = 5 + 6 | 11               |
| 6    | $k_{28} = k_2 + k_3$ = 6 + 10 | 16               |
| 10   | $k_{29} = k_3 + k_4$ = 10 + 15 | 25               |
| 15   | $k_{30} = k_4 + k_5$ = 15 + 17 | 6                |
| 17   | $k_{31} = k_5 + k_6$ = 17 + 9 | 0                |
| 9    | $k_{32} = k_6 + k_7$ = 9 + 22 | 5                |
| 22   | $k_{33} = k_7 + k_8$ = 22 + 18 | 14               |
| 18   | $k_{34} = k_8 + k_9$ = 18 + 13 | 5                |
| 13   | $k_{35} = k_9 + k_{10}$ = 13 + 4 | 7               |
| 4    | $k_{36} = k_{10} + k_{11}$ = 4 + 20 | 24              |
| 20   | $k_{37} = k_{11} + k_{12}$ = 20 + 14 | 8               |
| 14   | $k_{38} = k_{12} + k_{13}$ = 14 + 19 | 7               |
| 19   | $k_{39} = k_{13} + k_{14}$ = 19 + 8 | 1               |
| 8    | $k_{40} = k_{14} + k_{15}$ = 8 + 22 | 4               |
| 22   | $k_{41} = k_{15} + k_{16}$ = 22 + 23 | 19              |
| 23   | $k_{42} = k_{16} + k_{17}$ = 23 + 25 | 14              |
| 25   | $k_{43} = k_{17} + k_{18}$ = 25 + 3 | 2                |
| 3    | $k_{44} = k_{18} + k_{19}$ = 3 + 24 | 1                |
| 24   | $k_{45} = k_{19} + k_{20}$ = 24 + 7 | 5               |
| 7    | $k_{46} = k_{20} + k_{21}$ = 7 + 16 | 23              |
| 16   | $k_{47} = k_{21} + k_{22}$ = 16 + 11 | 1               |
| 11   | $k_{48} = k_{22} + k_{23}$ = 11 + 1 | 12              |
| 1    | $k_{49} = k_{23} + k_{24}$ = 1 + 2 | 3                |
| 2    | $k_{50} = k_{24} + k_{25}$ = 2 + 21 | 23              |
| 21   | $k_{51} = k_{25} + k_{26}$ = 21 + 16 | 11              |
| 16   | $k_{52} = k_{26} + k_{27}$ = 16 + 11 | 1               |
| 16   | $k_{52} = k_{26} + k_{27}$ = 16 + 11 | 1               |

etc.

e. for $i = 1$ until $[\frac{n}{b}]$, do the calculations ciphertext blocks with the calculation below:
$C_i = C_{i-1} + P_i + K_i \mod 26$ $P_i$ and $K_i$ respectively are the $i$-block of plaintext and the key row and $C_i$ are ciphertext in modulo 26 for $i = 1$, $C_{i-1}$ is zero vector (Prihandoko, 2016).

The graph $G$ is the products of the comb products, denoted by $G = C_5 \triangleright W_5$ and the labeling follows Figure 1. The message to be sent is "oktober delapan puluh delapan". The sentence is transformed into a secret sentence created by chipertext using super labeling $(1351,39)-P_2 \triangleright H$-antimagic total covering on graph $G = C_5 \triangleright W_5$ then drawn tree diagram as in Figure 2.
Table 2. Encryption using CBC method developed by $G = C_5 \triangleright W_5$

| Plaintext | o   | k   | t   | o   | b   | e   | r   | d   | e   | a   | p   |
|-----------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| $P_i$     | 14  | 10  | 19  | 14  | 1   | 4   | 17  | 3   | 4   | 11  | 0   | 15  |
| $C_{i-1}$ | 0   | 0   | 0   | 25  | 0   | 18  | 19  | 1   | 1   | 24  | 9   | 12  |
| $K_i \mod 26$ | 11 | 16 | 25 | 6 | 0 | 5 | 14 | 5 | 7 | 24 | 8 | 7 |
| $C_i$     | 25  | 0   | 18  | 19  | 1   | 1   | 24  | 9   | 12  | 7   | 17  | 8   |
| Ciphertext| Z   | A   | S   | T   | B   | Y   | J   | M   | H   | R   | I   |
| Plaintext | a   | n   | p   | u   | l   | u   | h   | d   | e   | l   | a   | p   |
| $P_i$     | 0   | 13  | 15  | 20  | 11  | 20  | 7   | 3   | 4   | 11  | 0   | 15  |
| $C_{i-1}$ | 7   | 17  | 8   | 8   | 8   | 16  | 16  | 21  | 11  | 2   | 0   | 16  |
| $K_i \mod 26$ | 1 | 4 | 19 | 14 | 2 | 1 | 5 | 2 | 1 | 12 | 3 | 2 |
| $C_i$     | 8   | 8   | 16  | 16  | 21  | 11  | 2   | 0   | 16  | 25  | 3   | 2   |
| Ciphertext| I   | I   | Q   | Q   | V   | L   | B   | A   | Q   | Z   | D   | C   |
| Plaintext | a   | n   |
| $P_i$     | 0   | 13  |
| $C_{i-1}$ | 25  | 3   |
| $K_i \mod 26$ | 11 | 1 |
| $C_i$     | 10  | 17  |
| Ciphertext| K   | R   |

Table 2 describes ciphertext. If there is a plaintext ”oktober delapan puluh delapan” then ignore the read sign so that, it becomes ”oktoberdelapanpuluhdelapan” So the alphabetic ciphertext is ”ZASTBBYJMHRIIIQQVLBAQZDCKR”. The decryption process is the process for retrieving plaintext the steps of the method are as follows:

a. suppose ciphertext $C = (c_i), 1 \leq i \leq h$.

In this study, ciphertext length is 26.
b. Let $K = (k_i)$ be the key line; $1 \leq i \leq m$. the length of the lock will adjust to the ciphertext length is 26.
   1) if $m < h$, then the key $K$ repeated $|K| = |C|$.
   2) if $m > h$, then $K = K - \{k_{h+1}, ..., k_m\}$.
c. divide $C$ into block with length $b$.
   in this study, determined block length $b = 3$
d. divide $K$ into block with length $b$.
   in this study, determined block length $b = 3$
e. for $i = 1$ until $\lceil \frac{h}{b} \rceil$, do the calculations ciphertext blocks with the calculation below:

$P_i = C_i - K_i - C_{i-1} \mod 26$ $P_i$ and $K_i$ respectively are the $i$-block of plaintext and the key row and $C_i$ is the ciphertext of modulo 26 for $i = 1$, $C_{i-1}$ is zero.

5. Conclusion
In this paper, we have implemented the ciphertext polyalphabetic cryptosystem for super labeling $(a,d) - P_2 \triangleright \mathcal{H}$ - antimagic total covering of graph $G = C_5 \triangleright W_5$ by using the
Table 3. Decryption Using Developmental Feed Methods from $G = C_5 \triangleright W_5$

| chipertext | Z | A | S | T | B | C | Y | J | M | H | R | I |
|------------|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_i$      | 25| 0 | 18| 19| 1 | 1 | 24| 9 | 12| 7 | 17| 8 |
| $K_i \mod 26$ | 11| 16| 25| 6 | 0 | 5 | 14| 5 | 7 | 24| 8 | 7 |
| $C_{i-1}$  | 0 | 0 | 0 | 25| 0 | 18| 19| 1 | 1 | 24| 9 | 12|
| $P_i$      | 14| 10| 19| 14| 1 | 4 | 17| 3 | 4 | 11| 0 | 15|
| plaintext  | o | k | t | o | b | e | r | d | e | l | a | p |

| chipertext | I | I | Q | Q | V | L | B | A | Q | Z | D | C |
|------------|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_i$      | 8 | 8 | 16| 16| 21| 11| 2 | 0 | 16| 25| 3 | 2 |
| $K_i \mod 26$ | 1| 4 | 19| 14| 2 | 1 | 5 | 2 | 1 | 12| 3 | 23|
| $C_{i-1}$  | 7 | 17| 8 | 8 | 8 | 16| 16| 21| 11| 2 | 0 | 16|
| $P_i$      | 0 | 13| 15| 20| 11| 20| 7 | 3 | 4 | 11| 0 | 15|
| plaintext  | a | n | p | u | l | u | h | d | e | l | a | p |

| chipertext | K | R |
|------------|---|---|
| $C_i$      | 10| 17|
| $K_i \mod 26$ | 11| 1|
| $C_{i-1} \mod 26$ | 25| 3|
| $P_i$      | 0 | 13|
| plaintext  | a | n|

cipher block chaining (CBC) method with the development of the keystream without spaces and punctuation.

References

[1] A C Prihandoko, Dafik, I H Agustin, D Susanto, Slamin 2016 The Construction of Encryption Key by Using a Super $H$-Antimagic Total Graph Asian Mathematical Conference submitted

[2] Bellare M, Kilian J, Rogaway P The security of cipher block chaining In Annual International Cryptology Conference 1994 Aug 21 341-358

[3] Dafik, A K Purnapraja, R Hidayat Cycle-Super Antimagicness of Connected and Disconnected Tensor Product of Graphs, Procedia Computer Science 2015 74 9399

[4] Dafik, Slamin, Dushyant Tanna, Andrea Semaničová-Fečcová, Martin Bača Constructions of $H$-antimagic graphs using smaller edge-antimagic graphs Ars Combinatoria 2017 133 pp 233-245

[5] Agustin I H, Dafik, and Prihandini R M $P_2 \triangleright H$-super antimagic total labeling of comb product of graphs AKCE International Journal of Graphs and Combinatorics 2016 In press

[6] Katz J and Lindell Y Introduction to modern cryptography CRC press 2014

[7] Jutla CS Encryption modes with almost free message integrity In International Conference on the Theory and Applications of Cryptographic Techniques 2001 529-544
[8] Pearson E Introduction to Cryptography with Coding Theory America: United States of America 2006

[9] Petrank E and Rackoff C CBC MAC for real-time data sources Journal of Cryptology 2000 13(3) 315-38

[10] Rogaway P, Bellare M and Black J 2003 OCB: A block-cipher mode of operation for efficient authenticated encryption ACM Transactions on Information and System Security (TISSEC) 6(3) 365-403

[11] Saputro S W, Mardiana Novi, Purwasih I A 2013 The Metric Dimension of Comb Product Graph Graph Theory Conference in Honor of Egawa’s 60th Birthday

[12] Wallis W D 2001 Magic Graphs Boston: Birkhauser