Advances in Computer Science Research, volume 96
Proceedings of the International Conference on Mathematics, Geometry, Statistics, and Computation (IC-MaGeStiC 2021)

Primary Key Encryption Using Hill Cipher Chain (Case Study: STIE Mandala PMB Site)

Muhamat Abdul Rohim*, Kiswara Agung Santoso, Alfian Futuhul Hadi

Department of Mathematics, FMIPA, University of Jember
* *Corresponding author. Email: muhamatabdulrohim@gmail.com*

ABSTRACT
The condition of the world experiencing the COVID-19 pandemic has resulted in some daily activities limited by health protocols. The Indonesian government's policy in the academic field has forced STIE Mandala Jember, as one of the private universities, to implement online-based new student admissions. The registrant's identity must be kept confidential during the online-based new student registration process, so the running system needs an identity coding (encryption) process. Hill Cipher is a cryptographic algorithm that utilizes the multiplication of matrix inverse operations. In ordinary Hill Cipher, to encrypt the entire plaintext, a key is needed. In this paper, we will modify the Hill Cipher named Hill Cipher Chain. The process of chained Hill Cipher will encrypt and decrypt the primary key based on the previous character. Firstly, we will encrypt the primary key with the key from the next column of the database. In this case, we use the name column. The encryption result will be used as a key for the subsequent character encryption. Implementation of this method makes the difficulty level of decryption more complex than the ordinary Hill Cipher, which only uses one key for all so that the security of the data obtained is also getting better.

Keywords: *Inverse matrix, cryptography, Hill cipher, Chained Hill cipher, Hill cipher chain.*

1. INTRODUCTION

2020 has been a challenging year for the community due to the COVID-19 pandemic, which is not over yet. The site liputan6.com quoted the WHO statement that the main transmission route of the Corona Virus is through droplets that spread when someone coughs, sneezes, or talks [1]. WHO also warned the public to maintain physical distance or maintain a distance of at least 1m from other people.

The Indonesian government, since March 2020, has issued a distance learning policy in the teaching and learning process in universities. This policy requires universities to improve the quality of their online information services to reduce interactions between the academic community. All universities, both private and public, are trying to support this policy by improving online services.

STIE Mandala is one of the private universities in Jember district. This private university developed various services to reduce interaction between the academic community in the STIE Mandala environment. One of the services currently being designed is the online new student registration service.

Prospective students will register their name and an active email address through the PMB website in the new student registration process. The site will automatically create a unique registered ID for each registrant and send a link containing that ID to the registered email. The Registered ID is critical and must keep secret, so third parties cannot take advantage of the information.

The running system can maintain the confidentiality of the registered ID sent to the registrant's email by applying a cryptographic process at the time of delivery. The paper written by Anjar Pradipta [2] explains that cryptography is the science and art of keeping messages secure when messages are sent from one place to another. There are two main processes in cryptography, namely, the process of encoding messages or encryption and the process of breaking messages or decrypting.

There are various cryptographic algorithms currently developing, including Hill Cipher Cryptography. Hill Cipher Cryptography is a cryptographic algorithm that uses multiplication and matrix inverse techniques for encryption and decryption [3]. The matrix used in this algorithm is a matrix of size nxn and invertible [9].

2. CRYPTOGRAPHY

Etymologically, cryptography comes from the Greek words kryptos, which means hidden, and graphein, which means writing [4]. In full, Cryptography is the science of writing secret messages to hide the meaning of the message [4].

Two terms are known in cryptography, namely Plaintext and Ciphertext. An original message called plaintext is encoded into an encrypted message called Ciphertext through the encryption process, and the Ciphertext is recovered into plaintext again through the decryption process. [5]. A more explicit description of the cryptographic process can be seen in Figure 1.

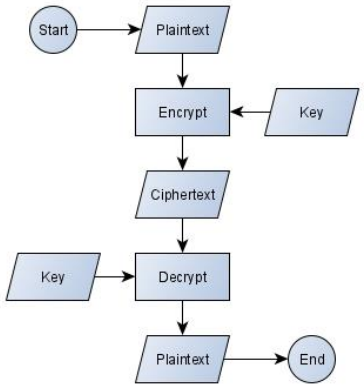

Figure 1 Cryptographic process.

Figure 1 explains that the initial process of cryptography is the presence of plaintext (messages to be encoded) which will be encrypted using a specific key and produce a ciphertext that is not understood. Ciphertext can be reread after decryption using a particular key and returned to plaintext form as before encryption.

3. HILL CIPHER

Hill Cipher is a symmetric-key cryptography algorithm using a *nxn* matrix [6]. The basis used in this algorithm is multiplying the matrix with its inverse matrix, which will produce an identity matrix. In general, the description of the Hill Cipher algorithm can be seen in Figure 2 and Figure 3.

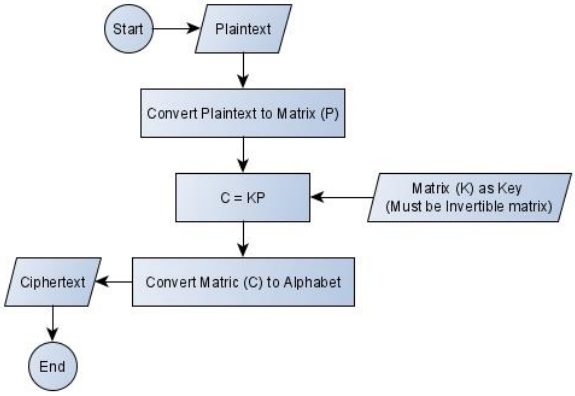

Figure 2 Hill Cipher Encryption Process.

Figure 2 describes the encryption process in Hill Cipher. This process begins with the plaintext to be encoded. Then, the plaintext is converted into a matrix form (P) with specific rules. The matrix (P) formed will be multiplied by the matrix (K) as the encryption key. The matrix (K) must be invertible because the matrix (K^{-1}) will be the key in the decryption process. The result of the multiplication between the matrix (P) and the matrix (K) will be a matrix (C). This matrix is converted into alphabetical form again using the same rules as changing the plaintext into a matrix form.

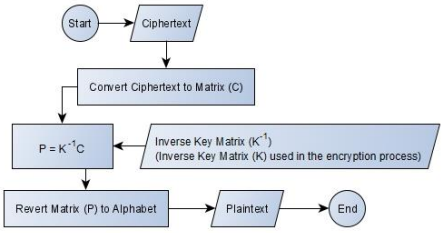

Figure 3 Hill Cipher Decryption Process.

Figure 3 explains that the decryption process in Hill Cipher begins with the Ciphertext as input. This Ciphertext will be converted into a matrix form (C) with certain rules. The matrix (C) that is formed will be multiplied by the inverse of the key matrix used during encryption and produce a matrix (P). The decryption process ends by changing the matrix (P) into alphabetical form again based on the rules used for converting Ciphertext into matrix form.

4. METHODS

The Hill Cipher method generally uses one key to encode the entire plaintext. In general, all the steps involved in the Hill Cipher encryption process can be seen in Figure 4.

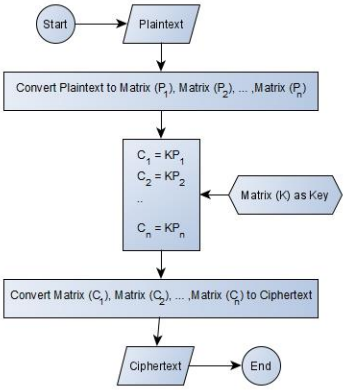

Figure 4 Encryption Process on Hill Cipher.

Figure 4 shows that the resulting matrix C (C_1, C_2, …, C_n) is the product of the matrix P (P_1, P_2, …, P_n) with the same key matrix (K). The hill cipher chain used in this study modifies the key used so that the process will look like Figure 5.

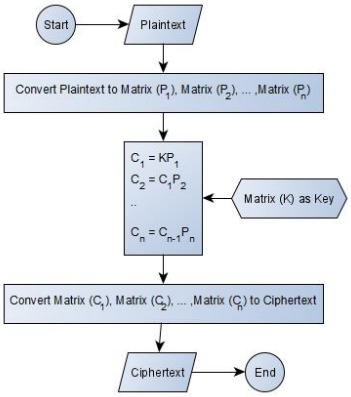

Figure 5 Encryption Process on Hill Cipher Chain.

Figure 5 shows Hill Cipher Chain encrypting plaintext using different keys in each matrix (P) formed. The matrix (K) is only used in the first encryption process of the matrix (P_1), while the key used in matrix encryption ($P_n \mid n \neq 1$) is the matrix (C_{n-1}) which is the result of the encryption of the matrix (P_{n-1}). The Hill Cipher key must be invertible, the matrix (C_{n-1}) will be a column matrix, so additional elements are needed. These elements are obtained randomly to make the matrix (Cn-1) invertible.

The difference in the encryption process results in a different decryption process. Figure 6 shows the steps for the decryption process in a typical Hill Cipher.

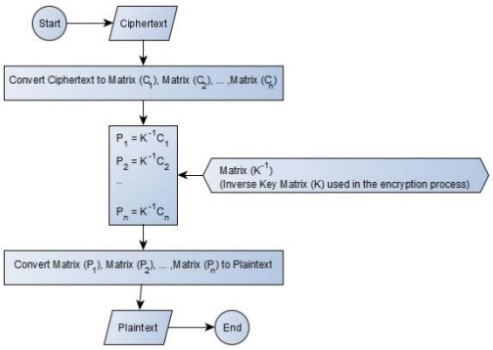

Figure 6 Decryption Process on Hill Cipher.

Figure 6 shows that the decryption process in Hill Cipher generally only requires one key matrix inverse (K^{-1}) to decrypt the entire matrix (C_1, C_2, …, C_n while in Hill Cipher Chain, the decryption process can be seen in Figure 7.

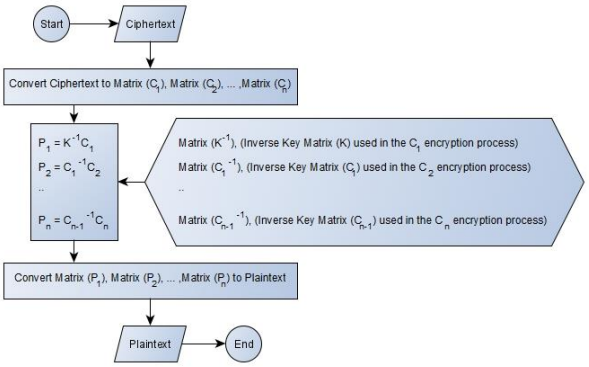

Figure 7 Decryption Process on Hill Cipher Chain.

Figure 7 shows the decryption process in the Hill Cipher Chain requiring the inverse of each key used in the encryption process. A matrix (K^{-1}) is required for matrix decryption (C_1), and a matrix ($C_{n-1}^{-1} \mid n \neq 1$) is required for matrix decryption (C_n).

5. ENCRYPTION PROCESS

The New Student Admission System for STIE Mandala uses UUID (Universally Unique Identifier) as the *primary key* in the registrant data. UUID is an identification standard in the form of 32-digit hexadecimal, which is divided into five groups and separated by hyphens [10]. The number of UUID characters with the hyphens is 36 characters.

The key matrix must be invertible. Therefore, to simplify calculations, the encryption and decryption process will use a square matrix having the order of 2x2. The 36 UUID characters will be split into 18 column matrices, each of which has two members representing two characters from UUID that have been converted into integers. The character conversion rules are based on Table 1.

Table 1. Character Conversion Rules

Character	Conversion	Character	Conversion	Character	Conversion	Character	Conversion
0	0	a	10	k	20	u	30
1	1	b	11	l	21	v	31
2	2	c	12	m	22	w	32
3	3	d	13	n	23	x	33
4	4	e	14	o	24	y	34
5	5	f	15	p	25	z	35
6	6	g	16	q	26	-	36
7	7	h	17	r	27		
8	8	i	18	s	28		
9	9	j	19	t	29		

Based on the book written by Howard Anton and Chris Rorres [7], matrix K = $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ said to be invertible if $ad - bc \neq 0$, where the inverse matrix is calculated using Equation (3).

$$K^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \quad (3)$$

Equation (3) is used to calculate the inverse of the matrix in general, while to calculate the inverse of the matrix on modulo *n*, the auxiliary variable *k* is used, which operates with the determinant value using Equation (4) [8].

$$x = \frac{n(k)+1}{ad-bc} \quad (4)$$

Calculate the value of *x* in equation (4) with *k* = {…, -1, 0, 1, …} so that *x* is an integer. After finding the *k* value, calculate the inverse of the key matrix by Equation (5).

$$K^{-1} = x \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} mod\ n \quad (5)$$

The key matrix used for the encryption process is different for the 18 column matrices that are formed. Each key will depend on a specific character. The initial key is created based on the first and second characters in the name column of the encrypted *primary key*. In contrast, the subsequent key formation is based on the first and second characters of the resulting Ciphertext, creating a chain process in key building and encryption. Figure 8 describe the detail of key construction.

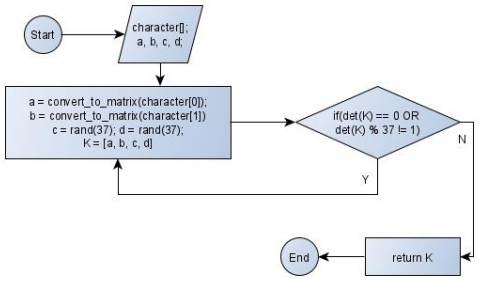

Figure 8 Key Formation Flow.

For example, any registrant data is taken as in Table 2.

Table 2. Sample of Registered Data

Primary Key	Name
d57ef4b8-069c-4d4b-9393-7e3576dc2b75	Muhamat Abdul Rohim

Based on Table 2, the first two characters from the name column are the letters M and U, then the values of *a* and *b* in the initial key matrix (K) are 22 and 30 (based on Table 1). For example, after being randomly found the numbers 9 and 14 as the values of *c* dan *d* so that they are formed matrix K = $\begin{bmatrix} 22 & 30 \\ 9 & 14 \end{bmatrix}$, this key matrix is invertible at modulo 37. The encryption process uses the key matrix (K). The details of the encryption process can be seen in Figure 9.

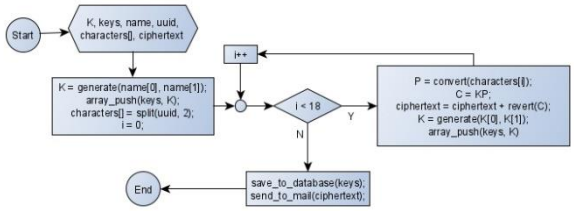

Figure 9 Encryption Flow.

For example, in Table 2, the *primary key* is 'd57ef4b8-069c-4d4b-9393-7e3576dc2b75', and the initial key K = $\begin{bmatrix} 22 & 30 \\ 9 & 14 \end{bmatrix}$. Based on the encryption flow in Figure 9, the following steps are taken:

1. Split plaintext into 18 character groups.

Plaintext:
d57ef4b8-069c-4d4b-9393-7e3576dc2b75

Character Groups:
d5 7e f4 b8 -0 69 c- 4d 4b -9 39 3- 7e 35 76 dc 2b 75

2. Convert each of character group into a matrix (P) based on Table 1.

Matrix P:

$$P_{d5} = \begin{bmatrix}13\\5\end{bmatrix}, P_{7e} = \begin{bmatrix}7\\14\end{bmatrix}, P_{f4} = \begin{bmatrix}15\\4\end{bmatrix}, P_{b8} = \begin{bmatrix}11\\8\end{bmatrix},$$

$$P_{-0} = \begin{bmatrix}36\\0\end{bmatrix}, P_{69} = \begin{bmatrix}6\\9\end{bmatrix}, P_{c-} = \begin{bmatrix}12\\36\end{bmatrix}, P_{4d} = \begin{bmatrix}4\\13\end{bmatrix},$$

$$P_{4b} = \begin{bmatrix}4\\11\end{bmatrix}, P_{-9} = \begin{bmatrix}36\\9\end{bmatrix}, P_{39} = \begin{bmatrix}3\\9\end{bmatrix}, P_{3-} = \begin{bmatrix}3\\36\end{bmatrix},$$

$$P_{7e} = \begin{bmatrix}7\\14\end{bmatrix}, P_{35} = \begin{bmatrix}3\\5\end{bmatrix}, P_{76} = \begin{bmatrix}7\\6\end{bmatrix}, P_{dc} = \begin{bmatrix}13\\12\end{bmatrix},$$

$$P_{2b} = \begin{bmatrix}2\\11\end{bmatrix}, P_{75} = \begin{bmatrix}7\\5\end{bmatrix}$$

3. Calculate matrix C (C = KP)

Matrix C:

$$C_1 = \begin{bmatrix}22 & 30\\9 & 14\end{bmatrix}\begin{bmatrix}13\\5\end{bmatrix} = \begin{bmatrix}436\\187\end{bmatrix}$$

4. Determine the Ciphertext by returning the matrix (C) modulo 37 to alphabetical form based on Table 1.

Reverse result:

$$C_1 = \begin{bmatrix}436\\187\end{bmatrix} mod\ 37 = \begin{bmatrix}29\\2\end{bmatrix} = \text{t2}$$

5. Generate new key

The new key is generated based on the character matrix conversion (C_1), combined with two random numbers. The Ciphertext of the conversion matrix (C_1) is t2, so the conversion of t2 characters based on Table 1 is 29 and 2, for example, two random numbers 6 and 3 are determined to form an invertible 2x2 matrix on modulo 37, then the new key created is K = $\begin{bmatrix}29 & 2\\6 & 3\end{bmatrix}$, this key is used to calculate the matrix (C_2).

6. Repeat process 3 to 5 until founding the matrix (C_{18}) value.

7. Merge Ciphertext

Ciphertext:
t29arhq4b9-k53mboatj-0oztz3ii8yl3tiq

6. DECRYPTION PROCESS

The decryption process begins by reading the entered Ciphertext and then looking for the inverse of the key matrix (K^{-1}) that has been stored in the database. The next step is to break the Ciphertext into 18 character groups, then convert it based on the rules in Table 1 into matrix form (C). The P matrix is obtained by the equation $P = K^{-1}C$. After founding the matrix (P) value, return the matrix (P) based on Table 1 rules into plaintext form. This process is performed on each matrix (C) using their respective keys. Details of the decryption steps can be seen in Figure 6.

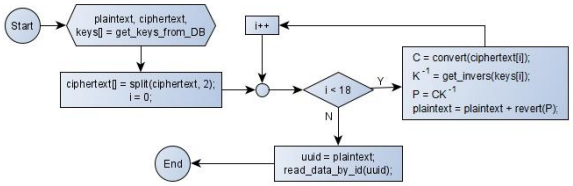

Figure 10 Decryption Flow.

For example, based on the steps in Figure 6, we will decrypt the Ciphertext 't29arhq4b9-k53mboatj-0oztz3ii8yl3tiq' using the previously-stored key, with the following steps:

1. Split Ciphertext into 18 character groups.

Ciphertext:
t29arhq4b9-k53mboatj-0oztz3ii8yl3tiq

Character Groups:
t2 9a rh q4 b9 -k 53 mb oa tj -0 oz tz 3i i8 yl 3t iq

2. Convert the 18 character groups into 18 column matrices (C) based on Table 1

$$C_{t2} = \begin{bmatrix}29\\2\end{bmatrix}, C_{9a} = \begin{bmatrix}9\\10\end{bmatrix}, C_{rh} = \begin{bmatrix}27\\17\end{bmatrix}, C_{q4} = \begin{bmatrix}26\\4\end{bmatrix},$$

$$C_{b9} = \begin{bmatrix}11\\9\end{bmatrix}, C_{-k} = \begin{bmatrix}36\\20\end{bmatrix}, C_{53} = \begin{bmatrix}5\\3\end{bmatrix}, C_{mb} = \begin{bmatrix}22\\11\end{bmatrix},$$

$$C_{oa} = \begin{bmatrix}24\\10\end{bmatrix}, C_{ti} = \begin{bmatrix}29\\18\end{bmatrix}, C_{-0} = \begin{bmatrix}36\\0\end{bmatrix}, C_{oz} = \begin{bmatrix}24\\35\end{bmatrix},$$

$$C_{tz} = \begin{bmatrix}29\\35\end{bmatrix}, C_{3i} = \begin{bmatrix}3\\18\end{bmatrix}, C_{i8} = \begin{bmatrix}18\\8\end{bmatrix}, C_{yl} = \begin{bmatrix}34\\21\end{bmatrix},$$

$$C_{3t} = \begin{bmatrix}3\\29\end{bmatrix}, C_{iq} = \begin{bmatrix}18\\26\end{bmatrix}$$

3. Calculate the inverse modulo 37 of the stored key (key for C_{t2} = $\begin{bmatrix}22 & 30\\9 & 14\end{bmatrix}$).

Calculate inverse modulo 37 using the auxiliary variable *k*, with Equation (4). For example, if *k* = 1, then based on Equation (4), the value of *x* is obtained as follow:

$$x = \frac{n(k)+1}{ad-bc} = \frac{37(1)+1}{22.14-30.9} = \frac{38}{38} = 1$$

Based on Equation (5), the matrix K^{-1} was obtained as follows:

$$K^{-1} = 1\begin{bmatrix}14 & -30\\-9 & 22\end{bmatrix} mod\ 37$$

$$K^{-1} = \begin{bmatrix}14 & -30\\-9 & 22\end{bmatrix} mod\ 37$$

$$K^{-1} = \begin{bmatrix}14 & 7\\28 & 22\end{bmatrix}$$

4. Calculate matrix P ($P = K^{-1}C$)

$$P_1 = \begin{bmatrix} 14 & 7 \\ 28 & 22 \end{bmatrix} \begin{bmatrix} 29 \\ 2 \end{bmatrix} = \begin{bmatrix} 420 \\ 856 \end{bmatrix}$$

5. Determine the plaintext by returning the matrix (P) at modulo 37 based on Table 1.

$$P_1 = \begin{bmatrix} 420 \\ 856 \end{bmatrix} mod\ 37 = \begin{bmatrix} 13 \\ 5 \end{bmatrix} = d5$$

6. Repeat steps 3 to 5 until matrix P_{18} value is found
7. Merge plaintext

Plaintext:
d57ef4b8-069c-4d4b-9393-7e3576dc2b75

7. CONCLUSION

The Hill Cipher algorithm can be used to encrypt data in the form of a collection of characters arranged in UUID form with 36 characters. To facilitate implementation into the programming language, PHP uses a key matrix that has the order of 2x2 to be implemented relatively quickly in the PHP programming language. The results of encryption using a Hill Cipher with the formation of a chain key (Hill Cipher Chain) will make the Ciphertext more challenging to decrypt if it does not have a set of chain keys that have been formed. This process results in the data being more secure than using only one key in the hill cipher algorithm.

REFERENCES

[1] B.M.Verdiana, Coverage 6, 2020, Retrieved from liputan6.com: https://www.liputan6.com/global/read/4214488/who-unjukkan-corona-covid-19-tak-menular-kapal-air-ini-pelaksanaannya

[2] A. Pradipta, Implementasi Metode Caesar Chiper Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan Informasi (in Indonesian), Indonesian Journal on Networking and Security, 2016, 16-19.

[3] A.R. Yuliandaru, Hill Cipher Cryptography Technique Using Matrix, IF2123 Geometric Algebra, 2018, 1-6.

[4] M. K. Harahap, Analisis Perbandiangan Algoritma Kriptografi Klasik Vigenere Cipher dan One Time Pad (in Indonesian), Jurnal Nasional Informatika dan Teknologi Jaringan (in Indonesian), 2016, 61-64

[5] Yusfrizal, Rancang Bangun Aplikasi Kriptografi pada Teks Menggunakan Metode Reverse Cipher dan RSA Berbasi Android (in Indonesian), Jurnal Teknik Informatika Kaputama (in Indonesian), 2019, 29-37.

[6] A. Putera, U. Siahaan, R. Rahim, Dynamic Key Matrix of Hill Cipher Genetic Algorithm. International Journal of Security and Its Applications, 2016, 173-180.

[7] H. Anton, C. Rorres, Elementary Linear Algebra, America, Wiley, 2004

[8] R.K. Hondro, Teknik enkripsi dan dekripsi Hill Cipher (in Indonesian), 2017, 1-5

[9] S. Maryanti, A. Rakhman. Perancangan Aplikasi Kerahasiaan Pesan dengan Algoritma Hill Cipher. Seminar Nasional Inovasi dan Aplikasi Teknologi di Industri (in Indonesian), 2018, 70-74

[10] B. Rizaldi, D.S. Pambudi, T. Bariyah, Implementasi Teknologi Bluetooth Low Energy dan Metode Trilaterasi untuk Pencarian Rute Indoor (in Indonesian), JUTI: Jurnal Ilmiah Teknologi Informasi (in Indonesian), 2020, 57-67