International Journal of Computer and Information System (IJCIS)
Peer Reviewed – International Journal
Vol : Vol. 02, Issue 04, November 2021
e-ISSN : 2745-9659
https://ijcis.net/index.php/ijcis/index

Optimization of Hill Cipher Method for Encryption and Decryption of Prescription Drugs at Puskesmas Twano Jayapura City

1st Elvis Pawan 2nd Patmawati Hasan
[1,2]*dept. informatics Of Engineering*
[1,2]*STIMIK Sepuluh Nopember Jayapura*
[1,2]Jayapura, Indonesia
[1]elvispawan09@gmail.com; [2]patmawatihasan@gmail.com

Abstract*—A drug prescription is a written request from a doctor to a pharmacist that must be kept secret because it contains certain doses of drugs and types of drugs that cannot be known by just anyone, especially those who are not interested. From time to time technological advances have a rapid impact on all sectors, both private and government agencies, including the health sector. One form of service in the health sector that can utilize information technology is the manufacture of electronic drug prescriptions that can be sent via an application from a doctor to a pharmacist. The frequent misuse of prescription drugs by unauthorized persons, as well as errors by officers at the pharmacy in reading prescriptions can be fatal for the community, so a solution is needed to overcome this problem. This application is designed using the Hill Cipher Algorithm which is one of the classic types of algorithms in the field of cryptography, but to get the maximum level of security, the algorithm key will be modified using a postal code pattern as a matrix key. Broadly speaking, the Encryption Stage is the first starting from the plaintext which is the type of drug and drug dose, the second key matrix using a POS code pattern, the three plaintexts are converted into blocks, the fourth is arranged into a 2x2 matrix, the fifth is multiplied between the key and the sixth plaintext is multiplied into mod 26 to generate an encrypted ciphertext or recipe. The success rate of system functionality testing using the blackbox method is 100%

Keywords : *Hill Cipher, Enkripsi, Dekripsi, Optimization*

I. INTRODUCTION

A drug prescription is a form of written request made by a doctor to a pharmacist and must be kept secret from unauthorized persons, the request is intended for the pharmacist to mix the drug in a certain dosage form and hand it over to the patient. [1]-[2].

The security and confidentiality of data and information at a Puskesmas is one of the benchmarks for the success of a service to the community. Information that must be kept confidential, such as medical records and drug prescriptions, aims to avoid misuse of the data or information contained in the drug prescription.

A study states that conventional drug prescription writing is very easy to experience errors called medication errors, as many as 4.3% of errors in the application of electronic prescription applications while 11% for manual writing. [3]-[4].

This study aims to provide a solution for sending prescription drugs online through an application while maintaining confidentiality through the encryption method. To encrypt drug prescriptions using the Hill cipher method, this method is a classic method and has been widely used so that a different strategy is needed to strengthen the hill cipher algorithm. [5]. The strategy for strengthening the algorithm in this research is to take four digits from the back of each postal code which is used as a key matrix.

There are several algorithms that have been created by cryptography experts or experts such as the DES algorithm, 3DES algorithm, IDEA algorithm, blowfish algorithm, RSA algorithm, MD4 algorithm, MD5 algorithm, SHA-1 algorithm, McEliecce algorithm and many other algorithms. However, not all of these algorithms can withstand attacks by eavesdroppers [6]. Encrypting using the hill cipher method is an encryption method that uses a matrix as a key 7].

II. STATE OF THE ART

The use of the Hill Cipher method has been carried out by several previous researchers but in different cases, including a study using the Hill Cipher algorithm to control IoT-based homes, in this study concluded that the use of the Hill Cipher method for home security design can work with well, the weakness of this research is that it does not modify the algorithm. The difference in the research that will be carried out lies in the object of research and modifications to the matrix key by using a four-digit postal code as the key. [8]. Furthermore, in research that uses Hill Cipher to encrypt and decrypt an image by modifying the padding, this study concludes that the Hill Cipher algorithm can encrypt quickly and in less than one second, but the weakness in this study is that all tests for image decryption fail done. The difference in the research to be carried out lies in the object to be encrypted, namely the drug prescription that is entered in the application [9]. Another study that uses the Hill Cipher method, which is to encrypt a message in the form of text and images, in this study concludes that using the Hill Cipher algorithm for text and image encryption gives very significant randomness results. [10], the difference in the research that will be carried out is that the object that is encrypted is a drug prescription that can be input into the system then encrypted and then sent to the pharmacist on duty at the pharmacy.

The use of the Hill Cipher method to encrypt and use drug prescriptions as research objects has never been done so that researchers are interested in developing an electronic drug prescribing system.

International Journal of Computer and Information System (IJCIS)
Peer Reviewed – International Journal
Vol : Vol. 02, Issue 04, November 2021
e-ISSN : 2745-9659
https://ijcis.net/index.php/ijcis/index

III. RESEARCH METHODS

3.1 Research Flow

In conducting this research, there are seven important steps that are carried out, namely, firstly, literature study sourced from research results such as journals, proceedings, literature studies aimed at formulating the background, state of the art and theoretical basis. The second interview at the interview stage aims to obtain information directly from doctors and pharmacists at the Twano health center, the third system modeling, at this stage using data flow diagrams with the aim of being able to create context diagrams and dfd level 1, the fourth system design using the PHP programming language, and the Hill Cipher method, the fifth application test using the Blackbox method, at this stage it is expected to know whether the performance of the application can work well or not. Sixth analysis and conclusion. The seventh step is to prepare research reports and publications. To further clarify the steps in this research, it can be seen in Figure 1.

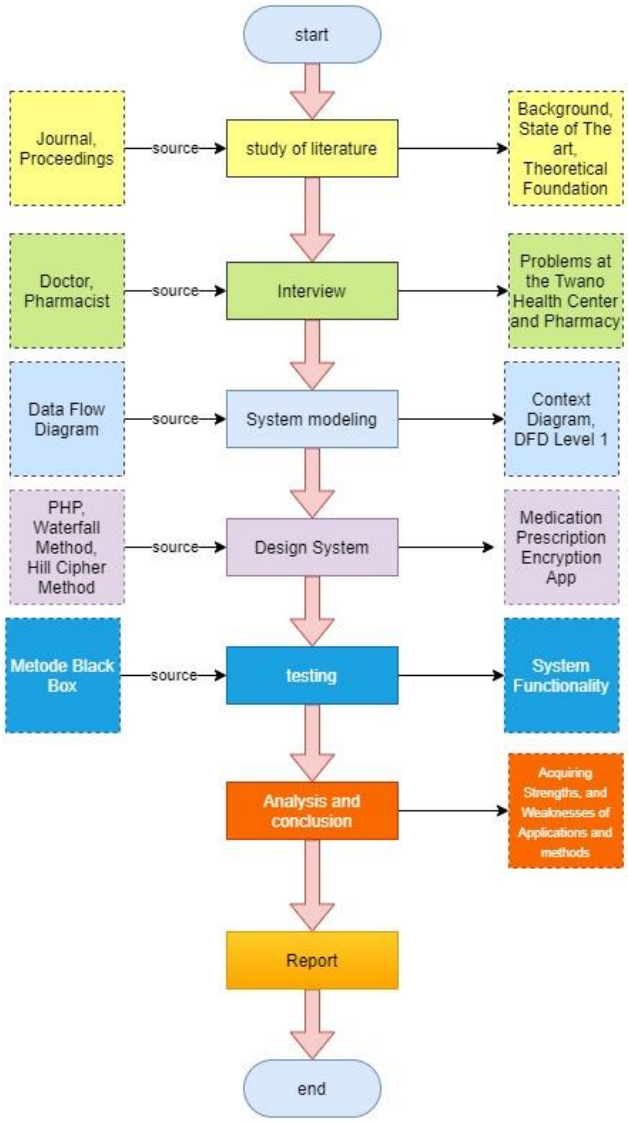

Figure 1 Research Flow

3.2 Hill Cipher

S One algorithm that is very difficult for cryptists to solve is the Hill Cipher algorithm. Modulo arithmetic is the basis of a Hill Cipher algorithm. In the application of the Hill Cipher algorithm, it uses matrix multiplication and inverse techniques. The key to a Hill Cipher algorithm can be seen in equation 1.

$n * n$ .....(1)

where n = block size

In the encryption process, plain text will be divided into several blocks which are adjusted to the size of the key matrix. Convert letters to numbers starting with zero. As in table 1.

Table 1. Convert Letter Values To Numbers

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

The encryption process on Hill Cipher uses the equation that can be seen in equation 2.

$C = K * P$ .....(2)

C = *Chiperteks*

K = *Key*

P = *Plaintext*

Meanwhile, to decrypt the Hill Cipher algorithm using the equation that can be seen in equation 3.

$P = K^{-1}.C$ .....(3)

To explain the steps in doing encryption using the Hill Cipher algorithm, see Figure 2.

International Journal of Computer and Information System (IJCIS)
Peer Reviewed – International Journal
Vol : Vol. 02, Issue 04, November 2021
e-ISSN : 2745-9659
https://ijcis.net/index.php/ijcis/index

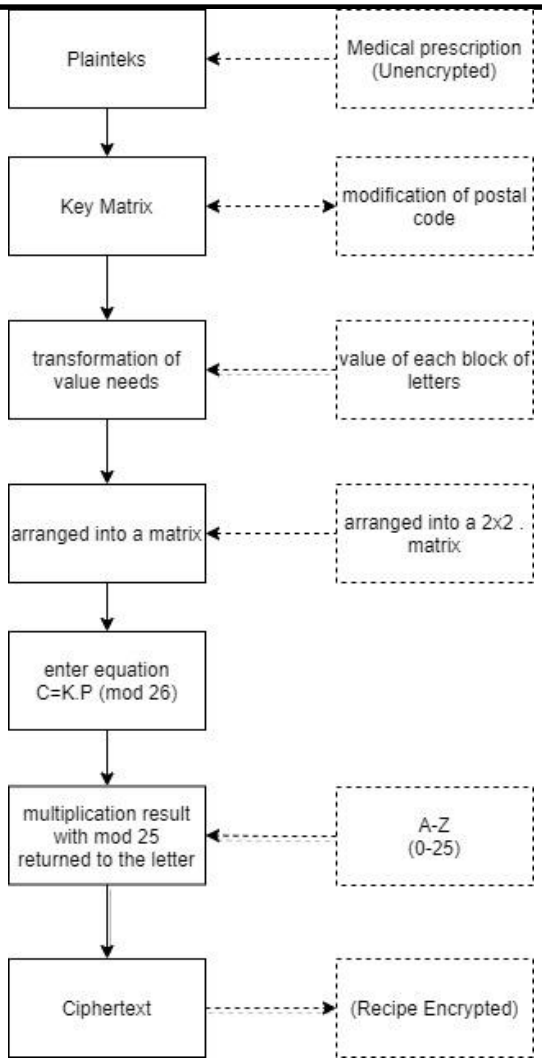

Figure 2. Encryption Steps

The first step starts from preparing plain text consisting of the names of drugs or prescriptions. The second is compiling the key sourced from the modified postal code. in the third stage, arrange the drug names into blocks that are adjusted to the matrix, and change the letters into numbers starting from A = 0, B = 1, C = 2 which is adjusted to the value in table 1. then perform calculations using the Hill algorithm equation Cipher, the last step is to obtain a prescription or drug name in the form of Cipher text.

3.3 Key List

In order for the encryption result to be stronger, the key used is modified from the postal code, besides it is expected that by using a postal code, the Hill Cipher algorithm key can be more structured and stronger. The list of keys used can be seen in table 2.

Table 2. Key List

Region	Postal code	Key Modification
Asmat	99729	9729
Biak Numfor	98511	8511
Boven Digoel	99651	9651
Deiyai	98751	8751
Intan Jaya	98794	8794
Kab. Jayapura	99350	9350
Kota Jayapura	99334	9334
Jayawijaya	99501	9501
Keerom	99473	9473
Lanny Jaya	99561	9561
Mappi	99851	9851
Mimika	99976	9976
Nduga	99901	9901
Paniai	98711	8711
P.Bintang	99401	9401
Puncak	98951	8951
P. Jaya	98911	8911
Sarmi	99370	9370
Supiori	98571	8571
Tolikara	99011	9011
Yahukimo	99701	9701
Yalimo	99081	9081

3.4 List of Drug Names

Some examples of encrypted drug names can be seen in table 3.

Table 3. List of Drug Names

No	Drug Names
1	Acetosal
2	Cetrizin
3	Ketoprofen
4	Fenitoin
5	Kolkisin
6	Meloksikam
7	Morfin
8	Pethidin
9	Piroksikam
10	Tramadol
11	Dapson
12	Kuinin
13	Antasida
14	Ketotifen
15	Terbutalin

IV. RESULT AND DISCUSSION

4.1 Encryption Process

To obtain more security for the drugs given to patients, it is necessary to encrypt so that the drugs are not misused by unauthorized persons. To prove the accuracy of encryption and decryption. In this study, the sample name of the drug "ACETOSAL" was carried out, the name of the drug was plain text. Meanwhile, the keys that are converted into matrix form are sourced from a modified list of postal codes. The plain text can be seen in table 4.

Table 4. Plain Teks

A	C	E	T	O	S	A	L
0	2	4	19	14	18	0	11

$$AC = \frac{0}{2} \quad ET = \frac{4}{19} \quad OS = \frac{14}{18} \quad AL = \frac{0}{11}$$

International Journal of Computer and Information System (IJCIS)
Peer Reviewed – International Journal
Vol : Vol. 02, Issue 04, November 2021
e-ISSN : 2745-9659
https://ijcis.net/index.php/ijcis/index

1) C(AC)

$$\begin{bmatrix}9 & 7\\9 & 2\end{bmatrix}\begin{bmatrix}0\\2\end{bmatrix}=\begin{bmatrix}0 & + & 14\\0 & + & 4\end{bmatrix}=\begin{bmatrix}14\\4\end{bmatrix} Mod\ 26 \begin{bmatrix}14\\4\end{bmatrix}=\begin{bmatrix}O\\E\end{bmatrix}$$

2) C(ET)

$$\begin{bmatrix}9 & 7\\9 & 2\end{bmatrix}\begin{bmatrix}4\\19\end{bmatrix}=\begin{bmatrix}36 & + & 133\\36 & + & 38\end{bmatrix}=\begin{bmatrix}169\\74\end{bmatrix} Mod\ 26 \begin{bmatrix}13\\22\end{bmatrix}$$
$$=\begin{bmatrix}N\\W\end{bmatrix}$$

3) C(OS)

$$\begin{bmatrix}9 & 7\\9 & 2\end{bmatrix}\begin{bmatrix}14\\18\end{bmatrix}=\begin{bmatrix}126 & + & 126\\36 & + & 36\end{bmatrix}=\begin{bmatrix}252\\162\end{bmatrix} Mod\ 26 \begin{bmatrix}18\\6\end{bmatrix}$$
$$=\begin{bmatrix}S\\G\end{bmatrix}$$

4) C(AL)

$$\begin{bmatrix}9 & 7\\9 & 2\end{bmatrix}\begin{bmatrix}0\\11\end{bmatrix}=\begin{bmatrix}0 & 77\\0 & 22\end{bmatrix}=\begin{bmatrix}77\\22\end{bmatrix} Mod\ 26 \begin{bmatrix}25\\22\end{bmatrix}=\begin{bmatrix}Z\\W\end{bmatrix}$$

The encryption process on the ASETOSAL plaintext obtained ciphertext which can be seen in table 5.

Table 5. Cipher Teks

O	E	N	W	S	G	Z	W
14	4	13	22	18	6	25	22

The results of the calculation of encryption manually are in accordance with the results of encryption using the system, while the results of encryption using the system can be seen in Figure 3.

Figure 3. Encryption Results

4.2 Decryption Process

The decryption process is the process of returning from cipher text to plain text.

$$\begin{bmatrix}9 & 7\\9 & 2\end{bmatrix}\begin{bmatrix}0\\2\end{bmatrix}=\begin{bmatrix}0 & + & 14\\0 & + & 4\end{bmatrix}=\begin{bmatrix}14\\4\end{bmatrix} Mod\ 26 \begin{bmatrix}14\\4\end{bmatrix}=\begin{bmatrix}O\\E\end{bmatrix}$$

Det K=(9 x 2)-(9 x 7) = -45
-45^{-1} mod 26 = x=45 mod 26

X=45 + 26x

$$X=\frac{45+26}{-1}$$

=-71

$$K^{-1}=71\begin{bmatrix}2 & -7\\-9 & 9\end{bmatrix}=\begin{bmatrix}-142 & 497\\639 & -639\end{bmatrix} mod\ 26$$

$$=\begin{bmatrix}14 & 3\\11 & 14\end{bmatrix}\begin{bmatrix}14\\4\end{bmatrix}=\begin{bmatrix}196 & + & 12\\154 & + & 56\end{bmatrix}$$

$$\begin{bmatrix}208\\210\end{bmatrix} mod\ 26 \begin{bmatrix}0\\2\end{bmatrix}=\begin{bmatrix}A\\C\end{bmatrix}$$

After all the cipher text blocks are decrypted using the same equation, the initial text or plain text "ACETOSAL" is obtained. To see the suitability between the results of manual decryption and the results of decryption using the system can be seen in Figure 4.

Figure 4. Decryption Results

4.3 Drug Form

The drug form is useful for inputting the names of drugs to be given to patients, while the drug form design can be seen in Figure 5.

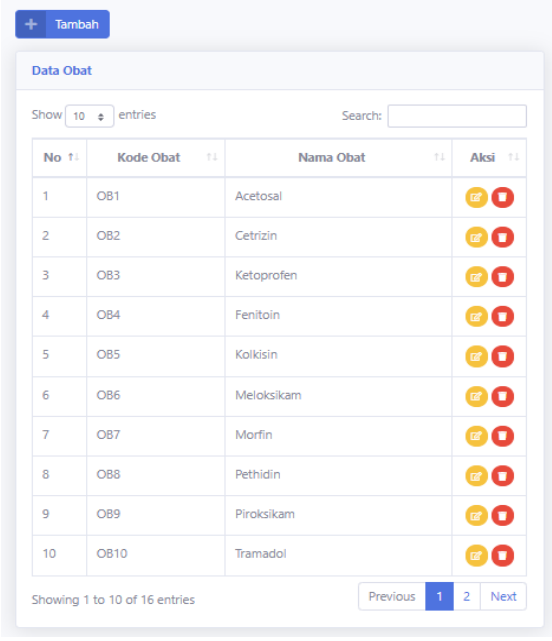

Figure 5. Drug Form

4.4 Electronic Prescribing

The prescription form is a form that can be used by doctors to input prescriptions that have been encrypted before being sent to the pharmacist. The recipe form can be seen in Figure 6.

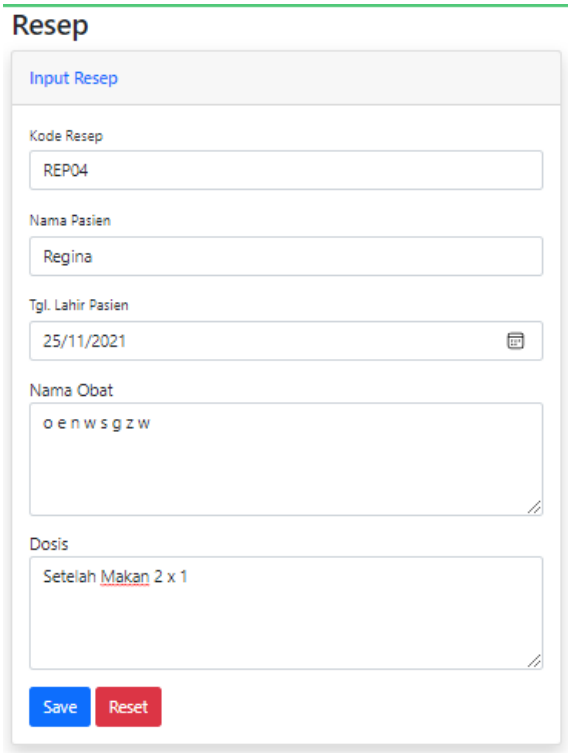

Figure 6. Recipe Form

4.5 System Testing

This test is carried out using the blackbox method, while the purpose of testing this system is to be able to find out the functionality of the system can work in accordance with the expectations and system development plans. The test results can be seen in the table 6.

Table 6. System Testing

No	Scenario	Result test	
		Valid	Invalid
1	On the login page enter the correct user name and password, the system is expected to lead to the main menu page	√	X
2	On the login page, enter the wrong user name and/or password, it is hoped that the system will provide information on failed logins because the password or username is wrong	√	X
3	On the Main menu, the Encryption sub menu, drug menu, user and logout appears	√	X
4	In the user menu, clicking the encryption sub menu, selecting the matrix and inputting the appropriate key, then clicking the submit button, the Encrypt and Decrypt menu will appear.	√	X
5	Users clicking encrypt or decrypt are expected to display a plain text input menu or text cipher	√	X
6	On the Plain Text input menu, the user inputs one of the drug names, then clicks encrypt, it is hoped that the system can display the encrypted drug name	√	X
7	In the decrypt menu, the user enters the cipher text or the name of the drug that has been encrypted, then clicks the Decrypt button, it is hoped that the system can display the real drug name..	√	X
8	On the main menu, the user clicks on the Drugs sub menu, it is hoped that the system can display a list of drug names in the database	√	X
9	On the drug menu, the user clicks add drug, the system is expected to display a form to input the code and name of the new drug	√	X
10	In the drug form, input the code and name of the drug, then the user clicks the save button, it is hoped that the system can save the code and name of the drug into the database and the system provides information	√	X

	on successfully adding drug data.		
11	On the drug menu, the user clicks edit, it is hoped that the system can display the name and code of the drug to be edited	√	X
12	On the main menu, the user clicks on the recipe submenu, it is hoped that the system can display a recipe list form	√	X
13	On the recipe menu, the user clicks add recipe, it is hoped that the system can display the add recipe form	√	X
14	In the recipe form, the user adds a new recipe, then clicks the save button, the system is expected to be able to save the new recipe in the database	√	X
15	On the recipe menu, the user clicks the edit recipe button, it is hoped that the system can display the recipe edit form	√	X
16	On the recipe menu, the user clicks the delete button, it is hoped that the recipe can be deleted and displays information that the recipe data has been successfully deleted	√	X
17	On the main menu, the user clicks the logout button, the system is expected to return to the login menu	√	X

VI. CONCLUSION

Some conclusions that can be drawn from the results of this study are as follows:

1. Modifying the key to the Hill Cipher algorithm can increase security, besides that the key for encryption and decryption is also more structured.
2. The success rate of system functionality testing using the blackbox method is 100%
3. The weakness in the Hill Cipher algorithm is that data encryption that has an odd number of letters or numbers tends to be difficult to encrypt.

REFERENCES

[1] Y. Yusuf, "Kualifikasi Tindak Pidana Atas Kesalahan Pe,Bacaan Resep Dokter Oleh Apoteker Yang Menimbulkan Kerugian Pada Pasien," Simp. Huk. Indones., vol. 1, no. 8, pp. 1–13, 2019.

[2] Rahmatini, "Agar Penulisan Resep Tetap Up To Date," Maj. Kedokt. Andalas, vol. 33, no. 2, pp. 101–108, 2015.

[3] F. C. Sabila, R. Z. Oktarlina, and N. Utami, "Peresepan Elektronik (E-Prescribing) Dalam Menurunkan Kesalahan Penulisan Resep," Med. J. Lampung Univ., vol. 7, no. 3, pp. 271–275, 2018.

[4] W. S. Margareta and D. Iwan, "Peran Resep Elektronik dalam meningkatkan Medication Safety pada proses peresepan," J. Manaj. Pelayanan Kesehat., vol. 17, no. 1, pp. 30–36, 2014.

[5] J. R. Paragas, A. M. Sison, and R. P. Medina, "An Improved Hill Cipher Algorithm using CBC and Hexadecimal S-Box," in 2019 IEEE Eurasia Conference on IoT, Communication and Engineering (ECICE), 2019, pp. 77–81

[6] Eddy and M. R. Pahlevi, "PEMBELAJARAN ENKRIPSI METODE WORD AUTO KEY ENCRYPTION," Sisfotenika, vol. 4, no. 1, pp. 23–32, 2014

[7] S. Hraoui, F. Gmira, M. F. Abbou, A. J. Oulidi, and A. Jarjar, "A New Cryptosystem of Color Image Using a Dynamic-Chaos Hill Cipher Algorithm," Procedia Comput. Sci., vol. 148, pp. 399–408, 2019.

[8] N. Nasron, S. Suroso, and C. Buana, "Rancang Bangun Pengaman Rumah dan Kontrol Pada Kunci Pintu dengan Metode Kriptogafi Hill Cipher Berbasis IoT," PRotek J. Ilm. Tek. Elektro, vol. 7, no. 2, pp. 104–109, 2020.

[9] D. M. Sholahudin and Asmunin, "Implementasi Algoritma Hill Cipher untuk Proses Enkripsi dan Dekripsi Citra Berwarna dengan Modifikasi Padding," J. Informatics Comput. Sci., vol. 01, no. 04, pp. 228–234, 2020.

[10] J. Freddy et al., "Kriptografi Teks dan Citra dengan Menggunakan Algoritma Hill Cipher pada Perangkat Android," J. Masy. Inform., vol. 8, no. 1, pp. 9–15, 2017.