Three Layer Encryption Protocol: an Approach of Super Encryption Algorithm

Muhammad Fadlan
Dept. of Information System
STMIK PPKIA Tarakanita Rahmawati
Tarakan, Indonesia
fadlan@ppkia.ac.id

Haryansyah
Dept. of Informatics Engineering
STMIK PPKIA Tarakanita Rahmawati
Tarakan, Indonesia
haryansyah@ppkia.ac.id

Rosmini
Dept. of Information System
STMIK PPKIA Tarakanita Rahmawati
Tarakan, Indonesia
rosmini@ppkia.ac.id

2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS) | 978-1-6654-2580-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICORIS52787.2021.9649574

***Abstract*— Data security is one of the critical things that must be considered along with the ease of the data distribution process in Era Society 5.0. Maintaining data security is not an easy thing to do. One way that can be used to secure data is through cryptographic techniques. In cryptography, two basic techniques are often used, namely substitution techniques and transposition techniques. The problem in this study is related to the weakness of the level of data security in the classical cryptography algorithm, substitution, and transposition techniques. This study aims to develop a cryptographic approach to super encryption by doing a hybrid or a combination of three cryptographic algorithms. The approach proposed in this study is also known as the three-layer encryption protocol. The algorithms that focus on this research are Autokey Cipher, Columnar Transposition, and Hill Cipher. Evaluation of the results of the application of the proposed three-layer protocol approach using the Avalanche Effect approach. As a result, the proposed three-layer protocol technique can produce a better level of security than single-layer encryption.**

Keywords—cryptography, data, hybrid, security, three-layer

I. INTRODUCTION

Data has a vital role in the era of the Industrial Revolution 4.0 and Society 5.0. There are three critical elements in data, namely Confidentiality, Integrity, and Availability [1]–[3]. Data security is an important issue today. Various threats to data security include Interruption, Interception, modification, and fabrication [4], [5]. The easy process of distributing data through various technology platforms carries a significant risk to data security issues [6], [7]. Maintaining the integrity and security of data is one of the toughest challenges [8], [9]. The fall of essential data and information belonging to an institution to others certainly brings losses in the sustainability of an institution. Therefore, a technique is needed to maintain data security. One technique that is widely used today is Cryptography.

Cryptography is a science that plays a vital role in information security because it can be used to secure data [10]–[12]. Cryptography can provide an added level of security to data during processing, storage, and communication. Cryptography plays a vital role in providing data security, and this makes the data not easily recognized by unauthorized external parties [13]. This knowledge can be used on almost all communication channels, both networked and non-networked [14]. There are two types of popularly used techniques in various types of cryptographic algorithms, namely, substitution and transposition techniques. The substitution technique is a technique that uses the method of exchanging characters in plaintext with other characters. Unlike the substitution technique, the transposition technique does not change plaintext letters into ciphertext letters. The transposition technique uses character permutations where the ciphertext is obtained by changing the arrangement of letters in the plaintext. The original message cannot be read except by the person who has the key to restore the message to its original form.

Each cryptographic algorithm has a different level of security. The main weakness of cryptographic algorithms that apply substitution and transposition techniques is the level of security that tends to be low [15], [16]. The main problem in this study is related to the weakness of the level of data security in the substitution and transposition cryptographic algorithms. The cryptographic algorithms that focus on this research are Autokey Cipher, Columnar Transposition, and Hill Cipher. Autokey cipher is a cryptographic algorithm that belongs to the substitution type [17], columnar transposition is included in the type of transposition [18]. Meanwhile, the Hill cipher is included in the polygraph cipher. One solution that can maximize the security level of a cryptographic algorithm is through a combination or hybrid with other cryptographic algorithms [19]–[21].

Autokey cipher is a development of Caesar and Vigenere cipher. Autokey cipher has a better level of security than the Viginere cipher and caesar cipher [22], [23]. In this technique, it takes a word as a key. This key is then followed by plaintext to form letters that are the same length as the plaintext. Columnar transposition is a cryptographic algorithm that transposes letters to perform encryption and decryption processes [24], [25]. This algorithm works by making ciphertext by replacing the position of the plaintext character without changing or changing the plaintext. The matrix reading is done column by column according to the key used in this column transposition technique.

Hill Cipher is a classic cryptographic algorithm that is very difficult to solve. This algorithm uses matrix multiplication based on encryption and decryption. This matrix-based makes Hill Cipher not replace every alphabet that is the same in the plaintext with other letters that are the same in the ciphertext [26]. In Hill cipher, each character in a block will affect the other in the encryption and decryption process so that the same character is not mapped into the same character. This is also known as a polyalphabetic cipher [27], [28].

This study aims to develop a super encryption approach by utilizing substitution and transposition techniques to produce a more reliable level of data security. The solution proposed in this research is through a combination process between the Hill Cipher algorithm, Autokey Cipher, and Columnar Transposition. In this study, the combination of these three algorithms is called the Three-layer encryption protocol. This

is because three algorithms are derived from two different techniques used in the data security process, namely substitution, and transposition techniques. In this study's three-layer encryption protocol approach, the Hill cipher is the first layer of encryption, the autokey cipher is the second layer of encryption, and columnar is the final encryption layer. Through the proposed encryption process, it is expected that it will produce a more reliable and difficult-to-break algorithm. The avalanche effect will also be used to test the performance of the proposed approach.

II. Related Work

Research conducted by Budiman et al. [29] aims to secure data by proposing a combination of transposition cipher and Trithemius algorithm. This research has focused directly on testing the complexity of the proposed algorithm. This study uses the value of complexity in assessing the proposed algorithm. However, it does not show precisely how the encryption process is carried out and what the decryption results look like.

Research conducted by Djamalilleil et al. [30] proposed a cipher transposition algorithm in securing digital images. The way this algorithm works is by transposing the pixels contained in the digital image. This study indicates that the proposed algorithm can be used to encrypt and decrypt digital images into their original form. Research conducted by Maricel et al. [31] aims to secure the private key using a transposition cipher. This study uses the avalanche effect to measure the performance of the proposed algorithm. The results show that the proposed algorithm is more practical in securing private keys.

Frimpong et al. [32] proposed Rubik's Cube Transformations to increase the security of the transposition cipher algorithm. This study uses Rubik's Cube method to randomize the arrangement of plaintext characters to be secured. This study does not explicitly indicate the measuring instrument used to determine the performance of the proposed algorithm.

Research by Wafaa et al. [33] has proposed a new approach in hiding data through DNA-based steganography combined with the autokey Viginere algorithm. In this study, autokey is used to generate a secret message before it is hidden through DNA-based steganography techniques.

Nofriansyah et al. [26] researched with the hill cipher algorithm through a combination of the least significant bit. This study uses a combination of these methods in securing data in the form of images. The research proposed by Khalaf et al. [27] modify the hill cipher through the hill cipher encryption process, which is repeated three times in encrypting data. This three-stage hill cipher process is carried out to improve the security of the data. However, these two studies do not specifically indicate the measuring tools used to determine the performance of the proposed algorithm.

The research proposed by Sinaga et al. [21] performs a Caesar cipher algorithm and Word Autokey to improve data security. The results of this study indicate that the Wake Algorithm can be combined with caesar to increase the level of data security. Nasution et al. [34] have used the Goldbach Codes Algorithm to improve the data security of the Viginere cipher algorithm. This research has tried to improve the data security of the Viginere cipher algorithm, which is the forerunner of the autokey cipher algorithm. The results show that the encryption results are more challenging to identify and difficult to hack than using only the Viginere cipher algorithm.

Some related studies did not show the tools used to measure the performance or reliability of the proposed technique. These studies only show that the algorithm can be encrypted and decrypted to its original form without knowing the extent of the performance of these algorithms.

III. Methodology

This section describes the proposed approach and is divided into three main parts: the proposed encryption, the proposed decryption, and the tools used to evaluate the proposed approach.

A. Proposed Encryption Approach

One of the critical stages in cryptography is the stage of converting the original data into encrypted data. This process is also known as the encryption process. This study proposes an encryption process known as a three-layer encryption protocol because three encryption processes are to be carried out. The encryption stages in this study can be seen in Fig. 1.

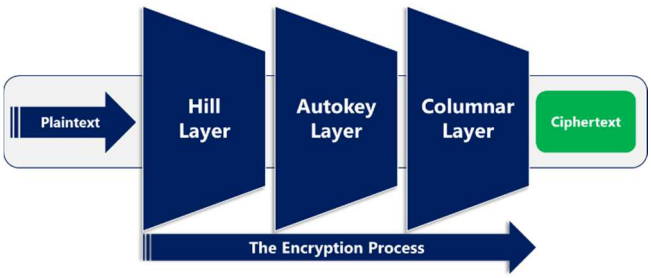

Fig. 1. The Proposed Encryption Process

In Fig. 1, it can be seen that the process of converting plaintext into ciphertext is carried out through three layers of encryption processes, including:

1. Hill Layer. At this layer the plaintext will be encrypted using the hill cipher algorithm. Equation 1 shows the encryption process at this layer [27], [35], [36].

$$C = (k * p) \bmod n \qquad (1)$$

With, k is the key; C is ciphertext; p is the message; n is the numbers of characters. A 2x2 matrix will be used in this study as a key.

2. Autokey Layer. In this layer, the encryption results from the hill layer will be re-encrypted with the autokey cipher algorithm. Equation 2 shows the encryption process at this layer [22].

$$C(i) = (p(i) + k(i) \bmod m \qquad (2)$$

C(i) is the encryption process; p(i) is the index of the character to be encrypted; k(i) is the index of the key, and "m" is the total number of characters used. In the autokey algorithm, if the key has a less than plaintext length, then the key will be combined with the plaintext itself.

3. Columnar Layers, the last layer in the proposed encryption process. In this layer, the encryption results from the second layer will be re-encrypted. The encryption process is done by dividing the characters in the plaintext into several blocks based on the key. The ciphertext will be obtained by taking the characters in certain columns according to the specified key [30], [32].

B. Proposed Decryption Approach

The decryption process is another critical process in cryptography. In this process, the encrypted message will be returned to the original message. The decryption process proposed in this study can be seen in Fig. 2

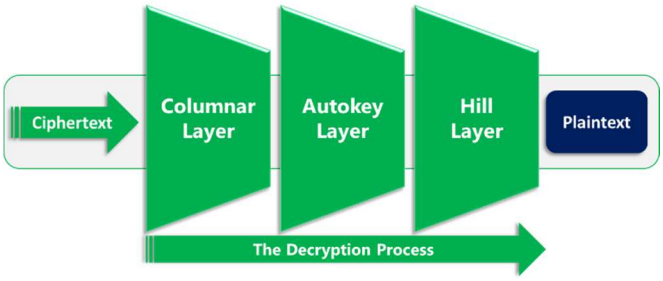

Fig. 2. The Proposed Decryption Process

The proposed decryption process will also go through a three-layer decryption process. The layers of the decryption process include:

1. Columnar Layer. In the proposed decryption process, the columnar transposition becomes the first layer. The process passed in this layer is the same as the process contained in the columnar encryption layer.
2. Autokey Layer. In this decryption layer, the decryption's decryption from the first layer will be decrypted again using an autokey cipher. The decryption process is carried out by referring to Equation 3 [22], which is the opposite of the process contained in Equation 2.

$$p(i) = (C(i) - k(i) \bmod m \qquad (3)$$

3. Hill Layer. The last layer of the decryption process is the hill layer. The decryption process is carried out by referring to Equation 4 [27], [35], [36].

$$p = (k^{-1} * C) \bmod N \qquad (4)$$

Where, K^{-1} the inverse of the key used during the encryption process.

C. Evaluation Tools

This study uses the Avalanche Effect to evaluate the proposed encryption and decryption approaches. Measurement of the avalanche effect is done by looking at any changes that occur in the ciphertext caused by changes in the plaintext [6], [37].

In this study, the length of the text used will be changed by one character to see the results of changing the encrypted characters with the proposed approach. In addition, avalanche effect calculation is used to see the number of bit changes that occur. The process contained in the avalanche effect can be seen in Equation (5).

$$AE = \frac{Dx}{total} x\ 100\% \qquad (5)$$

Dx is the sum of different bits; AE is the avalanche effect score, and the total is the total bits in the ciphertext.

IV. Result

This section explains the results of testing the three-layer encryption protocol approach proposed in this study. The following are the details of the proposed encryption process steps according to the stages contained in Fig. 1.

1. In testing the proposed three-layer encryption protocol, the plaintext is needed as a sample. The plaintext for the sample is *"We will Attack Their Website Tomorrow Night"*
2. Furthermore, the specified plaintext will be encrypted in the first layer. The first layer encryption process is carried out using a hill cipher based on Equation 1. The key matrix used in this layer is a=2, b=1, c=3, d=4. After going through this first layer encryption process, the ciphertext results are *_AKqM@3jt,X1/q_TDhS.`f,Md|b&_TZ"eNhK`^8|E q.i*
3. Next, the results of the first layer of encryption are re-encrypted in the second layer using an autokey cipher. The key used in this case is *c0risind0_1ndon3si@_2021*. The results of the second layer of encryption based on Equation 2 are *J01=4FB@E^=/c|U_v%|&m\w#K|lS"\{c+H \4!=Rp IH+Nd*
4. The last step is the third layer encryption process using columnar transposition. In this layer, the results of the second stage of encryption will be re-encrypted. The result of the third layer encryption process is the final ciphertext of the encryption process proposed in this study. The final result of this case is *0|\ E+=4# m w _I|N&d^HJKc=@ c%+F\=S UpB{/!| R1lvH4"*

By using the proposed three-layer encryption protocol approach, from the plaintext "We will Attack Their Website Tomorrow Night" after going through the three-layer encryption protocol proposed in this study, the final ciphertext is generated, namely 0|\ E+=4# m w I|N&d^HJ Kc=@ c% +F\=SUpB{/!| R1lvH4". This is one of the sample trials conducted on the encryption approach proposed in this study. It can be seen that there is a significant difference between the initial plaintext and the ciphertext of the encryption results.

Other trials have been carried out on the proposed approach, and measurements of the encryption results have also been carried out using the avalanche effect, as shown in Equation 5. One of the avalanche effect benefits is to determine the number of bits that change after the encryption process. The more bits that change will make the better algorithm. Some of the results of the trials that have been carried out can be seen in Table I.

TABLE I. TEST RESULTS AND NUMBER OF BITS FLIPPED

Case Number	Bits Total	Number of Bits Flipped		
		First Character of Key	Middle Character of Key	Last Character of Key
1	352	72	106	83
2	2560	559	816	571
3	3088	695	1040	648
4	3472	769	1188	660
5	3840	821	1287	843
Average Bits Flipped		583	887.4	561

To find out the value of the avalanche effect, first look for the number of different bits. Table I shows that there are five sample case studies conducted on the proposed three-layer encryption approach. The five cases have different bits, from the smallest to the largest, with the smallest number of bits

being 352 bits and the largest being 3840 bits. Therefore, several parameters are needed to get the different number of bits. The avalanche effect measurement in Table 1 is based on three parameters, namely changes to the initial character of the key, the middle character of the key, and the final character of the key.

In Table 1, the number of bits flipped shows the number of bits that change when changes are made to the key used. For example, case number 5 has a total of 3840 bits. After changing the initial character of the key used, the number of bits changed is 821 bits, the middle character of the key is 1287 bits, and the final character is 843 bits. This shows that changes made to the key have an impact on the number of different bits of the encryption result. Based on the average of the Number of Bits Flipped contained in Table I, the change in the middle character of the key has the most significant result, which is 887.4 bits flipped.

For a more comprehensive test, another trial was also carried out by comparing the avalanche effect value of the proposed approach with the avalanche effect measurement results from the hill cipher only, autokey only, and columnar transportation only algorithms. The measurement results for each of these algorithms can be seen in Table II.

TABLE II. AVALANCHE EFFECT MEASUREMENT RESULTS

Case Number	Avalanche Effect			
	Hill	Autokey	Colomnar	Proposed
1	21.59%	1.45%	16.89%	30.11%
2	23.44%	0.16%	19.32%	31.88%
3	23.32%	0.16%	19.31%	33.68%
4	20.54%	0.09%	19.74%	34.22%
5	22.94%	0.13%	18.75%	33.52%
Average	22.37%	0.40%	18.80%	32.68%

Table II shows the results of the avalanche effect measurement on the existing sample. The avalanche effect measurements contained in Table II are carried out based on changes in the parameters of the middle character of the key, both in the autokey key, Hill cipher, and column transposition. It can be seen in Table II that each method for each case has different avalanche effect measurement results. Based on Table II, the avalanche effect values for each algorithm are not much different for each case sample. For example, the proposed approach has an avalanche effect value range between 30-33%. Hill cipher has a value range between 20-23% and columnar with an AE value range between 16-19%. It can be concluded that the three-layer encryption protocol proposed in this study has a higher avalanche effect value than other algorithms. More clearly, these results can also be seen in Fig. 3.

Based on Fig. 3, the autokey cipher has the smallest avalanche effect value compared to other algorithms. Sequentially based on the value of the most significant avalanche effect from a sample of five cases, there are three-layer encryption protocols, hill cipher only, columnar only, and the last one is autokey only. Fig. 3 shows that the AE value of the proposed approach has a large gap compared to other methods. For example, the proposed approach with hill cipher only has a 10-12% gap, and even the autokey cipher has a gap of around 30%. These results indicate that the proposed three-layer encryption approach through a combination of substitution and transposition cryptography techniques can provide better results.

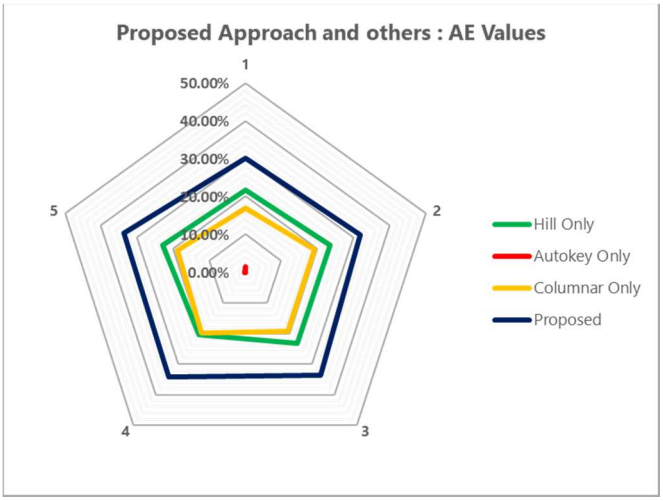

Fig. 3. The Comparison of Avalanche Effect Values

V. CONCLUSION

The three-layer encryption protocol proposed in this study consists of three encryption stages: the first layer encryption with the hill cipher, the second layer encryption using the autokey cipher, and the last layer encryption using columnar transposition cipher. The measurement results using the avalanche effect have shown that the proposed approach has the highest value with an average value of 32.68%. Based on the results of this study, it can be concluded that the proposed three-layer encryption approach, through a combination of hill cipher algorithms, autokey ciphers, and column transpositions, can produce a better level of security in securing data than single-layer encryption.

REFERENCES

[1] S. Aldossary and W. Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 4, pp. 485–498, 2016, doi: 10.14569/ijacsa.2016.070464.

[2] J. K. Shanmugam and M. H. C. Haat, "The Impact of Internal Control on the Performance of Small and Medium Enterprise : Malaysian Evidence," in *SIBR Conference on Interdisciplinary BUsiness and Economics Research*, 2012, no. JUNE, pp. 1–12.

[3] A. Tchernykh, U. Schwiegelsohn, E. ghazali Talbi, and M. Babenko, "Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability," *J. Comput. Sci.*, vol. 36, 2019, doi: 10.1016/j.jocs.2016.11.011.

[4] F. Thabit, S. Alhomdy, and S. Jagtap, "Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing," in *Global Transitions Proceedings*, 2021, vol. 2, no. 1, pp. 100–110, doi: 10.1016/j.gltp.2021.01.014.

[5] S. Choi, J. H. Yun, and S. K. Kim, "A comparison of ICS datasets for security research based on attack paths," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11260 LNCS, Springer International Publishing, 2019, pp. 154–166.

[6] H. N. Noor Muchsin, D. E. Sari, D. R. Ignatius Moses Setiadi, and E. H. Rachmawanto, "Text Encryption using Extended Bit Circular Shift Cipher," in *Proceedings of 2019 4th International Conference on Informatics and Computing, ICIC 2019*, 2019, pp. 0–4, doi: 10.1109/ICIC47613.2019.8985708.

[7] O. G. Abood and S. K. Guirguis, "A Survey on Cryptography Algorithms," *Int. J. Sci. Res. Publ.*, vol. 8, no. 7, 2018, doi: 10.29322/ijsrp.8.7.2018.p7978.

[8] B. B. Ahamed and M. Krishnamoorthy, "SMS Encryption and Decryption Using Modified Vigenere Cipher Algorithm," *J. Oper. Res. Soc. China*, 2020, doi: 10.1007/s40305-020-00320-x.

[9] J. R. Paragas, A. M. Sison, and R. P. Medina, "Hill cipher modification: A simplified approach," in *2019 IEEE 11th International Conference*

on Communication Software and Networks, ICCSN 2019, 2019, pp. 821–825, doi: 10.1109/ICCSN.2019.8905360.

[10] N. Atikah, M. R. Ashila, D. R. I. M. S. Setiadi, E. H. Rachmawanto, and C. A. Sari, "AES-RC4 Encryption Technique to Improve File Security," in *Proceedings of 2019 4th International Conference on Informatics and Computing, ICIC 2019*, 2019.

[11] F. Maqsood, M. Ahmed, M. Mumtaz, and M. Ali, "Cryptography: A Comparative Analysis for Modern Techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, 2017, doi: 10.14569/ijacsa.2017.080659.

[12] A. Elmogy, Y. Bouteraa, R. Alshabanat, and W. Alghaslan, "A New Cryptography Algorithm Based on ASCII Code," *19th Int. Conf. Sci. Tech. Autom. Control Comput. Eng. STA 2019*, pp. 626–631, 2019, doi: 10.1109/STA.2019.8717194.

[13] B. Purnama and A. H. H. Rohayani, "A New Modified Caesar Cipher Cryptography Method with LegibleCiphertext from a Message to Be Encrypted," *Procedia Comput. Sci.*, vol. 59, no. Iccsci, pp. 195–204, 2015, doi: 10.1016/j.procs.2015.07.552.

[14] A. Saraswat, C. Khatri, Sudhakar, P. Thakral, and P. Biswas, "An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication," in *Procedia Computer Science*, 2016, vol. 92, pp. 355–360, doi: 10.1016/j.procs.2016.07.390.

[15] P. Poonia and P. Kantha, "Comparative Study of Various Substitution and Transposition Encryption Techniques," *Int. J. Comput. Appl.*, vol. 145, no. 10, pp. 24–27, 2016, doi: 10.5120/ijca2016910783.

[16] A. Verma and N. Kaur, "A Comparative Study of Classical Substitution Ciphers," *Int. J. Eng. Res. Technol.*, vol. 3, no. 9, pp. 360–364, 2014.

[17] D. C. Brown, "A cryptanalysis of the autokey cipher using the index of coincidence," in *Proceedings of the ACMSE 2018 Conference*, 2018, vol. ACM SE '18, pp. 1–8, doi: 10.1145/3190645.3190679.

[18] S. Siregar, F. Fadlina, and S. Nasution, "Enhancing Data Security of Columnar Transposition Cipher by Fibonacci Codes Algorithm," in *Proceedings of the Third Workshop on Multidisciplinary and Its Applications, WMA-3 2019*, 2020, pp. 1–10, doi: 10.4108/eai.11-12-2019.2290839.

[19] D. P. Timothy and A. K. Santra, "A hybrid cryptography algorithm for cloud computing security," *2017 Int. Conf. Microelectron. Devices, Circuits Syst. ICMDCS 2017*, vol. 2017-Janua, pp. 1–5, 2017, doi: 10.1109/ICMDCS.2017.8211728.

[20] D. Vashi, H. B. Bhadka, K. Patel, and S. Garg, "An Efficient Hybrid Approach of Attribute Based Encryption for Privacy Preserving Through Horizontally Partitioned Data," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 2437–2444, 2020, doi: 10.1016/j.procs.2020.03.296.

[21] M. D. Sinaga, N. S. B. Sembiring, F. Tambunan, and C. J. M. Sianturi, "Hybrid Cryptography WAKE (Word Auto Key Encryption) and Binary Caesar Cipher Method for Data Security," *2018 6th Int. Conf. Cyber IT Serv. Manag. CITSM 2018*, no. Citsm, pp. 1–5, 2019, doi: 10.1109/CITSM.2018.8674346.

[22] O. Grošek, E. Antal, and T. Fabšič, "Remarks on breaking the Vigenère autokey cipher," *Cryptologia*, vol. 43, no. 6, pp. 486–496, 2019, doi: 10.1080/01611194.2019.1596997.

[23] B. Triandi, E. Ekadiansyah, R. Puspasari, L. T. Iwan, and F. Rahmad, "Improve Security Algorithm Cryptography Vigenere Cipher Using Chaos Functions," *2018 6th Int. Conf. Cyber IT Serv. Manag. CITSM 2018*, no. Citsm, pp. 1–5, 2019, doi: 10.1109/CITSM.2018.8674376.

[24] B. Bjorkman and R. Talbert, "Fixed Points of Columnar Transpositions," *J. Discret. Math. Sci. Cryptogr.*, vol. 18, no. 5, pp. 541–557, 2015, doi: 10.1080/09720529.2014.986910.

[25] G. Lasry, N. Kopal, and A. Wacker, "Cryptanalysis of columnar transposition cipher with long keys," *Cryptologia*, vol. 40, no. 4, pp. 374–398, 2016, doi: 10.1080/01611194.2015.1087074.

[26] D. Nofriansyah *et al.*, "A New Image Encryption Technique Combining Hill Cipher Method, Morse Code and Least Significant Bit Algorithm," *J. Phys. Conf. Ser.*, vol. 954, no. 1, 2018, doi: 10.1088/1742-6596/954/1/012003.

[27] A. A. M. Khalaf, M. S. A. El-Karim, and H. F. A. Hamed, "A triple hill cipher algorithm proposed to increase the security of encrypted binary dataand its implementation using FPGA," *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 2016-March, no. 1, pp. 752–759, 2016, doi: 10.1109/ICACT.2016.7423615.

[28] Z. E. Dawahdeh, S. N. Yaakob, and R. Razif bin Othman, "A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 3, pp. 349–355, 2018, doi: 10.1016/j.jksuci.2017.06.004.

[29] M. A. Budiman, D. Rachmawati, and Jessica, "Implementation of Super-Encryption with Trithemius Algorithm and Double Transposition Cipher in Securing PDF Files on Android Platform," *J. Phys. Conf. Ser.*, vol. 978, no. 1, 2018, doi: 10.1088/1742-6596/978/1/012088.

[30] A. Djamalilleil, M. Muslim, Y. Salim, E. I. Alwi, H. Azis, and Herman, "Modified Transposition Cipher Algorithm for Images Encryption," in *Proceedings - 2nd East Indonesia Conference on Computer and Information Technology: Internet of Things for Industry, EIConCIT 2018*, 2018, pp. 1–4, doi: 10.1109/EIConCIT.2018.8878326.

[31] M. G. Z. Fernando, A. M. Sison, and R. P. Medina, "Securing Private Key using New Transposition Cipher Technique," in *2019 IEEE Eurasia Conference on IOT, Communication and Engineering, ECICE 2019*, 2019, pp. 490–493, doi: 10.1109/ECICE47484.2019.8942798.

[32] F. Twum, J. B., and M.-D. William, "A Proposed Enhanced Transposition Cipher Algorithm based on Rubik's Cube Transformations," *Int. J. Comput. Appl.*, vol. 182, no. 35, pp. 18–26, 2019, doi: 10.5120/ijca2019918323.

[33] W. Abduallah and S. Mohammed Zeebaree, "New Data hiding method based on DNA and Vigenere Autokey," *Acad. J. Nawroz Univ.*, vol. 6, no. 3, pp. 83–88, 2017, doi: 10.25007/ajnu.v6n3a83.

[34] S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, "Data Security Using Vigenere Cipher and Goldbach Codes Algorithm," *Int. J. Eng. Res. Technol.*, vol. 6, no. 01, pp. 360–363, 2017.

[35] R. Mahendran and K. Mani, "Generation of Key Matrix for Hill Cipher Encryption Using Classical Cipher," *Proc. - 2nd World Congr. Comput. Commun. Technol. WCCCT 2017*, pp. 51–54, 2017, doi: 10.1109/WCCCT.2016.22.

[36] E. H. Rachmawanto, D. R. I. M. Setiadi, C. A. Sari, and N. Rijati, "Imperceptible and secure image watermarking using DCT and random spread technique," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 4, pp. 1750–1757, 2019, doi: 10.12928/TELKOMNIKA.v17i4.9227.

[37] S. Patidar, Ganesh Agrawal, Nitin Tarmakar, "A block based Encryption Model to improve Avalanche Effect for data Security," *Int. J. Sci. Res. Publ.*, vol. 3, no. 1, pp. 1–4, 2013.